SECNAP
NETWORK SECURITY

CLOUDJACKETX

On-Premises | Cloud Delivered | Hybrid

Cybersecurity Managed By
The Team Who Developed It

Managed Cybersecurity Platform With Flexible Modules

CloudJacketX is a managed security solution developed to address the major pain points of IT teams such as alert fatigue, lack of resources and the shortfall of vulnerability visibility. Our patented and patent pending technology 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 platform is built to be customized so our clients only pay for the components their environment needs.

It can take mere seconds for an intruder to compromise a network and just minutes to start extracting data. Yet according to the 2019 Verizon Data Breach Report, 56% of breaches took months or longer to be discovered. Having a proactive and in-line multilayered security approach, such as CloudJacketX, is the effective way to safeguard your data within Google Cloud, AWS, Azure, on-premise or hybrid environments.

Managed Cybersecurity Layers

Detection and Prevention Technology works in-line and passively to actively detect and block based on severity, source, reputation, geography, custom tuning. advanced heuristics, and deep packet inspection.

Internal Threat Detection is designed to mimic legitimate services, such as servers and file shares, in order to attract and detect unauthorized access, which provides effective protection against Advanced Persistent Threats, Ransomware, and Insider Threats.

Lateral Threat Detection* help stops the spread of internal infection throughout your network by allowing our SOC to detect threats as they attempt to spread between hosts and working locations.

Security Information and Event Management (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.

Intrusion Prevention System

Intrusion Detection System

Security Information and Event Management

Internal Threat Detection

Lateral Threat Detection*

Vulnerability Management

Endpoint Detection

Data Loss Prevention

MANAGED 24/7 BY SECURITY OPERATIONS CENTER

V20.3

*Lateral Threat Detection availability based on configurations.

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

SECNAP
NETWORK SECURITY

CLOUDJACKETX

Cybersecurity Needs Relentless Monitoring

With the industrialization of cybercrime and the increase in government privacy regulations, cybersecurity has now become boardroom priority. Protecting your network has many moving parts and has to be done around-the-clock in order to be effective. When choosing cybersecurity solutions, it is important to know that security minded personnel are actually tuning and monitoring the tools.

Cure Alert Fatigue

79% of security teams are overwhelmed by the volume of alerts.* The alerts being received are nearly impossible to manage without using overly permissive security policies. This results in more threats slipping through as the volume and complexity of alerts increase.

Solution to Reactive Log Review

Traditional log-based tools can be the inexpensive option but your team will need to manage and review historical information to decide what to block. Our technology works in sync with our SOC to secure your network and thus allowing your team to focus on actual business needs.

PROACTIVE TECHNOLOGY + SECURITY EXPERTS

- Advanced heuristics and deep packet inspection to detect anomalous activity before it enters the network
- In-line technology actively blocks based on severity, source, reputation, geography and custom tuning
- Advanced threat detection that protects against known, emerging and advanced persistent threats
- Contain and block installation, spread, and execution of malicious code
- Improved visibility into network that endpoint and firewalls lack
- Client data is not stored, narrowing down the scope for regulatory and compliance audits
- Built-in Vulnerability Management

- US Based Security Operations Center (SOC) is staffed 24/7 with highly trained analysts
- Real-time monitoring with immediate analysis and response that eliminates labor intensive log analysis
- Manage use of ports, protocols, and services on networked devices
- Over 99% of events are mitigated by our SOC without client intervention
- SOC manages same-day deployment with little to no effort from IT Team
- Eliminates labor-intensive log analysis and alert fatigue inherent with unmanaged SIEM solutions
- Analyst available 24/7 over phone or ticket system

Security Experts Managing, Detecting and Responding to Cyber Threats

Our security analysts are dedicated to reviewing every alert in order to identify, confirm and block threats. The team will get to know your business policies and tailor our service to ensure that security does not interrupt legitimate business. Less than 1% of alerts will actually need any intervention from your team. This frees up your inbox from unread alerts and eliminates labor intensive log analysis.

Our real-time dashboards and reports provide visibility and facilitate regulatory compliance. CloudJacketX is a SOC 2 compliant solution and based out of a datacenter in the US. We value customer service and consider our SOC experts as an extension of your team.

