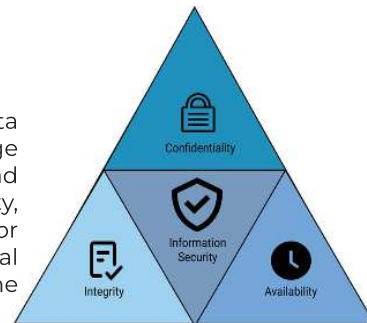


Information Security



The Global Information Security Landscape

Information security protects sensitive data from unauthorized access, theft, and damage through policies, procedures, technologies, and training. It ensures the confidentiality, integrity, and availability of information, crucial for businesses and individuals in today's digital world where reliance on technology and the internet is ever-increasing.



Humans are the weakest link in the security chain.
 – Kevin Mitnick, computer security consultant, author, and convicted hacker

The global market size was valued at USD 172.24 billion in 2023. The market is projected to grow from USD 193.73 billion in 2024 to USD 562.72 billion by 2032, exhibiting a CAGR of 14.3% during the forecast period.¹

Since COVID-19, cybercrime has surged by 300%, with the cost of such breaches expected to top USD 5 trillion by 2024.² This surge is fueled by the growing dependency on technology, expanding attack surface, increasing interconnectedness of systems, the rise of the Internet of Things (IoT), AI integration, cloud adoption, and stringent regulations like General Data Protection Regulation (GDPR) in EU and Personal Information Protection Law (PIPL) in China.

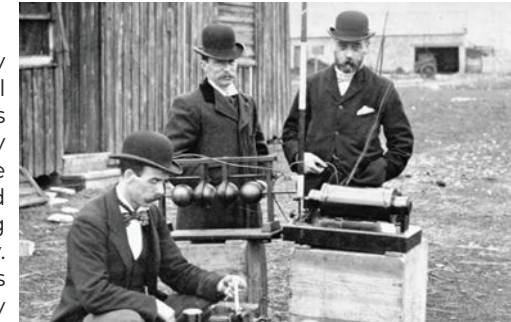
As cyber threats evolve and increase, investment in this sector is continuously growing as well. According to Gartner, 80% of CIOs plan to boost cybersecurity

spending in 2024.³ The Global X Cybersecurity ETF, tracking sector performance, rose by 20% in the past year⁴.

The top three cybersecurity companies by market value are Fortinet, Palo Alto Networks, and CrowdStrike. Fortinet, valued at USD 441 billion, is known for its comprehensive network security solutions, including firewalls, and reported a 20% revenue growth in 2023. Palo Alto Networks, with a market value of USD 106.2 billion, focuses on network and cloud security and invests over USD 1 billion annually in research and development (R&D) to maintain its technological edge. CrowdStrike, valued at USD 77.2 billion, is a leader in AI-driven threat detection and aims to capture a USD 100 billion market by 2024 with its cloud-native Falcon platform.⁵

A Historical Perspective

The first known hack dates back to the early 20th century, when magician Nevil Maskelyne interrupted Guglielmo Marconi's wireless telegraph demonstration. Hired by the Eastern Telegraph Company, Maskelyne used a powerful wireless transmitter to send disruptive Morse code messages, including the word "rats" and mocking lines of poetry. This public stunt revealed the vulnerabilities in Marconi's invention and marked an early instance of technological interference in communication systems.



British Post Office engineers inspect Marconi's radio equipment during a demonstration on Flat Holm Island, 13 May 1897.



Information security originated in the early days of computing, with a primary focus on securing physical access to mainframes and protecting sensitive data. In the 1950s, hacking began to surface through phone phreaking. The 1960s introduced basic access controls and laid the foundation for computer security principles as computing expanded into institutional settings. The 1970s saw the development of encryption standards like the Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA). Reaper was the first anti-virus software,

designed to delete Creeper by moving across the ARPANET. It was created by Tomlinson in 1972.⁶

The 1980s marked a shift towards network security, with the invention of firewalls creating barriers between internal networks and external threats. In 1986, the Brain virus, created by Pakistani brothers Amjad and Basit Farooq Alvi, became the first PC virus to spread globally, showing the impact of malware on personal computers. In 1987, antivirus software like McAfee, NOD, and UVK

¹ Cybersecurity Market Size, Share, Analysis | Global Report 2032. (2024, September 09). Retrieved from <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>

² United Nations. (2024, September 12). As Internet user numbers swell due to pandemic, UN Forum discusses measures to improve safety of cyberspace | United Nations. United Nations. Retrieved from <https://www.un.org/en/desa/internet-user-numbers-swell-due-pandemic-un-forum-discusses-measures-improve-safety-cyberspace>

³ IT Spending & Budgets: Trends & Forecasts 2024 | Splunk. (2024, September 24). Retrieved from https://www.splunk.com/en_us/blog/learn/it-tech-spending.html

⁴ Global X Cybersecurity ETF (BUG). (2024, June 27). Retrieved from <https://www.globalxetfs.com/funds/bug>

⁵ Taulli, T. (2024). 6 Cybersecurity Stocks to Buy Now. Kiplinger. Retrieved from <https://www.kiplinger.com/investing/stocks/tech-stocks/602685/cybersecurity-stocks-to-lock-up-growth>

⁶ A Brief History of Computer Viruses & What the Future Holds. (2018, October 19). Retrieved from <https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>



officially marked the birth of the information security industry.⁷ This era witnessed the rise of computer worms and viruses, including the Morris Worm in 1988, which demonstrated the potential for widespread disruption.⁸

The 1990s brought significant advancements, including public key infrastructure (PKI) for secure communications, the Secure Sockets Layer (SSL)⁹ protocol for encrypting internet traffic, and intrusion detection systems (IDS). These innovations were crucial as the internet expanded, and e-commerce became prevalent.

In the 2000s, information security evolved into a formal discipline with the development of advanced threat detection tools. Incidents like the Code Red and Slammer worms underscored the need for improved security technologies.¹⁰

The 2010s expanded into cloud and mobile security, driven by the adoption of cloud computing and mobile devices, alongside stricter data privacy regulations like GDPR. The 2020s have seen the rise of AI and machine learning for enhanced threat detection, the adoption of zero-trust architecture, and a critical focus on securing supply chains, highlighted by incidents like the SolarWinds breach,¹¹ underscoring vulnerabilities in interconnected systems.



Pakistani brothers Amjad and Basit Farooq Alvi, creators of the Brain virus, 1986

Contemporary Attacks

Over the years, threats have evolved in sophistication and scale, with each major breach highlighting new vulnerabilities and driving the need for stronger information security measures.

In 2005, the TJX Companies Inc. data breach exposed 94 million credit and debit card numbers due to weak encryption, prompting a major shift in payment security standards.¹² The 2011 Sony PlayStation Network hack compromised 77 million accounts, leading to a 23-day outage and substantial financial losses.¹³

By 2013, the Target data breach revealed vulnerabilities in point-of-sale systems, affecting 110 million customers. The Yahoo data breaches in 2013 and 2014, impacting over 3 billion accounts,¹⁴ became the largest ever and significantly hurt Yahoo's valuation during its acquisition by Verizon.¹⁵

Trust but verify.
– Ronald Reagan (often used in the context of cybersecurity)



The threat landscape continued to evolve with the 2015 Ukrainian Power Grid Hack, which caused a blackout for 230,000 people, marking a notable attack on critical infrastructure.¹⁶ In 2016, the Mirai Botnet Attack exploited unsecured IoT devices for DDoS attacks, exposing flaws in

everyday technology.¹⁸ The 2017 WannaCry ransomware attack crippled healthcare systems globally, highlighting risks from outdated systems. The Aadhaar data leak in 2018, revealing biometric information of 1.1 billion Indian citizens, raised national security concerns.¹⁹

⁷ Xu, W., & Gran, G. (2008). Security breach: The case of TJX Companies, Inc. *Communications of the Association for Information Systems*, 23(11). Retrieved from <https://aiselaisnet.org/cgi/viewcontent.cgi?article=3391&context=cais>

⁸ Ibid.

⁹ The Evolution of SSL and TLS. (2024, September 12). Retrieved from <https://www.digicert.com/blog/evolution-of-ssl>

¹⁰ Of Encyclopaedia Britannica, T. E. (2024). Computer worm | Malware, Cybersecurity & Networking. Encyclopaedia Britannica. Retrieved from <https://www.britannica.com/technology/computer-worm>

¹¹ Temple-Raston, D. (2021). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. NPR. Retrieved from <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>

¹² Xu, W., & Gran, G. (2008). Security breach: The case of TJX Companies, Inc. *Communications of the Association for Information Systems*, 23(11). Retrieved from <https://aiselaisnet.org/cgi/viewcontent.cgi?article=3391&context=cais>

¹³ Quinn, B., & Arthur, C. (2020). PlayStation Network hackers access data of 77m users. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data>

¹⁴ Columbia University School of International and Public Affairs. (2022). Target final report. Columbia University. Retrieved from <https://www-sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf>

¹⁵ Peritoth, N. (2017). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. *N.Y. Times*. Retrieved from <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>

¹⁶ Of Encyclopaedia Britannica, T. E. (2024). Computer worm | Malware, Cybersecurity & Networking. Encyclopaedia Britannica. Retrieved from <https://www.britannica.com/technology/computer-worm>

¹⁷ Temple-Raston, D. (2021). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. NPR. Retrieved from <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>

¹⁸ Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat. *Ransomware attack 2017. International journal of advanced research in computer science*, 8(5), 1938-1940.

