SECNAP NETWORK SECURITY

Cybersecurity Services Overview

Multilayered Cybersecurity Beyond The Traditional

It can take merely seconds for an intruder to compromise a network and just minutes to start extracting data. Yet in 2018 Verizon Reported that 56% of breaches took months or longer to be discovered.* Having a proactive multilayered security approach is the effective way to safeguard your data. As security provider, we pride ourselves in offering a unified platform of offerings that allows us to support our clients as they scale towards a mature security offering.

Vulnerability Management

External Penetration Testing

Only by conducting regular External Penetration Testing can an organization ensure that information and network assets remain safeguarded from unauthorized access and abuse. SECNAP's External Penetration Testing provides reporting that includes current vulnerabilities prioritized by severity and the actions you can take to resolve them.

Internal Vulnerability Assessment

This assessment is a comprehensive review of your company's internal network focusing on vulnerabilities that can be exploited by authenticated internal users as well as unprivileged guests. Every device within your network is evaluated for configuration backdoors, malware, trojans, and configuration errors. Specific remedial actions are recommended and prioritized so that your IT team can address the most significant vulnerabilities immediately.

Web Application Security Assessment

Web application attacks have accounted for the largest number of confirmed data disclosure breaches[1]. Our security experts test for security risk, including OWASP Top 10 as well as Black and White Box testing, providing detailed next steps to prevent you from becoming a statistic.

Managed Detection and Response

Cloud Delivered | Hybrid | On-Premises

Our Managed Multilayered Security offering features patented technology that manages, detects and responds to ongoing cybersecurity threats. We protect against data breaches by leveraging our technology and highly trained security experts who monitor your network around the clock and in real-time.

Our technology, in combination with our SOC, eliminates labor intensive log analysis and alert fatigue allowing your IT resources to focus on your actual business needs.

PROACTIVE TECHNOLOGY + SECURITY EXPERTS

MANAGED 24/7 BY SECURITY OPERATIONS CENTER

*Lateral Threat Detection availability based on configurations.

V19.1

SECNAP NETWORK SECURITY

Cybersecurity Services Overview

Consulting and Regulatory Compliance

IT Risk Assessments | HIPAA | HITECH | HITRUST | GLBA | ISO 27001/2 | ISO/IEC 9126 | PCI | SOX

Our certified security auditors leverage a complete audit toolkit to ensure that you receive useful, comprehensive information suitable for immediate action. Our procedural and process evaluations include automated testing, network and wireless scans, personnel interviews, social engineering, and policy reviews. Regulatory compliance assessments provide you with gap analysis allowing you to meet your compliance deadlines.

Email Security

Using advanced algorithms and spam pattern detection methods, our Email Security Solution filters inbound and outbound emails separating the legitimate from the unsolicited. Protect inboxes from spam, viruses, phishing harvesting and other malicious threats. The outbound filtering ensures continuous email delivery by filtering outbound spam messages which avoids blacklisting and undelivered outbound emails due to low reputation issues.

Cybersecurity Awareness

Phishing Simulations

Phishing simulations test employees on how they would respond to a real-life phishing attack. We can send these mock attacks at staggered times which helps avoid the "prairie dog effect" where employees warn one another of the email. We'll track which employee behaviors and report on which employees ignored, click or completed the objected of the simulated attack.

Security Awareness Training

It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee. Our easy-to-understand, short and visually engaging training videos end with an online quiz to verify the employee's retention of the training content.

Dark Web Monitoring

Our Dark Web Monitoring service leverages Dark Web intelligence with search capabilities to be able to identify, analyze and proactively monitor for your organization's compromised PII and employee credentials. Being aware of exposed stolen data can allow you to take steps such as resetting passwords to avoid further compromise.

Incident Response

Get back online quickly with the help from our security consultants who will detect, contain and take action to prevent future attacks. Our consultants are available 24/7 to respond to an attack and will leverage our 24/7 Security Operations Center in combination with our patented proprietary technology.