* 2017 Bay Dynamics Report

SECNAP
NETWORK SECURITY

CLOUDJACKET SIEM

On-Premises | Cloud Delivered | Hybrid

Fully Managed, Expertly Monitored SIEM + MDR Services

Comprehensive Cybersecurity that Fits Your Budget

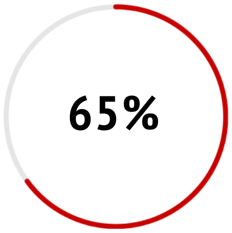
Inadequately protected networks are extremely vulnerable to infiltration by a variety of rapidly changing and increasingly sophisticated global cyber threats, including data breaches, ransomware, phishing, insider threats, and advanced persistent threats (APTs).

A security information and event management (SIEM) solution collects logs and event data from clients' host systems, applications, and security devices throughout the organization's infrastructure and organizes the information into a single, easily viewed platform. In addition to correlation, categorization, analysis, and alerting of security incidents and events, a SIEM provides log retention and retrieval functions that aid in compliance reporting.

Organizations can mitigate risk, defend against cyber threats, simplify compliance, and improve forensic capabilities by deploying a managed SIEM solution backed up by 24/7 SOC monitoring. However, most fully managed SIEM tools with SOC monitoring -- let alone managed detection and response (MDR) -- are cost prohibitive for many organizations. Less expensive solutions instead offload some or all of the management, support, and data output monitoring to the organization's IT team. This poses a significant internal challenge even for many large organizations.

A SIEM is Only as Good as The People Monitoring it

SIEMs must be monitored 24/7 so that identified threats can be responded to immediately. Most organizations lack sufficient staff to devote to round-the-clock SIEM monitoring and threat management. Internal IT personnel struggle to find the time to properly manage the SIEM and still complete their other job duties. The typical organizational network generates 10,000 alerts each day. Nearly all of these are false positives, but since the risk posed by a bona fide threat is so dire, each one must be investigated. Alert fatigue sets in, and malicious activity slips through.



Percent of organizations that struggle to find qualified cybersecurity personnel.

Finding, Retaining and Scheduling Cybersecurity Staff

Another common issue is a lack of in-house security expertise. SIEMs are valuable tools, but they provide only incident monitoring and alerts, not response. Early detection of a cyber threat is of no value if the staff monitoring the SIEM lack the expertise and ability to immediately respond to the threat. Cybersecurity personnel are difficult to find and retain. Nearly two-thirds (65%) of organizations report a shortage of qualified cybersecurity personnel, and 51% of cybersecurity personnel report that their organizations are at moderate or severe risk of cyberattacks due to a lack of adequate cybersecurity staffing.

Due to a lack of adequate staff to monitor a SIEM around the clock, and staff who also may lack security expertise and experience to respond to threats, organizations may struggle with a security tool they are unable to use properly -- which results in a network that remains vulnerable to attack.

Multiple Layers, Timely Monitoring, and Rapid Response

SECNAP's CloudJacketX Managed SIEM is a security-as-a-service solution that provides superior layers of detection and protection, backed up with real-time incident response by our 24/7, U.S.-based SOCs, all at a fraction of the price of competing solutions.

Early identification is of no value if a threat is not stopped. The CloudJacketX Managed SIEM combines MDR services with a fully managed SIEM, enabling SECNAP to respond immediately and block cyberthreats in real-time.

24/7 Monitoring for Threats to be Detected Rapidly.

Real-time security monitoring from our 24/7/365, U.S.-based SOC, staffed by U.S. citizens who are all highly vetted SECNAP employees.

