Product Overview

For Threats That Lurk in the Deep - Skylight Interceptor™

Cloud-Native NDR

Skylight Interceptor is a SaaS Cloud-Native Network Detection and Response (NDR) solution with real-time network detection to respond to increasingly sophisticated threat tactics with confidence.

Vigilant Detection for Threat Insights

Correlated alerts and attack progression

Don't wait until it is too late. Virtualized and hybrid cloud networks are increasingly complex and it is easy to miss threat actors that lurk in your network.

Skylight Interceptor remains vigilant, collecting and correlating metadata from network packets from all your transations. The tracking of attack progression utilizing the MITRE ATT&CK framework lets your team easily visualize what is happening across the network to detect threats.

Benefits

Single platform for performance and security
Multi-use sensors

Deploy where others can't
100% end-to-end visibility with flexible sensors

Skylight Interceptor sensors are easy to deploy where you most need them to provide deep visibility into complex cloud network flows. They capture and correlate metadata from both north-south and east-west traffic that traverses your network and across your clouds. No need to spend on storing full network packets for investigations. Faster detection and more cost effective threat hunting and forensics with optimized metadata collection.

Skylight Interceptor monitors traffic and creates behavioral models to detect any dangerous or suspicious anomalies. Alerts are correlated to create incidents, providing the context you need to understand and respond to attacks of all types.

Why NDR?

Your team will be better prepared for any situation since NDR solutions inform incident response (IR) workflows by providing:

1. Scope, severity, and the probability of an unusual event being malicious
2. Incident reporting based on correlated events and alerts of suspicious behavior
3. Insights for an appropriate course of action for responding to threats
4. The ability to see network threats such as insider threats that typically are difficult to detect with traditional security tools

The Right Response is Critical When Your Network is Being Targeted

Detection

- Receive early indicators of suspicious behavior
- Faster detection with real-time metadata
- Actionable insights from prioritized incidents

Threat Hunting

- Find hidden threats with extensive metadata
- Reveal threat patterns using MITRE ATT&CK framework
- Close security gaps proactively

Forensics

- Easy collection, storage, and retrieval capabilities
- Reduce costs for preservation of evidence
- Satisfy investigations with rigor from metadata collection

Vigilant Detection

- Network metadata reveals every detail of every action taken in your network across all your users, services, and servers. Always on and always correlating.
- Automatically track every device in your network so that you can identify potentially dangerous actors within your network.
- Meaningful alerts with severity levels help guide IT and security teams to what requires immediate action.

Intelligent Threat Hunting

- Strict detection can lead to a high number of false positives so Skylight Interceptor tracks relevant activity and correlates to network elements to create context and more relevant alerts so your team knows what they need to focus on.
- Alerts are mapped to the MITRE ATT&CK framework to make it easier to interpret threat activity and plan for appropriate remediation. Alerts are reported based on severity and the implied objective of the tactics identified.

