SECNAP NETWORK SECURITY

Cybersecurity Beyond The Traditional

It can take seconds for an intruder to compromise a network and minutes to start extracting or encrypting data. Over 50% of breaches go undetected until the cybercriminal informs the cyber victim that they've been infiltrated.* Having a proactive, multilayered security approach is the best way to safeguard your data. As a cybersecurity provider, we pride ourselves on offering a unified platform of product offerings that allows us to support our clients as they scale towards a mature security posture.

Vulnerability Management

External Vulnerability Assessment

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

Internal Vulnerability Assessment

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. Devices within your network are evaluated for configuration backdoors, malware, trojans, and configuration errors. Remedial actions are recommended and prioritized so that your IT team can address the vulnerabilities immediately.

Web Application Security Assessment

Web application attacks have accounted for the largest number of confirmed data disclosure breaches. 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

- **Intrusion Prevention System**
- **Intrusion Detection System**
- **Security Information and Event Management**
- **Internal Threat Detection**
- **Lateral Threat Detection**
- **Vulnerability Management**
- **Integrated Endpoint Detection****
- **Data Loss Prevention**

Managed 24/7 by Security Operations Center

*2022 Verizon Data Breach Investigations Report ** Optional Feature

V22

SECNAP NETWORK SECURITY

Cybersecurity Services Overview

Security Information and Event Management

A fully Managed and Monitored SIEM centralizes data by collecting logs and events generated by host systems, security devices, and applications on a single platform. These logs and events are then translated into actionable reports and alerts through our proprietary advanced intelligence engine and provided to our 24/7, U.S.-based SOCs enabling SECNAP to respond immediately and block cyber threats in real-time.

Extended Detection and Response

Our extended detection and response (XDR) solution provides the ultimate security posture. By integrating both our Managed Detection and Response (MDR) product with our SIEM solution, and incorporating an integrated endpoint agent, we obtain full visibility into your network, and enable our advanced intelligence engines and security operations analysts to provide comprehensive cybersecurity to your network.

Cybersecurity Awareness

Phishing Simulations

Phishing simulations test employees on how they would respond to a real-life phishing attack. We'll track employee behaviors and report on which employees ignored, clicked or completed the objective 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.

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.