SECNAP
NETWORK SECURITY

On-Premises • Cloud-Delivered • Virtual • Hybrid

SECNAP Network Securityis a managed security service provider (MSSP) and a cybersecurity research and development company. Since 2001, we have been combining **human intelligence** with **innovative patented technology**, designed inhouse, to protect private sector organizations and government agencies of all sizes against data breaches, ransomware, phishing, advanced persistent threats (APTs), and other cyberattacks. Our mission is to assist our clients in safely and securely conducting business across the internet by providing organizations of any size, with the same comprehensive protection against cyberattacks that large enterprises and the federal government enjoy but at a fraction of the cost.

CLOUDJACKETXi

Our **Flagship Cybersecurity Service** provides state-of-the-art protection against malware, ransomware, data breaches, unauthorized access, and other sophisticated attack vectors.

CloudJacketXi™ delivers an **enterprise-grade cybersecurity** platform at a **cost accessible to SMBs and mid-market organizations**. **CloudJacketXi** unifies **EDR, SIEM**, **MDR**, and **NDR** functionalities together with a **threat intelligence platform** in a single comprehensive solution. This cutting-edge technology collects vital data from a myriad of sources, which is then analyzed through our proprietary **extended intelligence engine** and assessed by our **Security Operations Center** (SOC) - a dedicated team of highly-experienced cybersecurity experts based in the USA. **CloudJacketXi** provides complete security for your organization, empowering you to focus on your business growth.

Fully Managed and Operated by our 24/7 SOC:

Run by a team of expert cybersecurity professionals who hunt, investigate, and advise clients on sophisticated threats 24/7/365.

Greater Visibility and Response:

Expanded integration with endpoint agents and new technical abilities that leverage endpoint agent capabilities

Proprietary Cloud-Based Analysis Engine and Security Operation Center:

The CloudJacketXi proprietary cloud-native analysis engine and security operation center work together to provide both human and Machine Intelligence to secure your networks and data.

Behavioral Analytics:

Real-time visibility & identification of threats that prevent attacks by automatically blocking suspicious activity & recognizing patterns.

Extensive Forensic Knowledge:

Quickly detect and identify both historical and emerging threats using well-trained cybersecurity experts and data since 2001.

No Hardware Required, Cloud-Native And Cloud Delivered:

Hardware-free, fully cloud-native XDR & SIEM solution that eliminates the need for expensive equipment and upgrades. Fast and effortless deployment across a variety of endpoints. No hardware or hosting required on the customer side for SIEM+EDR (XDR).

Storage and Log Retention:

Comprehensive storage and log retention capabilities, including “Cold Storage” for compliance or forensics purposes, and “Hot Storage.

Flexibility and Scalability:

No need to replace SIEM hardware if scaling operations up or down. Deployments can evolve with an organization.

Compliance and Regulatory Matters:

Provides SIEM, XDR & MDR functionality, log analysis, file monitoring, assessments, incident response and other services for compliance.

Internal Vulnerability Assessments safeguard the network's assets that could be exploited and affect the confidentiality, availability and integrity of your network. A security assessment reveals your organization's existing IT vulnerabilities and provides recommendations on improvements to your security defenses.

External Security Assessments are designed to identify vulnerabilities and weaknesses in an organization's external facing infrastructure. Our certified security experts test against over 100,000 vulnerabilities that could give an attacker access to an organization's network, steal sensitive data, or cause other types of harm. We provide a detailed report which includes remediation recommendations.

Compliance Consulting Services help organizations navigate the complex regulatory landscape and can reduce the risk of data breaches, regulatory fines, and other legal liabilities. A compliance assessment evaluates an organization's compliance with regulatory requirements and industry standards. This assessment may include a review of policies and procedures, security controls, and risk management processes. By leveraging SECNAP as a third-party auditor, organizations ensure that objective experts are engaged and that in-house IT and audit personnel are able to remain focused on mission-critical responsibilities.

Incident Response Teams help organizations quickly identify and contain the breach. The team provides forensic analysis, remediation planning and recovery assistance to ensure minimal disruption to the organization's operations.

Web Application Assessments help identify and address potential vulnerabilities in web applications that could be exploited by attackers. The assessment is designed to address the components and variables unique to your organization in order to deliver results that will assist you in hardening your application security.

Dark Web Monitoring helps organizations identify potential threats and vulnerabilities on the dark web. This service scans the dark web for stolen credentials, sensitive data, and other indicators of potential compromise, enabling organizations to take proactive steps to mitigate any potential threats.

Awareness Training Programs educate employees and other stakeholders on how to protect themselves and their organization from risks associated with cyber threats and sophisticated phishing attacks. The training has been designed using online modules or courses that employees can complete on their own time. These courses cover a range of topics, such as how to recognize phishing emails, how to use secure passwords, and how to avoid downloading malware. Our program tracks employees progress, identifies employees who are struggling, and provides additional training for those who need it.

Our flexible security-as-a-service platform allows for a multi-layered approach where you can choose exactly what your organization needs.