¹⁹ Safi, M. (2018). Personal data of a billion Indians sold online for £6. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar>

The 2020-2021 SolarWinds supply chain attack demonstrated vulnerabilities in software supply chains, affecting thousands of organizations, including U.S. government agencies.²⁰ In 2021, the Log4Shell vulnerability exploited flaws in embedded software across millions of applications.²¹ That year also saw the Pegasus spyware scandal, revealing state-sponsored surveillance of high-profile targets.²² The T-Mobile data breach of 2021, compromising over 40 million customers' data, underscored the persistent threat of large-scale data theft.²³ Finally, the Kaseya ransomware attack in 2021 impacted up to 1,500 businesses globally, highlighting the escalating danger of ransomware in supply chains.²⁴

The intentions behind attacks are diverse: insiders, such as employees or contractors, may exploit their access for personal gain or revenge, as demonstrated by Terry Childs in 2008 when he locked San Francisco's network and withheld passwords.²⁵ State-sponsored hackers, such as those behind the 2010 Stuxnet's sabotage of Iran's nuclear program, aim to conduct espionage or disrupt infrastructure.²⁶

Hackers, driven by ideological motives, use hacking as a form of protest or to expose corruption, as seen in Anonymous's 2012 DDoS attacks against government and corporate websites in protest of anti-piracy laws.²⁷ Script kiddies, often inexperienced hackers, use pre-written scripts for fame or mischief; a notable example is the 2015 TalkTalk hack, where a 17-year-old exploited an SQL vulnerability to steal data.²⁸ Cyber terrorists seek to instill fear or disrupt critical systems, as demonstrated by the 2015 Ukrainian Power Grid Hack, which caused a blackout affecting 230,000 people.²⁹ Brokers, meanwhile, exploit vulnerabilities to sell stolen data, such as the 2016 Yahoo breach, where data from 500 million users was sold on the dark web.³⁰ Cyber criminals, motivated by financial gain, conduct attacks like the 2017 WannaCry ransomware, which targeted computers globally, demanding Bitcoin payments to unlock files.³¹



Future of Information Security

You can't protect what you don't understand.
– Gerald Koch, German scientist and professor

In 2023 alone, startups in this space globally raised over USD 10 billion, with significant investments flowing into sectors such as financial services, supply chain and critical infrastructure. The global cybersecurity market size was valued at USD 172.24 billion in 2023. The market is projected to grow from USD 193.73 billion in 2024 to USD 562.72 billion by 2032, exhibiting a CAGR of 14.3% during the forecast period.³²

Information security threats are rapidly evolving, driven by advances in technology and the increasing sophistication of attacks. Emerging technologies such as blockchain, AI, and machine learning (ML) have become both tools for cybercriminals and vital defenses for organizations. AI and ML are transforming information



security by enhancing threat detection, automating incident responses, and predicting potential vulnerabilities. These technologies excel at analyzing large datasets to identify patterns and anomalies, crucial for detecting advanced persistent threats (APTs) and sophisticated attacks. In Security Operations Centers (SOCs), AI is enhancing efficiency by automating routine tasks like log analysis and incident triage, allowing security teams to focus on more complex and strategic issues.

The growing emphasis on supply chain security is another key trend, as organizations become more reliant on third-party vendors. The recent pager explosions in Lebanon have brought renewed attention to the importance of securing supply chains. The devices, which were tampered with during their manufacturing and distribution process, illustrate how vulnerabilities in supply chains can be exploited to execute cyber-physical attacks.³³

It is estimated that a powerful enough quantum computer could crack state of the art encryption (RSA-2048) in



³² Cybersecurity Market Size, Share, Analysis | Global Report 2032. (2024, September 09). Retrieved from <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>

³³ Exploding pagers injure thousands in Lebanon: New details emerge. (2024, September 18). NBC News. Retrieved from <https://www.nbcnews.com/news/world/taiwan-firm-denies-making-pagers-used-lebanon-explosions-rcna171594>

²⁰ Temple-Raston, D. (2021). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. NPR. Retrieved from <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>

²¹ Everson, D., Cheng, L., & Zhang, Z. (2022, November). Log4shell: Redefining the web attack surface. In Proc. Workshop Meas., Attacks, Defenses Web (MADWeb) (pp. 1-8).

²² Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries.

²³ I. V., A. P. (2024). T-Mobile Will Pay Record-Breaking \$60 Million Settlement Over Alleged National Security Violations. Forbes. Retrieved from <https://www.forbes.com/sites/antoniopequenoi/2024/08/14/t-mobile-will-pay-record-breaking-60-million-settlement-over-alleged-data-breach-violations>

²⁴ Krehel, O. (2022). The 2021 Kaseya Attack Highlighted The Seven Deadly Sins Of Future Ransomware Attacks. Forbes. Retrieved from <https://www.forbes.com/councils/forbestechcouncil/2022/01/25/the2021-kaseyattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks>

²⁵ Reuters. (2010). After the verdict, debate rages in Terry Childs' case. Reuters. Retrieved from <https://www.reuters.com/article/world/after-verdict-debate-rages-in-terry-childs-case-idUS2783388820>

²⁶ Kushner, D. (2024). The Real Story of Stuxnet. IEEE Spectr. Retrieved from <https://spectrum.ieee.org/the-real-story-of-stuxnet>

²⁷ Coleman, G. (2012). Beacons of Freedom. Index on Censorship, 41(4), 62-71. doi: 10.1177/0306422012466029

²⁸ A former hacker wants to stop others like him. The law won't allow him. (2024, September 12). Retrieved from <https://www.werone-ws.com/next/2022/08/21/i-went-to-prison-for-the-77m-talktalk-hacking-i-could-be-sent-back-for-ordering-a-mcdonald>

²⁹ Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388(1-29), 3.

³⁰ Perltroth, N. (2016). Yahoo Says Hackers Stole Data on 500 Million Users in 2014. N.Y. Times. Retrieved from <https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html>

³¹ Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International journal of advanced research in computer science, 8(5), 1938-1940.



just hours or days, a task that would take classical computers millions of years. In response to this threat, there is a significant push toward developing quantum-resistant encryption algorithms. In 2022, the U.S. National Institute of Standards and Technology (NIST) selected its first group of encryption algorithms for post-quantum cryptography, expected to be widely adopted by 2024 to safeguard against quantum attacks. The global market for quantum security solutions is expected to grow significantly, with estimates predicting the quantum cryptography market will exceed USD 2.9 billion by 2030, driven by rising concerns over quantum threats.

Enterprise customers are increasingly seeking comprehensive cybersecurity platforms over individual point solutions. They require coverage across all facets of their operations, including users (remote or in-office),

devices (IoT and OT), applications (SaaS), data (at rest or in motion), and development environments (on-premise or in the cloud). They also demand automation, analytics, AI, and generative AI for improved security.

In response, major cybersecurity players have adapted, driving significant vendor consolidation and strategic partnerships. Cisco acquired Splunk, Broadcom purchased VMware, and Fortinet is acquiring Lacework. Additionally, partnerships like IBM with Palo Alto Networks and CrowdStrike with Cloudflare demonstrate this strategic shift towards integrated, platform-based solutions.³⁴



Information Security Landscape in Pakistan

Pakistan's information security industry, its sustained innovation and commitment to excellence, have set the foundation for a secure digital future. In 2024, Pakistan has risen to the Tier-1 (Role-modelling) rating and is now among top 40 countries in the Global Cybersecurity Index (GCI) 2024 issued by International Telecommunication Union (ITU), a notable improvement from its previous 79th position.³⁵

Pakistan's revenue in the information security market is projected to reach USD 161.8 million in 2024. Information security solutions dominate the market with a projected market volume of USD 90.71 million in 2024.³⁵

The evolution of information security in Pakistan has been marked by a dynamic journey of growth, adaptation, and innovation. Some pioneering firms, established during the early 2000s, have played a pivotal role in shaping the country's information security industry, setting standards, and building capabilities that align with global benchmarks. The journey began with the establishment of Pakistan Computer Emergency Response Team (PakCERT) in 2000, the first



³⁴ 10 most powerful cybersecurity companies today. (2024, July 02). Retrieved from <https://www.csoonline.com/article/569075/the-10-most-powerful-cybersecurity-companies.html>

³⁵ Cybersecurity - Pakistan | Statista Market Forecast. (2024, June). Retrieved from <https://www.statista.com/outlook/tmo/cybersecurity/pakistan>

information security solutions provider in Pakistan. PakCERT's mission was to respond to security incidents, track intruder activities, and collaborate with international agencies on information security issues.

As the first line of defense, PakCERT laid the foundation for a structured approach to managing threats, offering services such as vulnerability assessments, penetration testing, and digital forensic analysis. Its contributions were crucial in fostering a security-conscious environment among public, private, and government entities in Pakistan. PakCERT's involvement in identifying vulnerabilities, such as the critical flaw in Microsoft .NET Passport services, showcased the country's growing expertise in global cybersecurity affairs.³⁶

In 2005, Trillium Information Security Systems (TISS) in 2005³⁷ was established which further strengthened Pakistan's

information security landscape. With regional offices in major cities and strategic partnerships with international giants like Kaspersky, Cisco, and IBM Security, TISS emerged as a formidable player.

Tranchulas, founded in 2006, also played a crucial role in this transformation. Tranchulas became a global provider of offensive and defensive security solutions, offering penetration testing, threat detection, incident response, and compliance management services.³⁸

By 2010, the information security landscape in Pakistan had evolved significantly, driven by an increasing number of intrusions and the expanding digital footprint of companies offering comprehensive information security services. From early pioneers to modern innovators, these organizations have helped build a resilient and adaptable information security ecosystem.



³⁶ PakCERT - Top Cyber Security Company in Pakistan (since 2000). Retrieved from <https://www.pakcert.org>

³⁷ Leading Global Provider of Cybersecurity Services | Trillium Information Security Systems | Trillium Information Security Systems. (2024, June 05). Retrieved from <https://www.trilliuminfosec.com>

³⁸ Tranchulas. Retrieved from <https://tranchulas.com>

Legal Reforms and Institutional Developments

Over the years, Pakistan has established information security and information protection frameworks, responding to evolving threats with legal reforms and institutional developments.

The Electronic Transactions Ordinance (ETO) 2002, was an early digital regulation in Pakistan, recognizing electronic documents, records, and signatures to facilitate electronic transactions and e-commerce.³⁹ While indirectly focused on information security, it mandated the protection of electronic records against unauthorized access and tampering, thereby establishing a legal foundation for information security in the country.

In 2007, the Federal Investigation Agency (FIA) established the National Response Centre for Cyber Crimes (NR3C), which was tasked with investigating and prosecuting cybercrimes in Pakistan.⁴⁰ NR3C has since become a central authority for handling cyber complaints, digital forensics, and cybercrime



investigations. It has played a pivotal role in creating awareness and enforcing cyber laws.

The Prevention of Electronic Crimes Act (PECA) 2016⁴¹ marked a significant milestone in Pakistan's information security landscape. PECA serves as the primary legislation for combating cybercrimes, criminalizing activities such as unauthorized access to information systems, data theft, cyber terrorism, and identity theft. While it does not include explicit provisions for breach notification, PECA has stringent penalties, including fines and imprisonment, for offenses related to unauthorized data access. PECA has since become the cornerstone of Pakistan's legal response to digital threats. The Pakistan Telecommunication Authority (PTA) regulates telecommunications and internet services in Pakistan, focusing on consumer data protection within the telecom sector.

In June 2018, the Government of Pakistan launched the National Centre for Cyber Security (NCCS) as a collaborative project between the Higher Education Commission (HEC) and the Planning Commission. The NCCS functions as a research and development hub for information security, with affiliated labs across 11 universities specializing in areas such as cybercrime forensics, smart devices, and network security. Air University serves as the NCCS Secretariat, highlighting academia's role in bolstering national information security capabilities.⁴²

³⁹ Government of Pakistan. (2002). Electronic Transactions Ordinance 2002. Pakistan Law Site. <http://www.pakistanlaw.com/eto.pdf>

⁴⁰ National Response Centre For Cyber Crime. (2024, July 12). Retrieved from <https://www.nr3c.gov.pk>

⁴² National Assembly of Pakistan. (2016). Prevention of Electronic Crimes Act 2016. Government of Pakistan. https://www.na.gov.pk/uploads/documents/1470910659_707.pdf

In January 2021, Pakistan introduced the National Cybersecurity Policy,⁴³ aiming to fortify existing information security frameworks, introduce advanced measures, and promote public-private partnerships. The policy emphasizes enhancing the country's resilience against digital threats, securing critical infrastructure, and developing a skilled information security workforce.