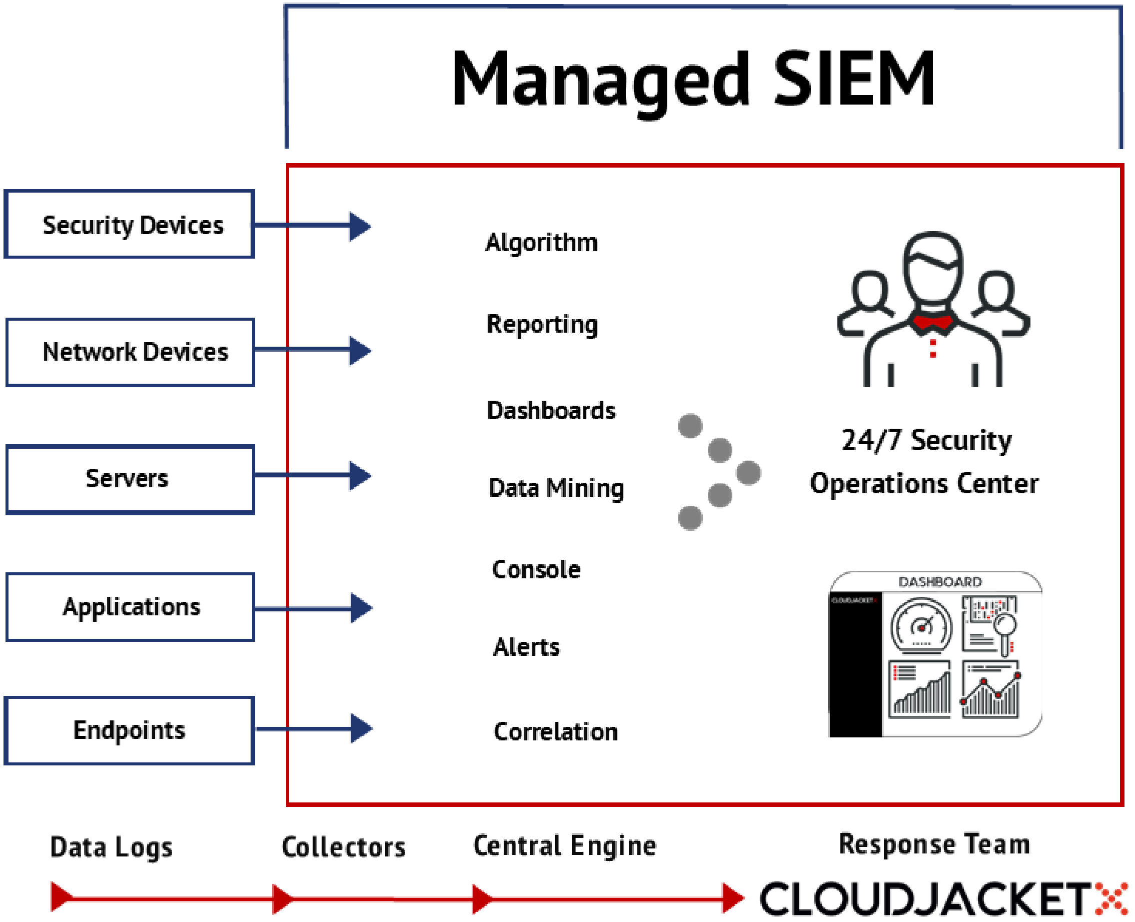
Active Directory Monitoring: allows our SOC to monitor when modifications such as add, change, remove and escalation of privileges, are made to computers, groups, group members and policies.

Behavior Profiling/Data & End User Monitoring. Immediate investigation of anomalous activity, such as strange DNS lookups or a user logging in at odd times.

Application monitoring allows SECNAP to alert clients if they are running outdated software that could leave them vulnerable to an attack, as well as notify them when their end users install or modify apps

Rapid Detection is Important. Rapid Response is Crucial.

- **Threat intelligence.** SECNAP develops our own threat intelligence in-house through a network of globally deployed sensors and honeypots which track the spread of international threats and views hacking activities in different regions, including the development and testing of malware. This allows us to program our systems and create patches which can block emerging malware well ahead of it being released into the wild.
- **Highly intuitive log search** with a web interface to search either current day or historical logs, retain, and retrieve them for compliance purposes, with reports to enhance visualization.
- **Forensic capabilities.** Logs are automatically sent to the SIEM so that analysts can analyze events; these logs can also be presented as a defense in court cases. One year of archived log data is retained for all devices.
- **Analytics.** One central dashboard allows clients to view the same information our SOC does, including when users are logging on and off.
- **Incident response** in compliance with NIST SP 800-61, Computer Security Incident Handling Guide.