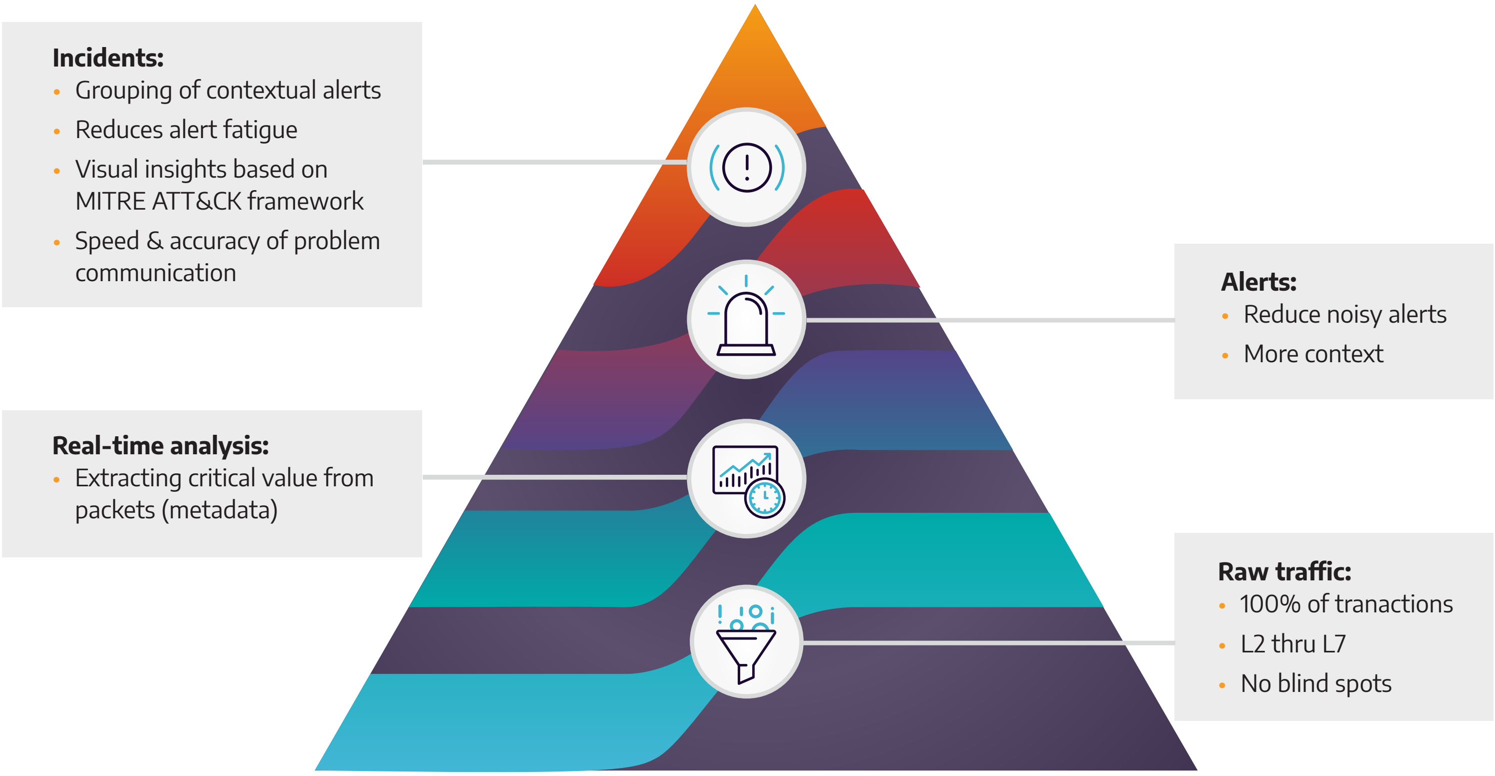
Forensics

Breaches are inevitable in today’s world so gathering evidence for insurance claims or for legal procedures against insiders or criminal investigations is necessary. To be prepared you need a tool that is collecting the information that you may need at all times and organizing it in a fashion that allows experts to build a story of what happened. Contextual evidence that has the time and place and the how and why is crucial to determine what happened and how.

Skylight Interceptor rigorously collects data directly from the network that will satisfy investigations. The metadata is collected and correlated such that it is easy for your forensic team to collect, store and retrieve the information they need. A metadata-based NDR solution, like Skylight Interceptor, reduces your storage and operating costs yet provides the power to dive as deep as your Forensic team needs to find answers.

Actionable Insights from Network Metadata

Accedian network sensors collect real-time traffic behaviors and create actionable insights from network packet metadata. The collection and analysis of network metadata creates context. Context will eliminate noisy alerts and identify malicious behaviors that need immediate investigation and possible remediation. The insights from network packet metadata deliver a more accurate picture than just Netflow without the expense of collecting and storing full packets. **NDR is necessary to see any manipulation of data communications by threat actors that most EDR or XDR solutions will miss.** With Accedian Interceptor NDR you can complement any security stack and gain additional insights for any type of threat from ransomware to insider threats. With metadata you have immediate visibility even to zero-day threats to see if newly identified vulnerabilities have been exploited.