In October 2023, Pakistan established its first-ever National Computer Emergency Response Team (CERT),⁴⁴ following the example of the European Computer Emergency Response Team (CERT-EU). This will be followed by provincial/sectoral CERTs to strengthen digital defense at the federal and provincial levels and facilitate

coordination between different tiers of government.

The Personal Data Protection Bill,⁵⁶ currently under consideration, aims to address data privacy and breach notification gaps by aligning Pakistan's laws with international standards like the GDPR. Key provisions include mandatory breach notifications, rights for individuals to access, correct, and delete their data, and penalties for non-compliance. If enacted, this bill would represent a significant leap toward comprehensive data protection in Pakistan.

Organizations like Digital Rights Foundation provide training and advocacy on digital privacy and online security.⁴⁵

Information Security Companies in Pakistan

Information Security companies have excited considerable interest in Pakistan. They can be broadly classified into the following categories:

Category	Companies
1. Cybersecurity Services	Tier3, Tranchulas, Compliance Wing, Trillium Information Security, TechnoGenics, Kualitatem, Global SNI, Pligence, Wateen Telecom, Inotech Solutions, Sparkeye Technologies, Catalytic Consulting, Secisys, PakCert, Rewterz, Di8it, Ebryx
2. IoT and Embedded Security	ThingzEye
3. Data Security and Privacy	Securiti AI
4. Communication & Training	Aegispeak, Commtel Systems, Cybercom Private Limited, PrivO
5. Emerging Security Platforms	Access Group, SlashNext, BugsLife, Growth Arbor, Lynx Infosec



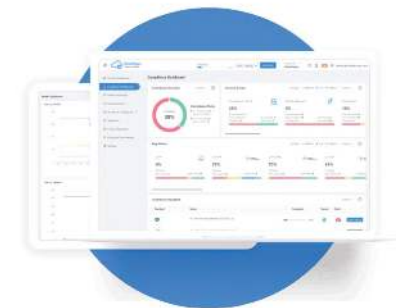
Atompoint

Atompoint is at the forefront of innovation, transforming industries, with expertise spanning cloud security and compliance, artificial intelligence, logistics, enterprise software, and IoT devices. Atompoint safeguards cloud infrastructures with real-time threat and compliance monitoring, auditing, and automated remediation. They develop scalable applications and build high impact teams, supporting different startups from launch to market readiness.

Atompoint recently integrated Cloudnosys, a state-of-the-art cybersecurity platform, across all active client projects to ensure security of digital assets.⁴⁶ They have undertaken workshops and hackathons focusing on generative AI and a wide-ranging bootcamp on software development.⁴⁷

Among other notable projects, Atompoint worked with Bykea to develop their website portal,

integrated IoT sensors for digitize the supply chain in GSK (Pharmaceutical) factories, developed the Snoonu food delivery mobile app, and built a remote team management platform for Timegram. To date they have incubated 4 startups, developed 50+ cloud solutions, and launched over 20+ enterprise applications and 10 mobile applications. Their website creation and customization tools have been used in over 75,000 websites. Their commitment to quality and innovation ensures high standards in product development and team support.



⁴³ National Centre for Cyber Security. Overview and projects. <https://nccs.pk>
⁴⁴ Ministry of Information Technology and Telecommunication. (2021). National Cyber Security Policy 2021. Government of Pakistan. <https://moitt.gov.pk/SitelImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>
⁴⁵ PKCERT - The National CERT of Pakistan. Retrieved from <https://pkcert.gov.pk>

⁴⁶ Asif. (2024). Protecting Our Clients Against Rising Cyber Threats - Atompoint. Atompoint. Retrieved from <https://atompoint.com/blog/protecting-our-clients-against-rising-cyber-threats>
⁴⁷ admin. (2024). Launch of Innovative Software Development Bootcamp - Atompoint. Atompoint. Retrieved from <https://atompoint.com/blog/innovative-software-development-bootcamp>



Tier3 Cyber Security Services

Tier3 is a leading provider of cybersecurity consultancy and IT advisory services, including cybersecurity assessments, incident response, threat intelligence, investigations, and training. The team comprises experts in cybersecurity, cryptography, digital forensics, offensive security, and intelligence and provides comprehensive solutions to safeguard digital assets. With over 12 years of expertise, Tier3 has established itself as a prominent cybersecurity authority in Pakistan. The company manages over 13,000 endpoints, has issued more than 19,000 cyber alerts, and produced over 700 in-depth reports and advisories on emerging threats.

Tier3 offers a broad range of cybersecurity services designed to address various security needs. Their cybersecurity services include a Cybersecurity Mesh Platform with Zero Trust Framework, MXDR, and 24/7 monitoring, threat hunting, and incident response. Their penetration testing services utilize chaos engineering to simulate real-world attacks, helping organizations uncover vulnerabilities and assess their security readiness. For application security, Tier3 provides Static Application Security Testing (SAST) to identify vulnerabilities in source code before compilation.



Tier3's Attack Surface Analysis helps businesses map their IT systems to identify vulnerabilities and maintain SBOMs, enhancing software supply chain security. Their Cyber Threat Intelligence services aggregate and analyze data in real-time, enabling proactive and data-driven cybersecurity actions. Additionally, Tier3 offers Cybersecurity Training and certifications, equipping employees with essential skills to defend against cyber threats.



To further support businesses, Tier3's is delivering timely cyber alerts and advisories, underscoring their commitment to fortifying the digital landscape of Pakistan.

Tier3 Pakistan also provides responsible and coordinated vulnerability disclosure programs to enhance the security posture of organizations in Pakistan. Their managed programs facilitate safe reporting of vulnerabilities by security researchers, offering end-to-end management of vulnerability submission, analysis, mitigation, and disclosure while rewarding contributors and helping organizations protect their digital assets.

Tier3 offers a range of cybersecurity products tailored to meet the needs of its clients. The Redteam Toolkit is an

advanced penetration testing suite with over 50 tools for offensive security operations, training, and real-world attack simulations. Their Digital Forensics Tools provide comprehensive software solutions for evidence collection, analysis, and court-ready reporting, supporting law enforcement and investigators. Additionally, STAFFCOP is an employee monitoring software that tracks user activity, detects insider threats, and improves workplace productivity and security with real-time alerts and intelligent behavior analysis.

Primary Products

- ▶ STAFFCOP
- ▶ Red Team Toolkit
- ▶ Digital Forensics Tool Kit





Compliance Wing

Compliance Wing specializes in providing comprehensive governance and cyber risk solutions, with a particular focus on securing payment systems. They offer a broad spectrum of services from security assessments and regulatory compliance to advanced threat intelligence and incident response. Compliance Wing has established itself as a trusted partner for government and private sector clients around the world.

The company partners with several prominent organizations across various industries, including financial services leaders like Meezan Bank, MCB, Askari Bank, EFU General Insurance, and Allianz. They also work closely with tech companies such as Sibisoft and PayFast, and collaborate with security-focused firms like IDEMIA and Twyla Technology, demonstrating a robust presence and expertise across diverse sectors.

Compliance Wing helps organizations meet international and local regulatory requirements, ensuring adherence to critical standards like PCI DSS (Payment Card Industry Data Security Standard), PCI SSF (Payment Card Industry Software Security Framework), ISMS – ISO 27001 (Information Security Management System), ISO/IEC 27017 (Cloud Security), NIST (National Institute of Standards and Technology), COBIT (Control Objectives for Information and Related Technologies), NCA Compliance (Saudi National Cybersecurity Authority), SAMA Cyber Security Framework (Saudi Arabian Monetary Authority), Saudi Data Management and Personal Data Protection Standards, General Data Protection Regulation (GDPR), HIPAA Compliance, and Swift CSP Assessment.



Compliance Wing's Security Assessments focus on identifying and mitigating vulnerabilities through services such as Penetration Testing, Source Code Review, Compromised Threat Assessment, and Cyber Security Health Check. These assessments aim to strengthen the security posture of systems, applications, and code, ensuring organizations meet best practices and remain compliant.

The company provides proactive and reactive cybersecurity solutions designed to protect against advanced threats. These include Digital Forensics & Incident Response to analyze and respond to cyber incidents, Breach and Attack Simulation (BAS) to test defense mechanisms, Virtual CISO (VCISO) services for strategic cybersecurity leadership, Threat Intelligence Service for insights into emerging threats, and OT/ICS/SCADA security to safeguard critical infrastructure and industrial control systems.

Compliance Wing offers Cyber Security Training tailored to enhance the skills

of security professionals within organizations. These programs focus on equipping teams with the necessary knowledge to protect against and respond to evolving cyber threats, supporting the development of a resilient cybersecurity framework.

Additional services include File Integrity Monitoring (FIM), which validates the integrity of system and application files through cryptographic checksums, and Security Information & Event Management (SIEM), a unified security management system integrating security information and event management functions. The company's Card Holder Data Scanning Tool, trusted by over 2,500 merchants globally, aids PCI compliance by accurately identifying cardholder data across various operating systems. The experienced compliance team ensures seamless deployment and training, empowering clients to manage their IT investments effectively and independently.





Trillium Information Security Systems (Pvt) Ltd

Trillium Information Security Systems (TISS), established in 2005, is a global leader in cybersecurity solutions with nearly two decades of expertise. With regional offices in Islamabad, Lahore, Karachi, Riyadh, and Doha, TISS delivers cutting-edge cybersecurity services, safeguarding businesses worldwide from evolving cyber threats.



Their strategic partnerships with industry giants like Kaspersky, Rapid7, Cisco, Forcepoint, and IBM Security enhance their ability to provide top-tier solutions across diverse industries. TISS's impressive track record includes serving over 600 customers, 60 financial institutions, training more than 3,000 information security professionals, and forging 20+



partnerships with leading cybersecurity companies.

They have also delivered cybersecurity solutions to 20+ telecom operators and over 50 companies in the industrial sector, showcasing their unmatched expertise, commitment to quality, and proven ability to meet the needs of clients across various sectors.

Trillium Information Security Systems (TISS) provides a robust portfolio of security services and products designed to protect organizations against evolving cyber threats.

Their Security Assessment Services simulate real-world attacks to identify system vulnerabilities, while their Managed SOC Services offer comprehensive threat monitoring and incident response without the need for in-house SOC capabilities. Governance, risk and compliance services help organizations assess security posture and ensure regulatory compliance across all locations.

TISS's Digital Forensics & Incident Response (DFIR) services enable swift investigation and remediation of cyber incidents, while their Email



Phishing Simulation Service tests employee responses to phishing attempts to strengthen security awareness. The Security Awareness Portfolio equips employees with the skills needed to detect and respond to cyber threats, and Red Team Services simulate attacks to test the effectiveness of an organization's defenses.