Managed SIEM

Security Devices

Network Devices

Servers

Applications

Endpoints

Algorithm

Reporting

Dashboards

Data Mining

Console

Alerts

Correlation

24/7 Security Operations Center

Data Logs

Collectors

Central Engine

Response Team

CLOUDJACKET

Cybersecurity Should Simplify Compliance and Be Flexible

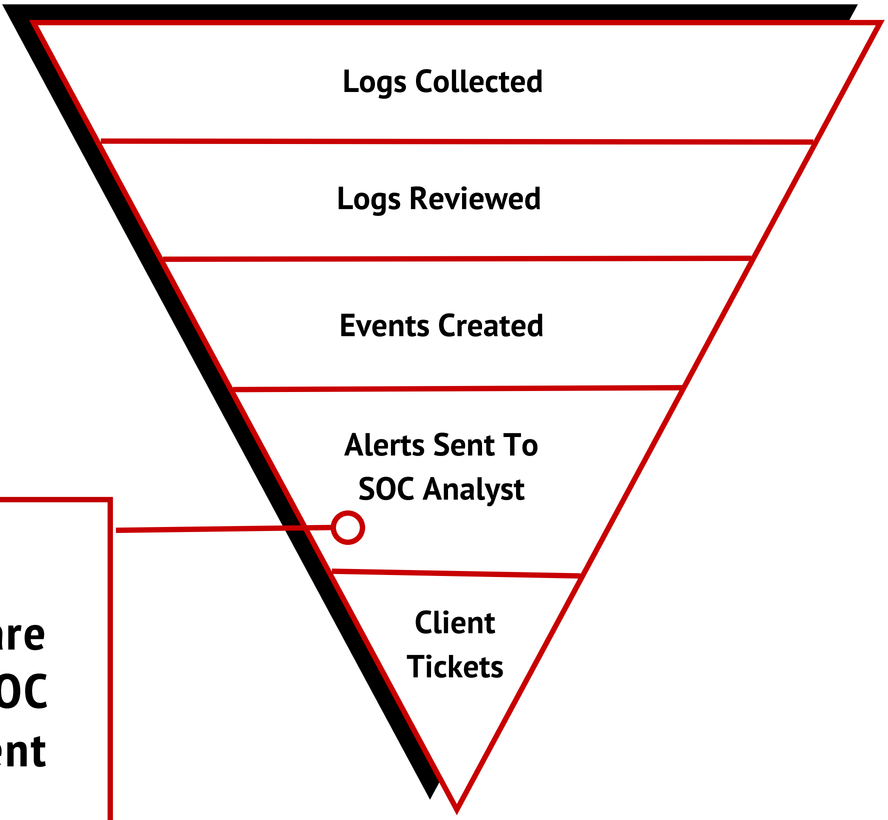
- **Facilitates Compliance** and can be configured to meet any SIEM-related compliance requirements, including PCI DSS and HIPAA.
- **Flexible deployment options,** with the ability to receive logs inline and in real time, on-prem or in the cloud, from any device that can export them.
- **Event collection rate suited for very large scale deployments.** SECNAP sizes our hardware and virtual machines based on each client's individual needs, so that our hardware will never slow down a client's network.

Seamless Teamwork from Your Cybersecurity Service Provider

Unlike some security providers, we don't outsource our development or our SOC. Our developers and security analysts are based in the same buildings, making communication seamless and allowing for a continuous feedback loop between the security experts in our SOC and our development team. SECNAP's security analysts provide feedback to our development team so that they can address specific client needs and make overall improvements and enhancements to our SIEM.

SECNAP's ability to rapidly develop new features to continually enhance network security provides a significant advantage over competitors who utilize outsourced third-party SOCs or SIEM tools.

Log Review in Real-Time.



99%

Percent of events are mitigated by our SOC Analysts without any client intervention.

SECNAP NETWORK SECURITY

CLOUDJACKETX SIEM

Continuous Feedback Loop for Continuous Improvement

The diagram below provides a visual model of how this system functions.

Threat Detection: CloudJacketX detects a potential threat in the client's network.