Incidents:

- Grouping of contextual alerts
- Reduces alert fatigue
- Visual insights based on MITRE ATT&CK framework
- Speed & accuracy of problem communication

Alerts:

- Reduce noisy alerts
- More context

Real-time analysis:

- Extracting critical value from packets (metadata)

Raw traffic:

- 100% of tranactions
- L2 thru L7
- No blind spots

Figure 1: Accedian secure network performance

Key Detection Features:
Vigilant Detection of Beaconing with Machine Learning

Skylight Interceptor Leverages Machine Learning to Detect Beaconing

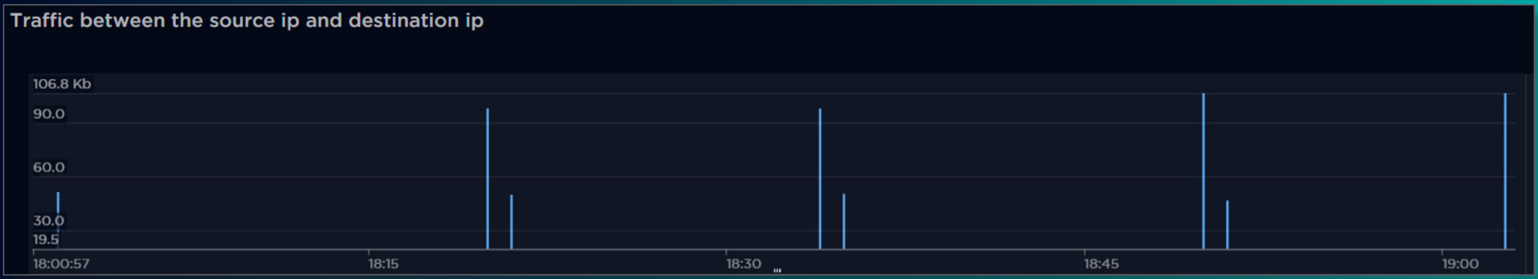


Figure 2: Example of detection of beaconing

Detect Command and Control(C2)

Beaconing is increasingly difficult to detect as threat actors obfuscate their activity. Therefore it is necessary to use machine learning to observe and correlate behaviors across time and across your network to identify any patterns that may indicate beaconing. While in many systems this can lead to a high number of false positives, Skylight Interceptor combines detection techniques to identify and validate beaconing to reduce the number of false positives.

More than 20 Beaconing Features, including:

- Beaconing detections by time
- Beaconing Detections by packet size
- DGA Detection
- Multiple suspicious DNS behavior
- HTTP/TLS malware
- Protocol or port mismatch
  e.g. TLS using port 53 (DNS) to pass through a firewall
- And more ...

MITRE | ATT&CK®

The MITRE ATT&CK* framework is a valuable tool to interpret the intent of threat actors and trace their actions. Mapping to the framework allows for network alerts to be interpreted with context relative to other network activity and identify high priority threats that need immediate attention.