TISS also offers advanced products, including the Cyber Deception Platform (CDP), which deploys decoys to detect breaches and capture forensic data on threat actors, and the Cyber Threat Intelligence Platform (CTIP), which aggregates threat data to inform security decisions. Finally, their Cydea Security Information and Event Management (SIEM) provides comprehensive infrastructure monitoring to help detect and respond to threats efficiently.

Primary Products

- ▶ **Cyber Deception Platform (CDP)**
- ▶ **Cyber Threat Intelligence Platform**
- ▶ **Cydea Security Information and Event Management (SIEM)**



As the oldest cybersecurity company in Pakistan, Trillium Information Security Systems has set the standard for excellence in the industry.

– Jawad Khalid Mirza, CISO, Askari Bank.



Tranchulas Private Limited

Founded in 2006, as a global provider of both offensive and defensive cyber solutions, Tranchulas is committed to safeguarding enterprises and government organizations through customized information security services tailored to meet their unique business needs.

With four offices worldwide, Tranchulas has built a robust global presence, serving 1,273 satisfied customers and training 3,209 students. Tranchulas has worked with a diverse range of prestigious clients, including BBC, DP World, Angel, Waterstone, Axiell, British Airways, and Cobham, showcasing their extensive expertise and trusted reputation in the industry.

Tranchulas offers a comprehensive suite of cybersecurity services. Their penetration testing services simulate realistic cyberattacks to identify and address vulnerabilities in systems. Their SOC (Security Operations Centre) as a Service delivers 24/7 monitoring, threat detection, incident response, and compliance management, including SIEM, intrusion detection, vulnerability scanning, dark web

monitoring, and endpoint protection. The Offensive Cyber Initiative provides advanced vulnerability research, consultative services, and educational courses aimed at enhancing the cyber capabilities of government agencies and national programs. In the realm of application security, Tranchulas conducts thorough assessments of web and mobile applications, including vulnerability analysis, penetration testing, and source code reviews.

Their compliance services support ISO/IEC 27001 certification, internal audits, and the development of security policies and processes. Additionally, Tranchulas offers professional training courses in cybersecurity, featuring hands-on penetration testing, ethical hacking, and certifications like CISA and CISM.



Technogenics

Technogenics SMC PVT LTD is a leading cybersecurity and engineering solutions provider, recognized for its expertise in security product engineering, malware research, and managed services. Led by a seasoned leadership team with over 20 years of global experience in technology development, product design, and strategic management, Technogenics excels in delivering customized, high-performance solutions that meet client-specific needs. The company is dedicated to solving complex challenges, attracting top industry talent, and offering flexible, client-centric services across all stages of the Software Development Life Cycle (SDLC).

Combining in-depth knowledge of cybersecurity product development with a diverse range of services, Technogenics supports sectors including education, technology,

healthcare, retail, and travel. Their services include cybersecurity product development and research, with a focus on network, endpoint, and cloud security solutions.

Their web development services deliver intuitive, user-friendly experiences wrapped in visually engaging designs, while their mobile app development for Android and iOS emphasizes elegant, easy-to-use interfaces. Technogenics also specializes in data mining and analysis, offering custom models, automated data scraping, and actionable insights to drive business decisions. Additionally, they provide comprehensive SDLC support, from graphic design and coding to software research, quality assurance, deployment, and ongoing maintenance, ensuring robust and secure solutions for their clients.





Kualitatem

Kualitatem is a leading software quality assurance and information security company that partners with businesses to enhance the performance and security of their software. With a dedicated team of experts, Kualitatem focuses on ensuring flawless functionality and robust security, proactively identifying and addressing potential issues before they impact end-users.

This approach not only improves user experience and reduces bugs but also strengthens the brand's reputation. Understanding the critical role software plays in today's business landscape, Kualitatem offers a comprehensive range of services designed to mitigate risks, accelerate time-to-market, and increase user satisfaction. The company's expertise spans various sectors, including government, finance, healthcare, and mobile development, making them a versatile partner for diverse industry needs.



Kualitatem is distinguished by its credentials and industry recognition, including being one of the world's only TMMi Level 4 testing services provider, reflecting its dedication to excellence in software testing. The company has also been ranked among the Top 10 by Gartner for mobile application testing services.

In partnership with ThreatLocker, Kualitatem provides advanced cybersecurity solutions with a focus on zero-trust endpoint protection and real-time monitoring.

Kualitatem's influence in the industry is further solidified through participation in key events, such as the IDC Saudi Arabia CIO Summit in September 2024, demonstrating its commitment to innovation and leadership. These accolades and ongoing collaborations highlight Kualitatem's pivotal role in advancing software quality and cybersecurity.

Kualitatem offers a comprehensive suite of services designed to ensure the highest standards of software quality and security. Their Managed Testing services provide end-to-end

testing solutions that guarantee product excellence. Automation Testing involves a thorough evaluation of tools, processes, and best practices to streamline testing efforts. Performance Testing ensures that applications are scalable, responsive, and reliable under real-world conditions.

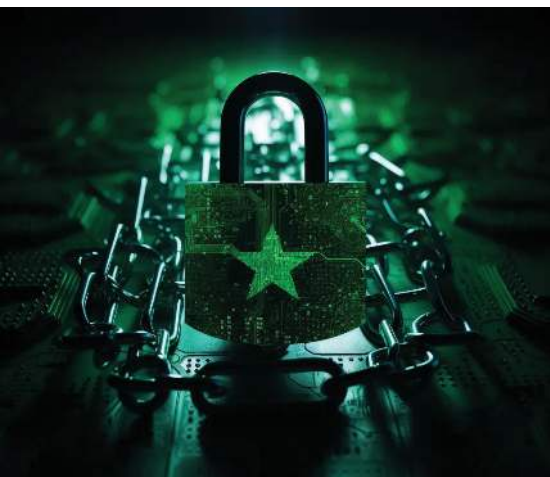
For mobile platforms, their Mobile App Testing delivers bug-free and user-friendly experiences. Security Code Reviews are conducted to identify and address critical security vulnerabilities within the code, strengthening overall application security. Additionally, Penetration Testing simulates real-world cyberattacks to enhance security measures and ensure compliance, helping organizations protect their digital assets effectively.



The team is experienced and well-versed in many different situations. Whenever our clients or external auditors came up with a compliance situation, the team was there to help.
- **Nayab Javed Meer, MENA Assistance**



Kualitatem had very structured approach on the penetration testing and defined the scope at the start of project with clear timelines which helped us align
- **Habeeb Ur Rahman, Merit Incentives LLC**





Global SNI

Global SNI Private Limited stands at the forefront of cybersecurity in Pakistan, specializing in Systems Networks Information (SNI). Renowned for their commitment to securing businesses against digital threats, they offer an extensive suite of solutions designed to safeguard data, networks, and digital assets, making them a trusted name in the industry.

Global SNI has built a stellar reputation through strategic collaborations with leading global firms, showcasing their capability to deliver world-class cybersecurity solutions. Their team of certified experts has successfully handled complex cybersecurity challenges, earning them recognition as a trusted partner in the field. Notable achievements include their partnership with Mobilink Microfinance Bank Limited (MABL), where deploying the Sophos Next Generation Firewall reduced cyber incidents by 40%, enhancing the bank's security posture.

At ICI Pakistan, implementing the innovative DigiDoc® document management system streamlined document handling processes, leading to a 30% increase in efficiency and a substantial reduction in operational risks. These success stories stand as testimonials to their

commitment to excellence and client satisfaction.

Operating around the clock, Global SNI's proactive threat management services leverage advanced technologies to detect, prevent, and respond to cybersecurity incidents. Their comprehensive offerings—ranging from malware detection and content delivery network protection to managed web application security—are meticulously tailored to meet the distinct needs of each client. With a focus on enhancing security standards, their ISO 27001 consulting services have guided numerous organizations toward achieving global compliance. The company's client-centric approach ensures that every solution is designed to align perfectly with the operational goals of their partners.

Global SNI provides an array of services including network security, threat detection and incident response, and managed protection services. They offer bespoke cybersecurity training programs and ISO 27001 certification consulting, with targeted training modules focusing on phishing awareness, data protection, and incident response strategies.

Primary Products

- ▶ Sophos Next Generation Firewall
- ▶ DigiDoc® document management system



Pligence

Pligence is a pioneering AI-based cybersecurity and privacy company dedicated to delivering intelligent and automated solutions that protect a diverse array of clients, including end users, IoT devices, enterprises, financial institutions, government organizations, and service providers. By focusing on state of the art threat intelligence, privacy protection, and real-time security measures, Pligence offers robust defenses against evolving cyber threats. Their flagship products, such as the Privacy Defender and Threat Intelligence Platform, exemplify their commitment to comprehensive digital security across various sectors. Pligence provides a range of advanced services designed to safeguard digital environments. Their cybersecurity and privacy solutions include cutting-edge technology to enhance real-time protection and threat detection capabilities. The Threat Intelligence Platform automates threat collection, transformation, and analysis, delivering actionable insights to prevent cyberattacks.

Their Privacy Defender Application ensures mobile privacy protection with advanced real-time security measures for consumers. Additionally, the Threat Protection System is tailored for enterprises, governments, and managed service providers, offering sophisticated threat identification and prevention. Pligence also excels in risk and compliance management and enterprise mobility and security solutions, ensuring comprehensive support for their clients' diverse needs.



Privacy Defender Application: A comprehensive mobile privacy protection suite with advanced threat detection and real-time defense for mobile users.

Threat Intelligence Platform: Provides machine intelligence-driven threat analysis, including the identification of threat vectors and actors, offering crucial insights to mitigate cyber risks.

Threat Protection System: Delivers real-time threat identification, prevention, and management solutions tailored for enterprises and government sectors.

GRCLens: A governance, risk, and compliance (GRC) platform offering real-time risk visualization and compliance management aligned with frameworks like ISO, NIST, and PCI.

Pligence Connect: An enterprise mobility and security solution integrating multisite VPN, threat management, and mobile device security, tailored for various corporate environments.

Managed Threat Intelligence and Assessment Platform (MANTIS): Offers real-time monitoring, advisories, and vulnerability management services through advanced threat analysis.



wateen
Wateren Solutions (Pvt.) Limited

Wateren Telecom is one of Pakistan's largest and fastest-growing fiber network infrastructure companies, supporting enterprises in their digital transformation journeys. Focusing on robust cybersecurity measures, Wateren integrates the NIST Cybersecurity Framework to protect its systems against cyber threats and enhance its cybersecurity capabilities.

Wateren Telecom has formed strategic collaborations, particularly with Huawei Technologies Pakistan. A Memorandum of Understanding (MoU) signed at Huawei's Headquarters in Dongguan, China, outlines an alliance that enhances Wateren's service offerings. This partnership allows Wateren to deploy advanced infrastructure in its data centers, supporting services like managed Wi-Fi, managed SD-WAN, and managed surveillance services. These developments aim to drive digital transformation in Pakistan, benefiting businesses and customers.



