ACCEDIAN splunk>

Skylight Powered Security for Splunk

Skylight powered Security for Splunk provides the data and visibility needed to detect real-time suspicious, malicious and anomalous behaviors. It provides a single source of truth for critical IT assets in the enterprise core, data center, and hybrid cloud architectures, monitoring every user, database, transaction, and packet with in-depth precision and unrivaled accuracy.

Increased threats. Ultimate control.

Skylight powered Security for Splunk rapidly provides the critical insight needed to detect advanced, targeted cyber breaches and other evasive attacks that are notably more difficult for organizations to find and prevent. Some of the challenges it addresses are:

- Advanced attacks that evade next-gen firewalls, security gateways, and antivirus solutions, oftentimes hiding and impacting organizations for months
- Polymorphic malware and malware-free attacks that make signature-based defenses ineffective against targeted attacks
- False positive noise: over 80% of alerts generated by signature- and policy-based security solutions are unreliable and take resources away from the most critical alerts

At the heart of Skylight powered Security for Splunk are the Skylight sensors which capture unstructured network packet information and turn it into compact, structured metadata, requiring a fraction of the data storage and power for historical analysis.

This method makes Skylight ideal for today's expansive virtual and perimeter-less attack surfaces – you need the power to see into the darkest reaches of your network with an agile, easy-to-deploy and cost-effective cyber security visibility solution.

Skylight powered Security for Splunk provides:

- Extremely granular security threat detection in real-time
- Forensic data for IR investigation
- Security analytics that provides Tactics, Techniques, and Procedures (TTP), as well as and Indicators of Compromise (IoC), and anomalous threat detection
- Visibility of suspicious lateral traffic that firewalls and other security gateways cannot detect
- Easy to deploy, lightweight sensors covering all network topologies, including hub and spoke, mesh and complex cloud & multi-cloud architectures, protecting high value critical server assets within the core and cloud and across network segments detecting suspicious and malicious internal traffic across the entire physical and virtual attack surface

High fidelity, high resolution, real time data

Ubiquitous, scalable sensors encompassing all virtual attack surfaces – including data center and East-West cloud environments.

- Scalable and available visibility covers your entire digital landscape with no perimeter
- Metadata-based: lightweight storage, no mirrored telemetry network needed
- Application-aware (full-stack visibility from Layer 2 to Layer 7)
- High definition resolution with microsecond detection granularity delivered in 1-minute reporting intervals, with 100% of decoded transactions captured
- Throughput greater than 10 Gpbs
- Economically viable and operationally feasible to deploy
- Rule-less deployment of Skylight sensors – no configuration required to capture 100% of TCP/IP flows and protocol transactions

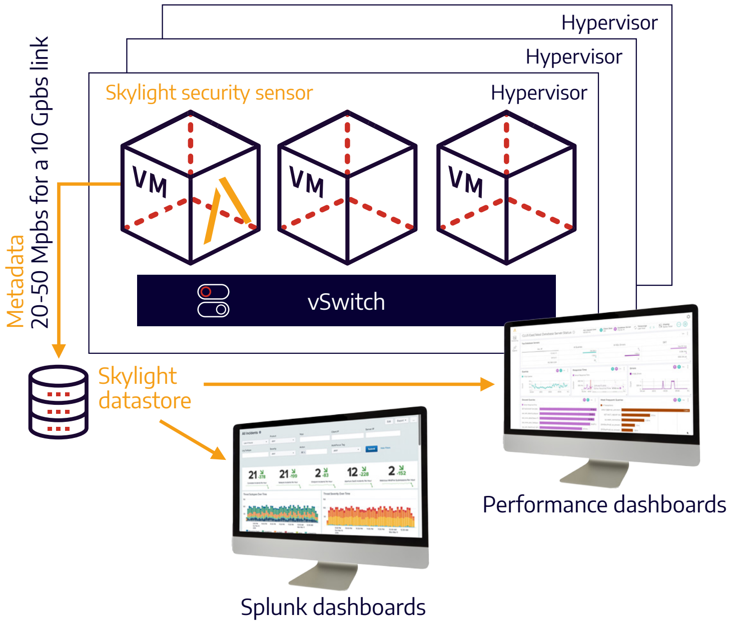

Figure 1: Skylight's dual use sensors provide full security and performance visibility

Skylight metadata reduces the size of the captured packets to less than 0.5% of the traffic analyzed, reducing, for example, 10 Gbps down to just 20-50 Mbps. This means Skylight has wider visibility and can capture security information from places other security monitoring technologies can't reach, and it doesn't require additional infrastructure to transport this information to the Skylight datastore. Instead, the highly compact metadata is easily transported over the production network with no impact to performance.

Skylight sensors use real-time stream analysis to capture wire data and generate an in-depth view of client, network and server interactions – no alternative network flow tools on the market capture 100% of client-server interactions with this agile method.

Skylight examines database transactions to look for possible SQL injections and to determine what information is going into and out of databases. It looks for unusual or large database transfers and notifies SecOps teams via alerts.

The most precise, scalable security monitoring solution available, Skylight powered Security for Splunk shows the security information that can't currently be seen for cloud, data center, and enterprise core and edge.