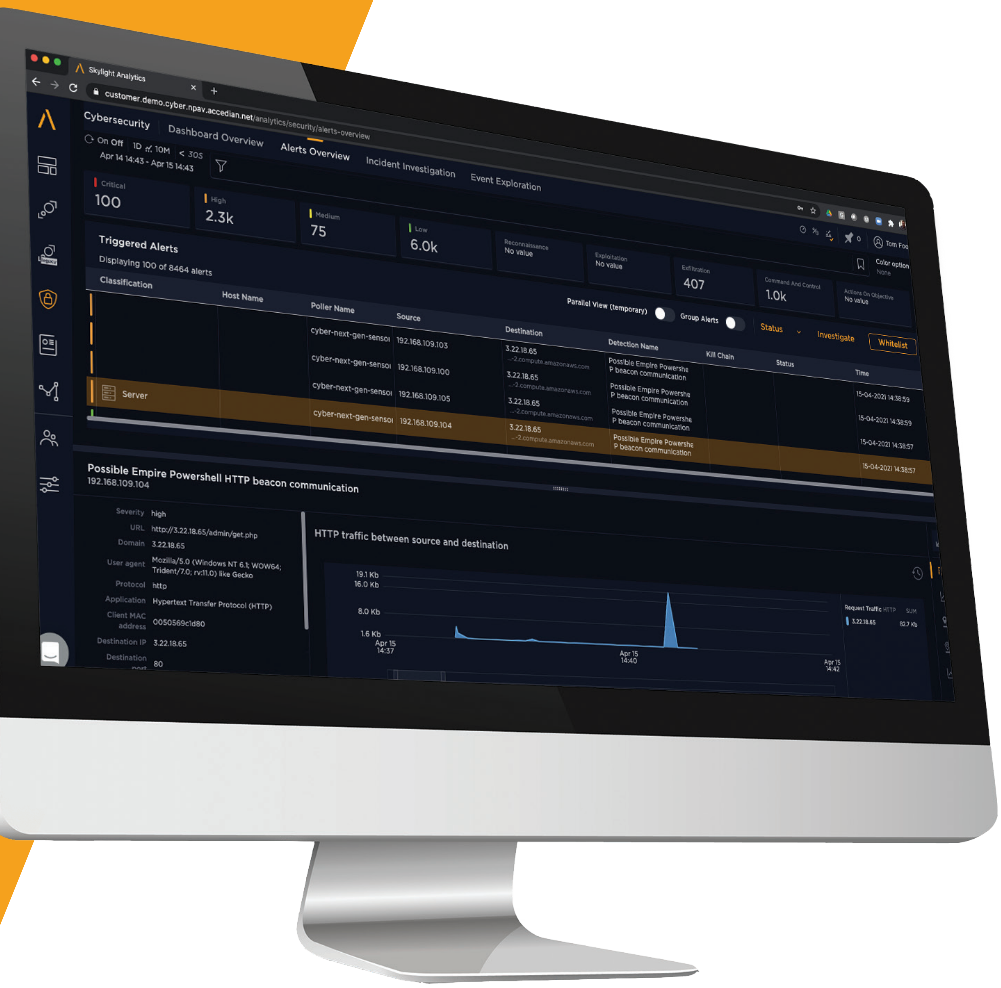
*MITRE ATT&CK is a registered trademark of The MITRE Corporation.

According to Gartner®

Infrastructure and Operations leaders must:

- “Increase alignment between network operations and security operations by coordinating NPM procurement decisions with security analytics solutions, including Network Detection and Response tools.”
- “Focus on vendors that provide support for cloud-native functions, such as APIs or true network data flow.”

Source: Gartner®, “Market Guide for Network Performance Monitoring” Josh Chessman, et al, 9 August 2021 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission



Triggered Alerts

Displaying 100 of 8464 alerts

Classification	Host Name	Poller Name	Source	Destination	Detection Name	Kill Chain	Status	Time
		cyber-next-gen-sensoı	192.168.109.103	3.22.18.65 ...-2.compute.amazonaws.com	Possible Empire Powershe P beacon communication			15-04-2021 14:38:59
		cyber-next-gen-sensoı	192.168.109.100	3.22.18.65 ...-2.compute.amazonaws.com	Possible Empire Powershe P beacon communication			15-04-2021 14:38:59
		cyber-next-gen-sensoı	192.168.109.105	3.22.18.65 ...-2.compute.amazonaws.com	Possible Empire Powershe P beacon communication			15-04-2021 14:38:57
Server		cyber-next-gen-sensoı	192.168.109.104	3.22.18.65 ...-2.compute.amazonaws.com	Possible Empire Powershe P beacon communication			15-04-2021 14:38:57

Possible Empire Powershell HTTP beacon communication
192.168.109.104

Severity: high
URL: http://3.22.18.65/admin/get.php
Domain: 3.22.18.65
User agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Protocol: http
Application: Hypertext Transfer Protocol (HTTP)
Client MAC address: 0050569c1d80
Destination IP: 3.22.18.65
Destination port: 80

Request a demo today
accedian.com

Secure Network Performance

Cloud applications will require new tools that assure and secure the customer experience. Convergence of Network Operations and Security Operations teams and tools is imperative to meeting digital transformation goals and improving security posture. Accedian has 15 years of experience delivering performance monitoring across the network stack
(from the data layer (L2) to the application layer (L7)).

Skylight Interceptor is an NDR solution that provides visibility across your performance and security challenges. Choose Skylight Interceptor for secure network performance today.