Wateren Telecom has the largest market share in tower fiberization across Pakistan and hosts the country's most extensive team of Cisco Certified Experts as a Cisco Gold partner. Its cybersecurity strategy, based on the NIST Cybersecurity Framework, uses tools like Endpoint Detection & Response (EDR), Security Information & Event Management (SIEM), and Data Loss Prevention (DLP) across devices, applications, networks, data, and users to defend against cyber threats.

Wateren's primary services include Managed Security Services, Cloud Services, and Business IT Solutions, alongside specialized offerings such as Incident Response & Recovery, Threat Intelligence, Extended Detection and Response (XDR), and Multi-Factor Authentication (MFA).



Inotech Solution Pvt Ltd

Inotech Solutions Pvt Ltd is an IT system integration, professional services, and software company operating in South Asia, providing comprehensive support for enterprise systems across various sectors. With a decade of industry experience, Inotech has developed a team of technical engineers, developers, and project managers who deliver tailored IT solutions that facilitate business growth and streamline processes. Their services encompass datacenter management, software development, ERP, HMS, cybersecurity, and GIS, catering to government, defense, semi-government, and private clients.

Inotech Solutions has launched over 240 projects, served 500 clients, and continues to manage 80 ongoing projects. Their portfolio includes the deployment of 211 websites and a wide array of solutions, such as Oracle EBS implementation, business intelligence, and cybersecurity services. The company's approach focuses on meeting the IT needs of diverse industries, ensuring reliable support and tailored solutions for each client.

Inotech's cybersecurity services emphasize protecting computer systems, networks, and data from unauthorized access, data breaches, and malicious attacks. Their cybersecurity strategy includes risk

assessment and management, where organizations conduct evaluations to identify vulnerabilities, threats, and potential risks. They then develop management strategies to mitigate these risks. Inotech's network security services involve safeguarding computer networks through firewalls, intrusion detection and prevention systems, secure configurations, and encryption to secure communications. Their endpoint security solutions protect individual devices, such as laptops and mobile devices, through antivirus software, endpoint protection tools, device encryption, and strong password policies.

Inotech Solutions also offers specialized products, including CCTV Surveillance & Security Systems, designed for medium to enterprise-sized deployments with hundreds of IP-based cameras. These systems enable customers to monitor multiple locations from a single Security Operations Center (SOC). They also provide Access Control & Perimeter Security systems, which include video analytics, video management, sensors, and physical security measures like fences, gates, and barriers to ensure a secure environment.

Primary Products

- ▶ **CCTV Surveillance & Security System**
- ▶ **Access Control & Perimeter Security System**



Sparkeye Technologies

Sparkeye Technologies is an IT company specializing in custom software development and security solutions, including IT consulting, software engineering, and product development. The company provides solutions aimed at automating business processes, enhancing employee efficiency, and reducing costs for both small businesses and large enterprises. Sparkeye's security products are designed to offer digital protection, maintain user privacy, secure internet freedom, and defend against online threats.

With operations in 135 countries and serving over 1.2 million users, Sparkeye Technologies has invested 71,000 hours into developing its security solutions. These services are designed to protect users from hackers, enable anonymous browsing, and secure internet connections with data encryption, merging technology with human oversight to offer security for digital devices. Their clients include organizations like CNBC, Mashable, Boston Globe, Fox 28, and ABC 2.

Sparkeye's offerings include protection from hackers, ensuring the security of users' online activities. The company provides tools for anonymous surfing, preventing third-party monitoring and tracking. Parental control software helps shield children from online dangers such as cyberbullying, sexual predators, and inappropriate content, while allowing parents to monitor and manage their



children's online activities remotely. Sparkeye Technologies also offers smart home DNS services that protect all connected digital devices, securing networks and maintaining data encryption. Sparkeye Technologies offers a range of security products designed to protect digital devices and ensure safe internet use.

Their flagship product, VantageMDM, provides comprehensive protection for all digital devices within both home and office environments, safeguarding against cyber threats. SecureTeen is a parental control solution available for iOS, Android, and Windows, allowing parents to monitor and manage their children's online activities, providing a secure digital environment for younger users. FalcoVPN is Sparkeye's VPN app, offering users security, privacy, and unrestricted internet access by masking their online presence and enabling anonymous browsing. These products collectively cater to the diverse security needs of individuals, families, and businesses.

Primary Products

- ▶ VantageMDM ▶ SecureTeen
- ▶ FalcoVPN



Secisys

Securing Information System (Pvt) Ltd. (SECISYS) is an information security company focused on protecting digital assets and sensitive information through tailored cybersecurity solutions. Specializing in ISO 27001, 27017, and GDPR certification processes. SECISYS's primary services include Vulnerability Assessment & Penetration Testing, Information Security Management, GDPR Compliance, Cloud Services, Information System Auditing, Managed Services, Infrastructure Development, and Security Code Review. The company's team of experts assesses vulnerabilities across applications, cloud systems, networks, and infrastructure,

identifying and mitigating risks to keep businesses secure from cyber threats.

With over 20 years of consulting experience, SECISYS has secured more than 70 cybersecurity projects and served over 40 clients across various industries. The company's core services include Vulnerability Assessment & Penetration Testing, Information Security Management Systems (ISMS) implementation (ISO: 27001), GDPR compliance, and cloud security solutions. SECISYS has also trained over 100 students, equipping them with the necessary skills to navigate the evolving cybersecurity landscape.

SECISYS emphasizes a customized approach to cybersecurity, ensuring that solutions are tailored to the specific needs of each client. Its service portfolio encompasses risk assessments, security policy development, managed services, and information system auditing. By offering comprehensive security solutions at competitive prices, SECISYS assists organizations in safeguarding their critical assets. With over 3,000 nodes and applications assessed, SECISYS plays a significant role in securing digital environments, helping businesses protect data, maintain trust, and secure their operations.





Catalytic Consulting

Catalytic Consulting is a firm specializing in advanced cybersecurity solutions, providing businesses with the tools to protect their digital assets and maintain operational integrity. With a focus on proactive security measures, Catalytic Consulting offers a range of services, including risk assessments, penetration testing, incident response, and managed security services.

Catalytic Consulting has a proven track record of implementing key cybersecurity and process improvement initiatives across various industries. Notable achievements include the implementation of ISMS 27001 for the Federal Board of Revenue (FBR) across Pakistan and the enhancement of CMMI Level 3 practices at Telenor by incorporating Agile Methodology. The firm has also delivered multiple CMMI Level 2, ISO 27001, and ISO 20000 projects in collaboration with the Pakistan Software Export Board (PSEB).

Catalytic Consulting supported NADRA in achieving and maintaining CMMI Level III certification, streamlining its Technology, Project, and Quality Management domains to enhance business process efficiency, organizational growth, and synergy. Additionally, Catalytic Consulting has executed high-profile business process reengineering projects for key ministries in the Kingdom of Saudi



"We strongly recommend our prestigious service provider "Catalytic" who are equipped with skilful people having strong background of software engineering, management and quality standards."

- Manager Quality, iApps Consultancy Department, Interactive Group

"Achievement of CMMI Level III certification has immensely enriched the business process dynamism of NADRA. The triad of Technology, Project and Quality Management domains at NADRA has been extensively streamlined for synergy and optimal business solutions. Ongoing CMMI Level III compliance in NADRA coupled with enhanced emphasis on agility, is appropriately bound for organizational growth and success through effective attainment of organizational objectives."

As the certification appraisals and continued support was provided by Catalytic Consultants, the appraisal company has also contributed to standardization and synergy in NADRA."

- Director General CQM & Chairperson AHC, NADRA



Arabia (KSA) to meet international standards.

The firm's services extend beyond external threat protection, addressing internal security measures through employee training and awareness programs. These initiatives ensure that teams are equipped to identify and respond to potential threats effectively.

Catalytic Consulting's managed security services provide continuous monitoring and support, reinforcing clients' security posture around the clock. With a history of 7 successful CMMI appraisals, 150 satisfied clients, and 1,600+ trained students, Catalytic Consulting continues to deliver secure and compliant solutions that meet the evolving needs of modern businesses.



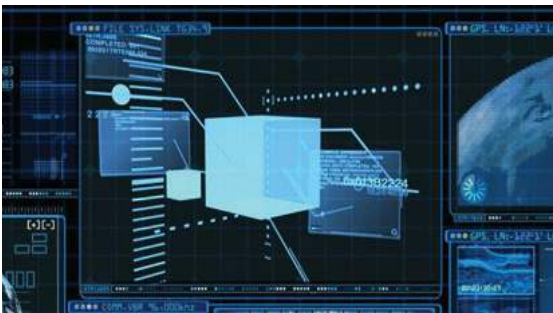
We strongly recommend our prestigious service provider "Catalytic" who are equipped with skilful people having strong background of software engineering, management and quality standards.

- Manager Quality, iApps Consultancy Department, Interactive Group



PakCerte

Founded in 2000 as Pakistan's first information security solutions provider, Pakistan Computer Emergency Response Team (PakCERT) has been involved in responding to security incidents, identifying intruder activity trends, and working with global security agencies to address cybersecurity challenges. The team analyzes product vulnerabilities, issues advisories and alerts on various threats, and coordinates with international CERTs to address security issues. PakCERT also provides seminars and training to help organizations understand and counter evolving cyber threats.



PakCERT is a cybersecurity entity that provides security services and training to public, government, and private sectors across the nation. PakCERT focuses on building secure infrastructures through education, advanced technology, and expertise to ensure the confidentiality and integrity of clients' information assets.



PakCERT provides services such as Information Security Services, Vulnerability Assessment & Penetration Testing, Cyber Security Operations Center (CSOC), Digital Forensic Analysis, ISO 27001 Compliance, Development of Information Security Policies, Business Continuity and Disaster Recovery Planning, and Malware Reverse Engineering.

PakCERT's experts hold certifications such as CISSP, CEH, CPTS, ITIL, and COBIT, and contribute to national and international media, conferences, and security programs. Among their key achievements is the discovery of a critical vulnerability in Microsoft .NET Passport services, which had a global impact.



Ebryx

Ebryx is a global leader in cybersecurity, providing comprehensive services to secure and empower organizations worldwide. With over a decade of experience, the company specializes in 360° cybersecurity, security product engineering, GRC services, and custom software development. As a CMMI Level 3 and ISO 27001 certified company, Ebryx ensures its solutions meet the highest quality and security standards, serving a diverse clientele across North America, EMEA, and APAC regions.

Ebryx's service portfolio includes security consulting, detection and response services, application security, and Zero Trust solutions like Invisily, a proprietary Zero Trust Network Access technology designed to protect critical infrastructure. The company's innovative approach is bolstered by its dedicated R&D wing, which focuses on developing cutting-edge solutions to counter advanced cyber threats.