Complete cyber security visibility with Skylight powered Security for Splunk

The Skylight sensors used within the Skylight powered Security for Splunk provide complete visibility as they are one and the same sensors used for the Skylight network and application performance monitoring solution. This makes Skylight capable of monitoring both East-West and North-South traffic for security and performance within the cloud, data center, hybrid and enterprise core and edge, all with one sensor – an exclusive Skylight capability.

Skylight's highly scalable architecture deploys in seconds, making it ideal for elastic cloud and hybrid infrastructures. It provides detailed actionable intelligence for SecOps teams to detect and avert security threats and to conduct forensic security investigations. Combined with Skylight network and application performance monitoring, Skylight powered Security for Splunk's capabilities provide a best-of-breed monitoring solution for complete visibility and control.

Let us help you detect the abnormal, take action, and take back control before it's too late.

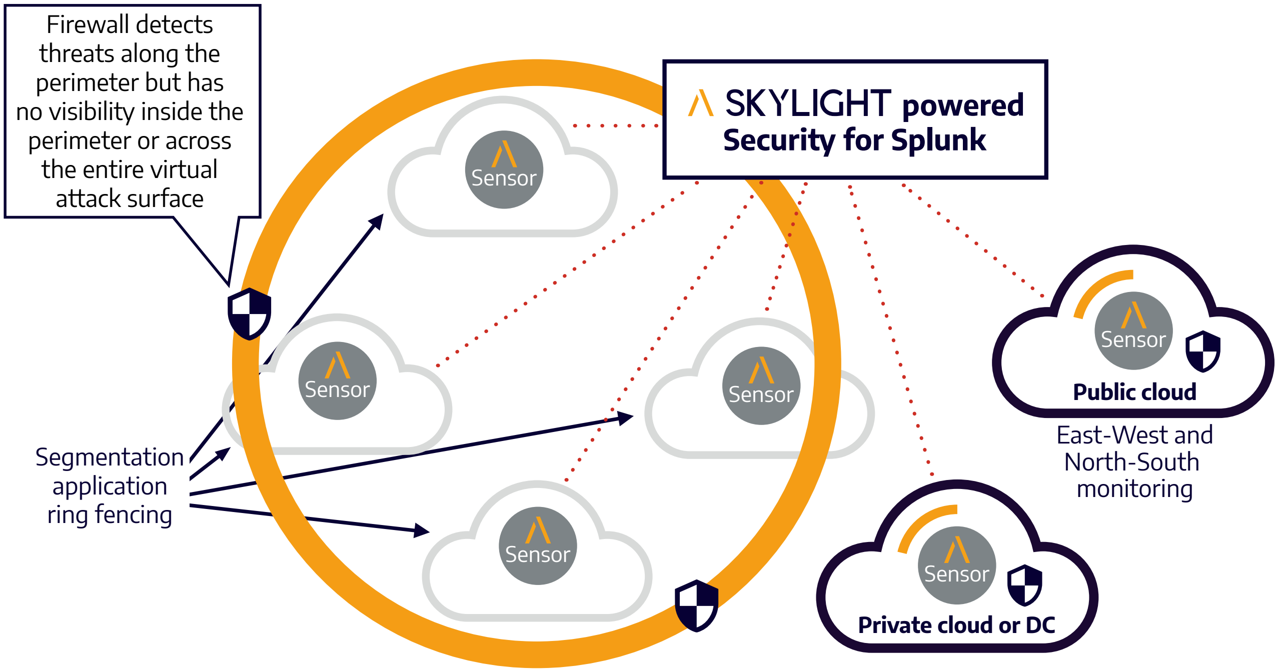
Firewall detects threats along the perimeter but has no visibility inside the perimeter or across the entire virtual attack surface
SKYLIGHT powered Security for Splunk
Sensor
Sensor
Sensor
Sensor
Segmentation application ring fencing
Sensor
Public cloud
East-West and North-South monitoring
Sensor
Private cloud or DC

Figure 2: Skylight sensors deployed across all physical and virtual assets, private or public

Open platform and UI

- Machine Learning enrichment from other data sources, such as the endpoint
- Ability to enforce in conjunction with 3rd party APIs and orchestrators
- Integration of 3rd party threat intel feeds

Ability to analyze and correlate wire data

- Early cyber kill chain warning signals for threats, IOCs, and attacks
- Malicious and suspicious behavior, such as breaches and exploits
- Anomalous behavior detection
- High fidelity forensic data for IR investigation

Complies with the MITRE ATT&CK framework

Splunk Security Essentials

Splunk Security Essentials is the free Splunk app that makes security easier by helping you find the best content, learn how it works, deploy it successfully, and measure your success. Shipping with 120+correlation searches spanning from basic SIEM to detecting advanced adversaries, everything is mapped to the Kill Chain and MITRE ATT&CK. The application also helps you get up to speed faster. It offers a variety of tools to help your deployment, as well as showing the business value of security through simple audit-friendly reports.

Accedian is the first 3rd party vendor available in Splunk Security Essentials. Accedian's list of detections is available to all users searching for these detections in the Essentials application.

To get Splunk Security Essentials, visit Splunkbase at splunkbase.splunk.com/app/3435

ACCEDIAN
splunk>

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 protect 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**