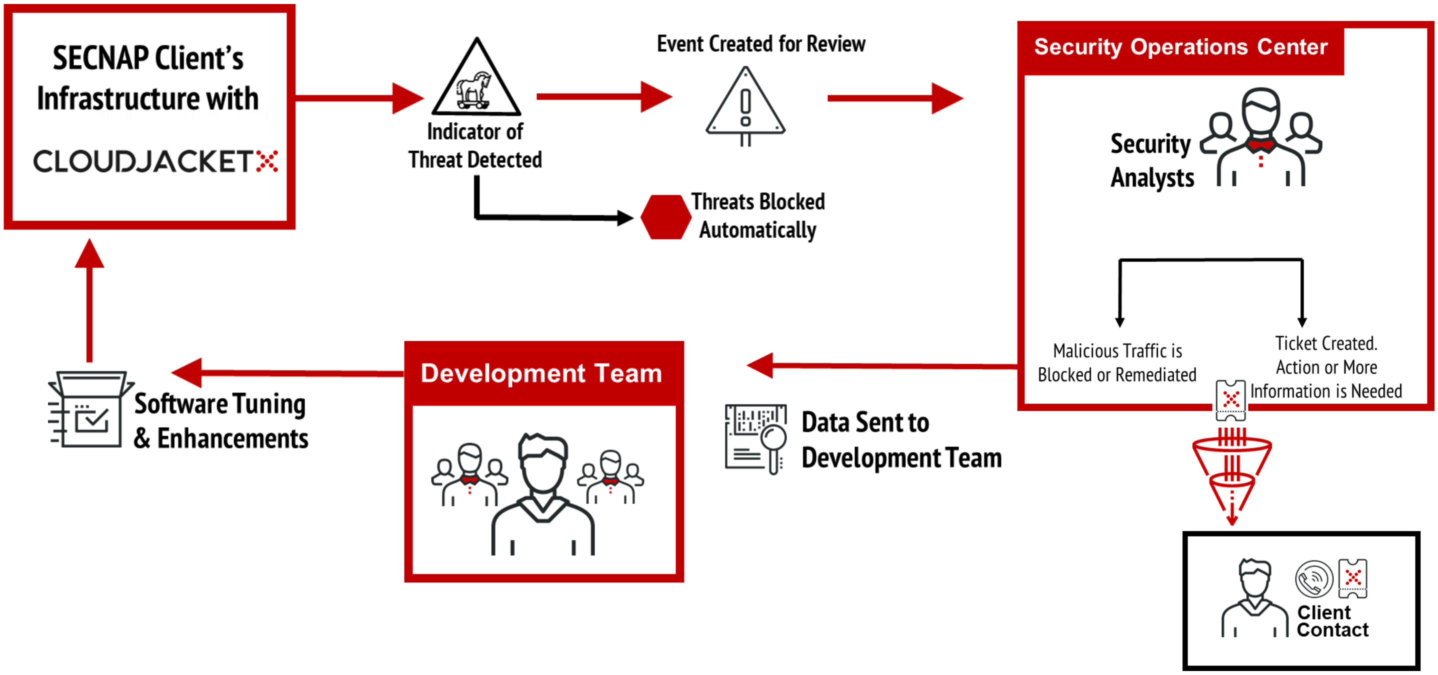
- Known threats are blocked automatically.
- If the threat requires further investigation, a ticket is generated and sent to SECNAP's SOC.

SOC Investigation & Response: At our SOC, a security analyst utilizes the platform's capabilities to investigate the corresponding events to determine if the alert is a legitimate threat or a false positive.

- If the analyst needs more information to proceed, the client is immediately contacted. Fewer than 1% of alerts require attention from our clients.
- After the threat has been addressed, our development team receives feedback from our SOC Analysts.

Technology Enhancements: Our development team uses this incident data to continually enhance our SIEM software, make necessary improvements, and harden its ability to identify and filter out false positives while blocking the actual threats.

Our can collaborate efficiently to get our clients the features they need.


SECNAP Client's Infrastructure with CLOUDJACKETX
Indicator of Threat Detected
Event Created for Review
Threats Blocked Automatically
Security Operations Center
Security Analysts
Malicious Traffic is Blocked or Remediated
Ticket Created. Action or More Information is Needed
Client Contact
Data Sent to Development Team
Development Team
Software Tuning & Enhancements

SECNAP
NETWORK SECURITY

About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP's proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

GSA Advantage!

Choose a managed security service provider that will secure your data and help facilitate compliance.