The company serves a wide range of clients, including renowned names like EA Sports FIFA, Coca-Cola, Verizon, and Randstad, alongside SMEs, governments, and public sector organizations. Ebryx has engaged in over 1,000 successful security projects, filed over five cybersecurity patents on behalf of its customers, and dedicated more than a million man-hours to security R&D.



With a commitment to protecting its clients from evolving cyber threats, Ebryx stands as a trusted partner for SMBs, Fortune 500 companies, and government bodies seeking robust cybersecurity solutions.

Invisily is a comprehensive Zero Trust Network Access (ZTNA) platform designed to provide seamless, secure connections without the technical complexities of traditional solutions. It supports diverse deployment scenarios and offers advanced features like device inventory and posture checks, agentless and embeddable connectivity, and integrated Data Loss Prevention (DLP) controls. Invisily's flexible architecture and Ebryx's extensive expertise in managed services enable organizations to adopt Zero Trust security effortlessly, protecting digital assets with a cost-effective and adaptable approach.

Primary Products

► Invisily

rewterz

Rewterz

Rewterz is a cybersecurity company focused on delivering advanced security solutions to protect businesses from the dynamic threat landscape. Specializing in threat intelligence, managed security services, and incident response, Rewterz helps organizations secure their digital assets with tailored approaches that address sector-specific challenges. Rewterz provides a broad range of services categorized into Assess, Transform, Train, and Respond modules. These include Compromise Assessment, APT Assessment, Penetration Testing, SOC Consultancy, SOC Maturity Assessment, Security Awareness Training, Incident Analysis, and Response.



Rewterz has over 16 years of experience in cybersecurity, serving more than 200 customers globally and processing over 10 million security events daily. Key clients include Bank Alfalah, Qatar University, Pakistan Stock Exchange Limited, and NIFT.

Rewterz has been recognized in the cybersecurity industry for its significant contributions and achievements. It was listed among the Top 250 MSSPs by MSSP Alert in 2022 and was a Bronze Winner in the GLOBE Awards for Cybersecurity in 2024. In 2023, Rewterz was featured in the KuppingerCole Market Compass Report for SOCAaaS in the UAE and received the Outstanding Performance of the Year award in Pakistan for FY23. Additional accolades include the Partner Excellence Award for Cyber Security Strategy from Starlink in 2019 and the Best New Partner Award from IBM in 2016.

Rewterz protects over 1,000 organizations worldwide, maintaining a 99% client retention rate, which reflects its commitment to reliable and effective security solutions. The company has detected and neutralized more than 10 million cyber threats, mitigating up to 80% of potential damages. Rewterz's incident

response time is 50% faster than industry standards, setting a high benchmark in cybersecurity operations. The leadership team, equipped with extensive industry experience, drives Rewterz's mission to deliver comprehensive protection and empower clients to secure their digital environments confidently.

Central to Rewterz's offerings is its XDR platform, an integrated solution combining Next Generation SIEM, SOAR, and EDR technologies, supplemented by real-time threat intelligence and 24/7 monitoring by security analysts. The platform enhances visibility across the security landscape, streamlines response actions, and integrates with over 170 security tools, enabling 750+ automated actions. Rewterz XDR provides an all-in-one dashboard, simplifying the security management process and allowing organizations to address threats swiftly and effectively.



Primary Products

- ▶ XDR Platform





Di8it by Digit Labs is a specialized cybersecurity consultancy offering a comprehensive suite of offensive, defensive, advisory, and Managed Security Services. Di8it adopts a tailored approach to each client's unique needs, addressing diverse cybersecurity challenges and leveraging its expertise to protect businesses against evolving cyber threats. As trusted system integrators, Di8it partners with leading OEMs such as LogRhythm, BeyondTrust, AlgoSec, and IBM Security, providing deep insights into security vulnerabilities and bespoke solutions to fortify digital environments.

Di8it's Offensive Security services focus on proactive measures to identify and mitigate vulnerabilities. The company offers Web and Mobile

App Penetration Testing, Network Penetration Testing, Red Team Assessments, Social Engineering Assessments, and Breach and Attack Simulations, all designed to expose weaknesses and enhance an organization's security posture.

The Advisory Services at Di8it enhance clients' security strategies by providing Network Architecture Reviews, System Hardening & Configuration, Risk and Compliance Assessments, and Cyber Security Maturity Evaluations. These services are crafted to ensure that organizations are not only protected against current threats but also prepared for future challenges.

Di8it's Defensive Security offerings are centered around detecting and mitigating cyber threats. Services such

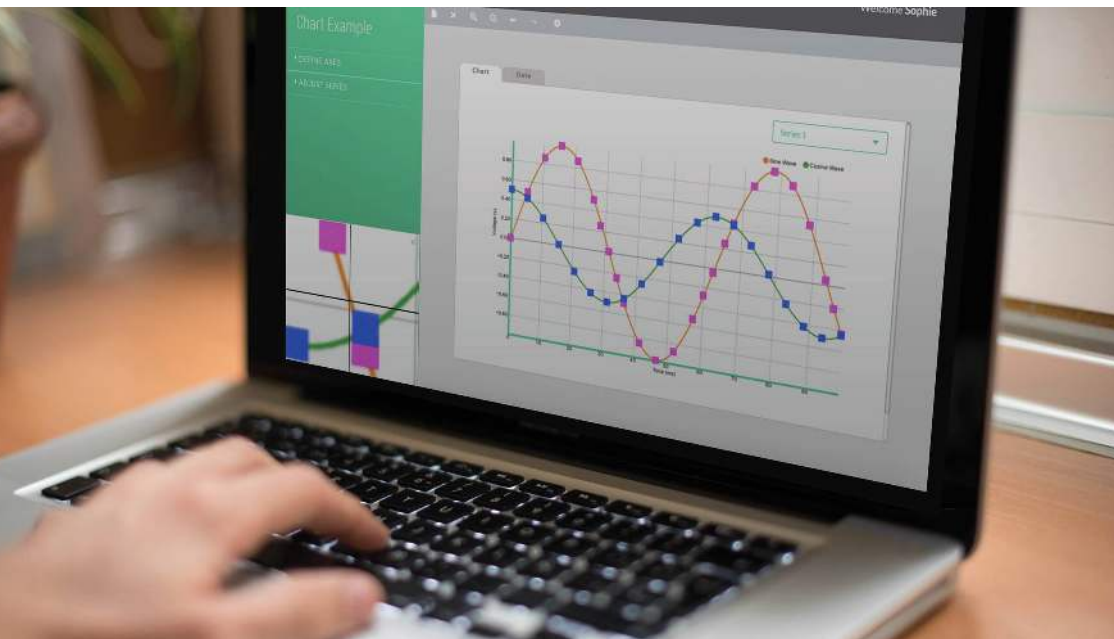


as Compromise Assessments and other defensive protocols help safeguard against unauthorized access and potential data breaches, offering organizations peace of mind in a constantly evolving threat landscape.

In addition to its service offerings, Di8it provides various security solutions, including Network and Web App Vulnerability Management, Database Encryption, Database Security Monitoring, Security Orchestration, Automation, and Response (SOAR), Security Analytics, Privileged Access Management, Endpoint Privilege Management, Server Security, and Access Control. These solutions are designed to deliver comprehensive protection across all aspects of an organization's digital infrastructure.

Di8it serves a diverse range of clients across multiple sectors, including financial institutions, healthcare, and logistics. Notable clients include JS Bank, Meezan Bank, Khaadi, Bank Alfalah, Bank Al Habib, EFU Life Insurance, Allied Bank, Zarai Taraqati Bank Limited, Aga Khan Hospital, Adamjee Insurance, TCS, and United Bank Limited, reflecting Di8it's capability to cater to large-scale and varied security needs.

A key feature of Di8it's service delivery is its XDR (Extended Detection and Response) platform, which integrates with over 170 security tools and enables more than 750 automated actions. The platform provides an all-in-one dashboard for end-to-end visibility and control, connecting an organization's entire security ecosystem—including networks, endpoints, and data centers—with Di8it's cloud-based solutions through APIs or on-premises collectors. This seamless integration enhances the ability of security teams to detect, analyze, and respond to threats efficiently.





ACCESS GROUP Access Group

Access Group (AG) is a leading provider of advanced technology solutions with a strong emphasis on information security and cybersecurity. With over 25 years of experience, AG has established itself as a key player in the market, particularly through its innovative point-of-sale (POS) solutions and a comprehensive POS transaction processing network across Pakistan. The company's success is driven by its partnerships with global technology leaders and a dedicated team of over 170 professionals.



cybersecurity domains, including data privacy and protection, access management, patch management, and threat intelligence. The company offers a wide range of solutions such as Security Incident and Event Management (SIEM),



Security Orchestration, Automation and Response (SOAR), and Extended Detection and Response (XDR). AG is committed to meeting regulatory requirements across industries like healthcare, banking, insurance, and retail, providing robust protection and prevention strategies to safeguard business environments.

The company's information security client base includes prominent organizations such as Atlas Honda, Covalent, Faysal Bank, and the Central Depository Company. Access Group is dedicated to fortifying systems, delivering professional services, and offering comprehensive training and 24/7 support to ensure resilience against evolving cyber threats.



We were looking for a strategic technology partner that was strong on the products side and was strong enough to cover the security landscape as much as possible, so that if in the future, we were opting for fraud/identity management or any other security solution, we would have those options available with Access Group.

Syed Asif Shah
(CIO, Central Depository Company of Pakistan Limited).



SecureBeans specializes in providing a comprehensive suite of information security solutions tailored to meet the specific needs of each client. The company's expert team, which includes certified professionals with credentials such as CISSP, CEH, CRISC, and CCISO, delivers advanced security solutions to address unique cybersecurity challenges. SecureBeans excels in regulatory compliance and cyber threat protection through detailed vulnerability assessments and penetration testing (VAPT). Their services simplify complex regulations and assist clients in achieving important certifications like ISO27001, HIPAA, SOC2, and GDPR.

The company's business model is built on a straightforward approach: consult, develop, and deliver top-notch information security solutions to effectively manage and mitigate risk. SecureBeans has a proven track record of success, with a distinguished clientele including Marriott, Shell, Bureau Veritas, AT&T, Brookes and many others. They offer specialized services in cyber security, forensics, and governance, ensuring robust protection and adherence to best practices across various industries.

SecureBeans's client base reflects its reputation for excellence, with notable clients such as Atlas Honda, Covalent, Faysal Bank, and Central Depository



Company. With nearly 1000 satisfied clients and 500 completed projects, and a dedicated team of 49 employees, SecureBeans is well-positioned to continue its leadership in the cybersecurity field. The company's commitment to high-quality service is evident in its client testimonials and successful project outcomes.



The main reason to select SecureBeans turned out to be their quality customer service and their track record in the financial industry. As long as I require penetration testing, I will be a client of SecureBeans.