Immediate Value for IT and Security Teams

Actionable Visibility

- Deep visibility with easy to deploy sensors for cloud and hybrid environments for both North-South and East-West traffic.

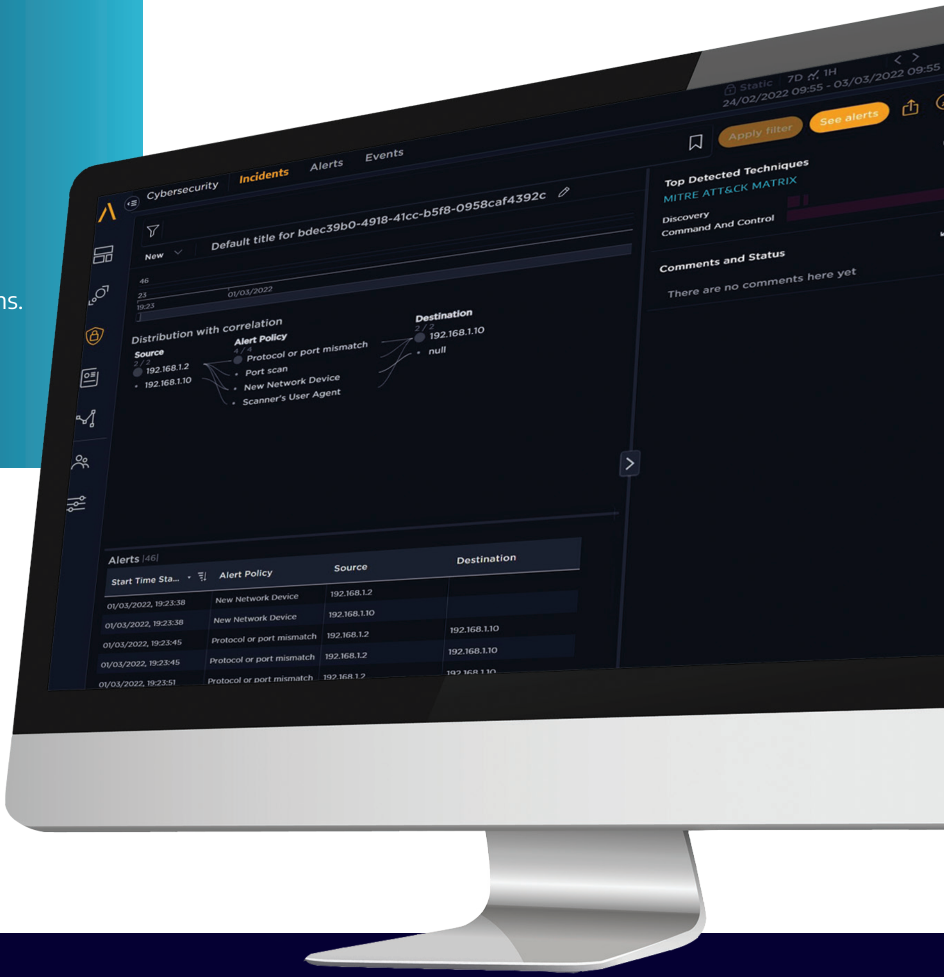
Intelligent Incident Reporting

- Correlated alerts create prioritized incident reporting with MITRE ATT&CK framework dashboard.

Open API's

- Easy to integrate with 3rd parties for automation and streamlined security operations.

Request a demo today
accedian.com



There are no comments here yet

Alerts |46|

Start Time Sta...	Alert Policy	Source	Destination
01/03/2022, 19:23:38	New Network Device	192.168.1.2	
01/03/2022, 19:23:38	New Network Device	192.168.1.10	
01/03/2022, 19:23:45	Protocol or port mismatch	192.168.1.2	192.168.1.10
01/03/2022, 19:23:45	Protocol or port mismatch	192.168.1.2	192.168.1.10
01/03/2022, 19:23:51	Protocol or port mismatch	192.168.1.2	192.168.1.10

About Accedian

Accedian is the leader in performance analytics, cybersecurity threat detection and end user experience solutions, dedicated to providing our customers with the ability to assure and secure their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at accedian.com

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**