-Sarwar Khan, Arif Habib Limited



I decided to go with SecureBeans for my penetration testing needs as it was the only vendor that performed manual testing in the same vein as actual hackers out on the internet as opposed to automated scanning tools. Most vendors I found offered automated services only, while I was also looking for manual testing.

-John Stewart, International Client



Priv0 is a cybersecurity firm specializing in defensive and offensive strategies to help organizations enhance their cyber readiness. Their services include advisory and consulting, endpoint detection and response, vulnerability management, and virtual CISO roles.

The Cyber Defensive services focus on safeguarding clients against cyber attacks through preventative controls, attack detection, and response capabilities. These services align with international standards and compliance requirements, such as ISO 27001, NIST, and PCI DSS, ensuring comprehensive security coverage. On the offensive side, Priv0 employs adversarial tactics to simulate real-world threats, identify vulnerabilities, and strengthen security postures, aiming to close gaps before they can be exploited.

Priv0 provides tailored solutions aligned with international standards like ISO 27001, NIST, and PCI DSS, aiming to protect businesses from evolving cyber threats. The firm emphasizes a proactive approach to identifying and mitigating vulnerabilities, ensuring compliance and resilience in a complex digital landscape. Priv0 has built partnerships with other cybersecurity companies and collaborates with regional Security



Operations Centers (SOCs) and Cyber Security Incident Response Teams (CSIRTs) to enhance its service offerings.

Priv0's expertise extends to building cyber capabilities that support digital transformation, addressing complex challenges, and mitigating inefficiencies within cybersecurity programs.

In addition to advisory services, Priv0 provides Endpoint Detection and Response (EDR) and Vulnerability Management solutions. EDR services include active threat response, guided investigations, and endpoint isolation, allowing organizations to contain and recover from incidents swiftly, including ransomware rollback capabilities. The Vulnerability Management service focuses on reducing the cyber attack surface by discovering, prioritizing, assessing, and remediating security flaws, supporting businesses in managing threats efficiently and effectively.



ThingzEye

ThingzEye, is a cybersecurity company specializing in comprehensive security for IoT networks. Originating from the IoT Research and Innovation Lab (IRIL) at UET Lahore and funded by the National Center for Cyber Security (NCCS), ThingzEye leverages advanced threat modeling, penetration testing, and embedded systems security to protect against IoT and emerging threats. Comprising senior PhDs, researchers, security consultants, embedded engineers, and software developers, the lab excels in replicating real-world hacker techniques in controlled environments.

This expertise enables the team to identify overlooked vulnerabilities and exploit chains that may pose significant risks. With extensive experience in offensive cybersecurity, they hold industry certifications, bug bounty awards, and actively contribute



to the penetration testing community. The company provides customized solutions through services like static and dynamic vulnerability assessments, security architecture compliance, and training workshops. With expertise in identifying and mitigating vulnerabilities in IoT hardware, firmware, and applications, ThingzEye supports a range of security needs from small smart home devices to large enterprise networks, aiming to simplify cybersecurity through scalable, user-friendly solutions.

ThingzEye offers a range of cybersecurity products tailored to various environments. Firewall Lite is designed for home and small office use, providing comprehensive protection for internet-connected devices. The Enterprise Firewall is a next-generation solution that delivers advanced threat protection for businesses with diverse security needs.

For industrial settings, the Industrial Firewall secures critical infrastructure. The Analyzer is a powerful tool for both static and dynamic analysis of device firmware, identifying vulnerabilities in IoT devices and systems without requiring physical access.

Primary Products

- ▶ Enterprise Firewall
- ▶ Firewall Lite
- ▶ Industrial Firewall
- ▶ Analyzer Box



SlashNext

SlashNext is a leading cybersecurity company renowned for its advanced threat detection and protection solutions. Specializing in email, SMS, mobile, and web messaging security, SlashNext utilizes cutting-edge AI technology to deliver comprehensive and real-time defenses against a wide array of cyber threats. The company's proprietary technologies, including HumanAI, ProactiveAI, and Fusion, enable it to predict and counter sophisticated attacks such as Business Email Compromise (BEC), QR-code phishing, SMiShing, and zero-hour social engineering threats.

With a 99.99% detection rate and the ability to identify approximately 1 million attacks per week, SlashNext's platform significantly outperforms traditional security solutions and first-generation AI technologies. Its advanced capabilities extend across various communication channels, including Microsoft 365, Slack, Zoom, and Teams, providing robust protection against the latest threat vectors. The company's cloud-native architecture ensures rapid deployment and seamless integration with existing systems, offering superior defense without additional operational overhead.

SlashNext is recognized for its exceptional service and support, consistently ranking higher than its

competitors in various Gartner reviews. Trusted by global enterprises, SlashNext's solutions are designed to address emerging security challenges and deliver unparalleled protection against evolving cyber threats.

SlashNext has been recognized for its excellence in cybersecurity, being named a finalist in the Best Secure Messaging Solution category at the 2024 SC Awards. The company also achieved significant wins at the 2024 Globee® Awards, earning Gold for Best Email Security and Management and Silver for Company of the Year in both Artificial Intelligence Security and Mobile Security. In addition to these accolades, SlashNext has partnered with Microsoft to enhance protection for Microsoft 365 customers against advanced phishing attacks.



BugsLife

BugsLife is a cybersecurity firm that specializes in comprehensive security testing for web, mobile applications, and infrastructure. Renowned for its expert security analysts, BugsLife delivers customized solutions designed to protect enterprises and business organizations from a wide range of cyber threats. The firm's core services include cybersecurity consulting, penetration testing, vulnerability assessment, and mobile and web application security.

The company offers several key services: Cybersecurity Consulting provides strategic advice to bolster information security; Penetration Testing evaluates network defenses through both external and internal assessments to uncover vulnerabilities; Mobile Security involves security evaluations for iOS and Android platforms, including

both static and dynamic testing; Vulnerability Assessment focuses on identifying and analyzing security weaknesses in systems and applications; Web Application Security involves testing and securing web applications against potential threats and exploits; and Infrastructure Security ensures the protection of network infrastructure from various attack vectors.

BugsLife employs methodologies that adhere to NIST and OWASP guidelines to ensure rigorous and reliable testing. The firm serves a diverse range of clients, from local businesses to large corporations, emphasizing ethical practices and high standards of security. Its approach is designed to safeguard digital information across sectors such as finance, economics, medical, and defense.



Growth Arbor

Growth Arbor is a leading advisory firm dedicated to enhancing digital infrastructure and protecting organizations from emerging cyber threats. The firm provides a comprehensive suite of services aimed at supporting businesses throughout their digital transformation journeys while ensuring their technology environments are secure and efficient.

These services include technology and platform advisory, cyber security, and managed services, all tailored to meet the specific needs of various sectors such as banking, capital markets, manufacturing, healthcare, and higher education.

The firm's technology and platform advisory services cover technology architecture, platform and product selection, enterprise architecture, as well as helping businesses make informed decisions and optimize their IT environments. In the domain of cyber security, Growth Arbor focuses on technology resilience with solutions including security architecture,

governance, risk and compliance, and security assessments. Their managed services offer continuous support and management of IT operations, cloud migrations, and digital infrastructure, enhancing operational efficiency and business value.

Additionally, Growth Arbor provides specialized training programs aimed at equipping teams with essential skills for cloud transformation, big data analytics, and cyber security. The firm's approach emphasizes aligning technology with business objectives, allowing clients to concentrate on growth while Growth Arbor manages their technological requirements.



KAZ Technologies

KAZ Technologies is an IT services company specializing in comprehensive cybersecurity solutions designed to protect computer systems from theft, damage, and unauthorized access. The company focuses on safeguarding hardware, software, and electronic data, ensuring that organizations maintain robust information security frameworks. With expertise across various sectors, KAZ Technologies provides tailored solutions that enable businesses to navigate the complexities of cybersecurity effectively. Its offerings include proactive threat detection, advanced network security measures, and comprehensive data protection. The company excels in delivering customized security audits, incident response, and compliance services. Additionally, KAZ Technologies provides specialized Vulnerability Assessment and Penetration Testing (VAPT) and Security Operations Center (SOC) services.



Key services provided by KAZ Technologies encompass Threat Detection and Prevention, Network Security, Data Encryption and Protection, Security Audits and Compliance, Incident Response and Recovery, Vulnerability Assessment and Penetration Testing (VAPT), Identity and Access Management (IAM), and Security Operations Center (SOC) Services. By offering these services, KAZ Technologies addresses a wide range of cybersecurity needs, helping organizations enhance their security posture and resilience against cyber threats.





Aegispeak Pvt. Ltd.

Aegispeak Pvt. Ltd. is a software development company specializing in high-quality IT solutions with a strong emphasis on cybersecurity. The company offers a wide range of services including Security Advisory Services, Incident Response Services, Cyber Security Consulting, and IT Services. Aegispeak's expertise lies in delivering secure and customized IT solutions for both single and multi-operating system environments, enabling clients to achieve their technological goals with enhanced security.

The company has established itself through strategic partnerships and collaborations, leveraging these alliances to provide solutions that are more effective than those achievable independently. Aegispeak's consulting services include tailored security strategies and compliance solutions, supported by 24/7 access to dedicated cybersecurity engineers. This approach ensures that businesses receive proactive and reactive support to handle advanced threats and security breaches effectively.

Aegispeak's focus on integrating security into business operations is a key differentiator. Their Security Advisory Services help organizations prioritize security projects, manage risks, and meet compliance standards.



The company also provides Incident Response Services designed to address complex detection challenges and evolving threats, ensuring comprehensive preparation and recovery strategies for security breaches.

In addition to cybersecurity, Aegispeak offers a broad range of IT services, including Security Application Development, E-commerce systems, Client-Server Applications, Web and Mobile Development, Quality Assurance, Geographic Information Systems, and Enterprise Application Integration. The company adheres to industry-standard process models such as Spiral, Waterfall, and RAD to ensure projects are delivered on time and within budget.

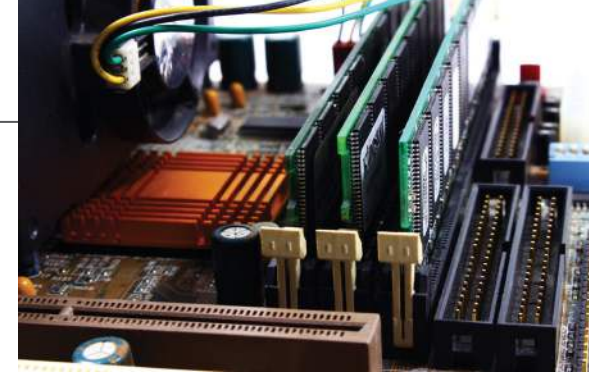
Notable clients of Aegispeak include Barbican LLC (USA), SecureNcrypt (USA), and Mato Grosso Ltd (Singapore), reflecting the company's global reach and capability to handle diverse IT and security needs.



Cybercom Private Limited

Cybercom Private Limited, founded in 2016, is a leading provider of IT and telecom infrastructure solutions specializing in network, data, and cyber security services. The company offers a comprehensive range of products and services, leveraging strategic partnerships with over 105 global IT manufacturers and market leaders. Cybercom's approach combines independent consulting with a focus on recommending reliable, long-term technologies, catering to the specific needs of diverse industries including finance, healthcare, government, and telecommunications.

Cybercom's service offerings are built on its expertise in Data Network Solutions, Security and Surveillance, Cyber Security, and Telecom Infrastructure. The company has successfully delivered over 1,000 projects, showcasing its ability to implement everything from Layer 2/3 manageable switches and routers to advanced surveillance systems. Cybercom's network security services include implementing secure data environments, configuring firewalls, and maintaining robust data protection protocols. Its comprehensive cyber security solutions address the growing need for safeguarding sensitive information against emerging threats.



In the realm of Security and Surveillance, Cybercom provides specialist design, installation, commissioning, project management, and maintenance services for businesses seeking to enhance their security posture. The company's telecom infrastructure solutions include IT and telecom hardware and software, ensuring seamless communication networks that are both resilient and scalable. These services are supported by a dedicated team of certified professionals who ensure that each deployment meets rigorous industry standards.

The company's clientele spans various sectors, including enterprise-level organizations, government institutions, and educational entities. Cybercom's ability to provide turnkey solutions, from consulting and design to implementation and maintenance, has solidified its position as a reliable partner in the technology landscape.

With a commitment to fostering growth both locally and internationally, Cybercom actively engages in community development initiatives and focuses on strategic expansion. Its approach to integrating technology, customer care, and innovation continues to drive the company forward, ensuring that it remains at the forefront of the IT and telecom sectors.



Commtel

Commtel Systems, established in 2001 and headquartered in Pakistan, is a leading provider of cybersecurity and technology solutions, specializing in Managed Security Services, Security Consulting, Data Center Solutions, and Collaboration Solutions. With over two decades of experience, Commtel delivers a wide range of services tailored to the needs of diverse industries. The company is recognized for its commitment to enhancing business operations through innovative technology solutions and cybersecurity measures.

Commtel's services are underpinned by strategic partnerships with top-tier technology providers, enabling the delivery of cutting-edge solutions from small-scale implementations to global



integrated systems. Commtel's Managed Security Services provide organizations with outsourced monitoring and management of security devices, including Managed Vulnerability Assessments, Security Controls, Endpoint Detection & Response (EDR), and 24/7 Security Operations Center (SOC) monitoring. These services help businesses strengthen their security posture, reduce risks, and focus on their core operations while relying on expert support for their security needs.

Commtel's Security Consulting Services are designed to help organizations establish formal security strategies, meet compliance requirements, and address emerging threats. These services include strategy and risk assessment, threat intelligence, predictive analytics, and

identity and access management. By leveraging a team of certified security professionals, Commtel assists clients in identifying vulnerabilities, prioritizing security initiatives, and implementing effective risk management controls.

Commtel's Data Center Solutions and Collaboration Services further enhance its portfolio, supporting businesses in optimizing their IT infrastructure, enhancing communication, and maintaining high levels of performance and reliability. The company provides end-to-end data center solutions, including design, deployment, and maintenance, ensuring secure and efficient data management.

Additionally, Commtel's collaboration solutions improve workplace productivity through advanced communication tools tailored to specific business needs.

With a strong focus on client satisfaction and a track record of delivering high-quality technology solutions, Commtel serves a diverse client base, including enterprises across various sectors such as finance, healthcare, manufacturing, and telecommunications. The company's dedication to continuous improvement and quality management systems ensures that clients receive reliable and state-of-the-art services that align with their evolving business requirements.



Saad Alam - Director Commtel receives the Impact Partner of the Year Award 2024 by Abdellah Nejari - Managing Director Gulf Region (Cisco), along with Ossama Eldeeb - Director of Technical Sales Gulf Region (Cisco), Priya Limaye - Partner Organisation Lead Gulf Region (Cisco), Kashif ul Haque - Country GM Pakistan (Cisco) and Anas Jarrar - Partner Account Manager (Cisco).



Software Productivity Strategists, Inc.

Software Productivity Strategists (SPS), Inc. is an IT solutions provider offering a range of services to enhance organizational security and efficiency. SPS provides dedicated security management experts to augment security staff and enhance safeguards. Their services include network visibility operations, design, and implementation services, Keysight network training, ATM security, security policy management as a service, and implementation of ISO/IEC 27001 and the SOC 2 compliance framework.

SPS provides additional services to reduce IT spend and enhance infrastructure resilience by leveraging the cloud. SPS utilizes generative AI and analytics to provide actionable insights to automate and improve execution of corporate processes.

Primary Products

- ▶ **Digital Trust (User Security, Data Security, Mobile Device Management)**
- ▶ **Threat Management (Cybersecurity Program, SIEM systems, Application Security, Network Security)**
- ▶ **Keysight (Professional Services, Help Desk Services, Security Operations)**
- ▶ **Virtual Platform Training**
- ▶ **Internet of Things**
- ▶ **DevOps and Migration Services**
- ▶ **Business Process Modelling & Automation**
- ▶ **Generative AI**
- ▶ **Data Analytics**
- ▶ **Event services**
- ▶ **SAP Security**



Their primary differentiator is this wide-ranging capability to integrate cybersecurity, AI development, cloud/infrastructure services, personnel training, and event management.

SPS has a track record of almost 25 years. They also provide services in a host of verticals including public sector services, healthcare, manufacturing, retail, energy, and telecommunications. They are particularly prominent for its strong industry-academia partnerships. They maintain a robust internship program and an active series of special interest groups (SIGs) focusing on cutting-edge technologies.



Kinverg

Kinverg is a technology and innovation consulting firm dedicated to driving growth for micro, small, and medium-sized enterprises, particularly technology-driven startups. Their expertise spans critical areas such as cybersecurity compliance, data privacy, AI strategy development, and digital transformation solutions.

Kinverg was one of the earliest consultancy firms helping US companies achieve the Cybersecurity Maturity Model Certification (CMMC), a compliance process enabling contractors to meet US Department of Defense security standards. Kinverg services also include services relating to SOC2, HIPAA, and ISO 27001 standards. They also provide AI strategy services and training and certification for Six Sigma and Crispa.ai.

Kinverg's contributions have earned significant recognition, including the prestigious Pakistan Innovation Award for their groundbreaking AI solution, ComplianceMachine.ai, a web-based solution tailored to help organizations

achieve and maintain compliance with various standards, cybersecurity, and data privacy regulations. With over a decade of excellence, they are trusted by a diverse clientele across industries like government, defense, AI, FinTech, SaaS, and more.

Backed by more than 10,000 consulting hours, 200+ successful client engagements, and a presence in UAE and Pakistan, they stand out for their proven results. Their tailored services ensure measurable outcomes, delivering value and transformative growth to businesses worldwide.



The Kinverg team demonstrated exceptional expertise and commitment throughout our project. Their dedication and professionalism were outstanding, and we are extremely pleased with the high-quality work they delivered. Kinverg's thorough approach and in-depth knowledge have made a significant impact on our project's success.

– Dave Engberg, Partner, Cleryedge⁴⁸

Primary Products

- ▶ **ComplianceMachine.ai:** Award-winning AI tool for automating regulatory compliance.
- ▶ **Cybersecurity Compliance:** Solutions for NIST, ISO 27001, and DoD regulations.
- ▶ **Data Privacy:** GDPR, HIPAA compliance, risk assessment, and mitigation.
- ▶ **AI Strategy:** Tailored roadmaps for leveraging AI in business transformation.
- ▶ **Training & Certifications:** Professional training, including Lean Six Sigma.
- ▶ **Digital Transformation:** Modernizing operations and optimizing business processes.

⁴⁸ Testimonials - kinverg. (2024, October 27). Retrieved from <https://kinverg.com/testimonials>

INFOGISTIC®

Infogistic

Infogistic Pvt Ltd is a leading IT solutions provider specializing in Information Security, Healthcare IT, and AI/Analytics. Founded in 2012, this Pakistan-based company excels in transforming innovative ideas into robust technology solutions, helping organizations optimize processes and enhance revenue streams. Infogistic has established a strong presence across the GCC, MENA, and Pakistan.

Infogistic also offers a diverse range of services, including Penetration Testing, IT security audits, technology risk assessments, and vulnerability assessments. The company particularly specializes in assisting clients with implementing best practices using international standards, such as CMMI, ISO 9001, and ISO 27001.

Their security solutions include PhishRod, an anti-phishing platform, and CloudClinik, a cloud-based EMR and practice management system. In the healthcare sector, the company's CloudClinik platform provides cloud-based EMR and practice management solutions for medical professionals. Additionally, their AI-powered tools, such as the Smart Surveyor automate feedback and survey management, providing real-time insights to improve customer satisfaction. Their dedication to delivering customized, high-quality solutions makes them a trusted partner for clients aiming to achieve their strategic objectives.



Primary Products

► **PhishRod**

A leading anti-phishing solution that empowers organizations to combat cyberattacks by educating employees and implementing advanced security measures.

► **CloudClinik**

A cloud-based EMR (Electronic Medical Record) and Practice Management system designed for healthcare professionals, offering telemedicine, appointment management, and secure data storage.

► **Smart Surveyor**

An AI-powered feedback and survey management system that automates branch surveys, providing real-time insights to enhance customer satisfaction.

► **Retail Analytics**

A comprehensive analytics solution offering insights like footfall, heatmaps, demographics, and audience behavior to optimize retail performance.

► **Dynamic Ad Analytics**

A tool to measure the effectiveness of digital ads by analyzing footfall, dwell time, gaze time, and audience demographics, enabling targeted and interactive ad campaigns.

► **COVID-19 SOP Compliance**

A real-time analytics solution ensuring compliance with health and safety protocols, including mask-wearing, social distancing, and occupancy management.



TALK TO US



**Do you run a business in the
Information Security industry?**

Get in touch with your details now at

mkt@pseb.org.pk

and we'll take it from there.

**Also email us for any comments, suggestions
or errors in this whitepaper.**

**For more information on
registered companies, please visit**

<https://techdestination.com>

About this Industry Roundup

Pakistan Software Export Board developed this paper by hiring services of independent consulting firms to prepare this roundup on Pakistan's Information Security sector. The paper focuses on Pakistan-based companies in this vertical and appraises the reader of the expertise available in this domain.

Disclaimer

All the information provided in this roundup is compiled by the consulting firms and based on the available material about the companies covered in this roundup. Coverage in this industry roundup document is not an endorsement by Pakistan Software Export Board (PSEB), Ministry of Information Technology and Telecommunication (MoITT) or the Government of Pakistan (GOP). The Pakistan Software Export Board, Ministry of Information Technology and Telecommunication, or the Government of Pakistan assumes no commercial financial or legal liability accruing from any transactions with the firms featured in this industry roundup.

A product of TECH destiNATION Media

Commissioned by:

