AWAKE | SentinelOne™

The Power of Integrated Network & Endpoint Detection and Response

Get a Holistic View of Your Entire Environment

Detecting and responding to an attacker's tactics, techniques and procedures (TTPs) benefits from a holistic view of everything that is happening in your environment–starting with network which reveals the entire attack surface, like IoT devices and including traditional endpoints that often serve as the vectors for attack. The integration of network and endpoint security enables the most effective defense-in-depth against even the most advanced cyber threats.

The Awake Security Platform, the world's leading network detection and response platform, integrates fully and easily with the SentinelOne Singularity Platform to provide the most comprehensive threat detection, rapid and effective response as well as containment and forensic analysis capabilities. This combination delivers the visibility and confidence you need to maintain a strong security posture across your enterprise.

Better Together: The Benefits

- Visibility & detection for managed and unmanaged devices
- Investigations across the kill chain with endpoint and network detection and response
- Integrated security operations that lower the cost of response
- Rapid and effective response and containment that speeds up time to remediation.

The Strengths of Each Platform

AWAKE

The Awake platform provides broad context beyond managed endpoints to the 50+% of unmanaged infrastructure. Awake thus provides a complete view of the potential attack surface and the business assets that are part of it.

By observing and analyzing every behavior on the network, Awake tracks assets as they move across your network. It autonomously builds an understanding of the relationships and similarities between entities. The platform can sense abnormalities and threats, reacting within seconds if necessary.

SentinelOne™

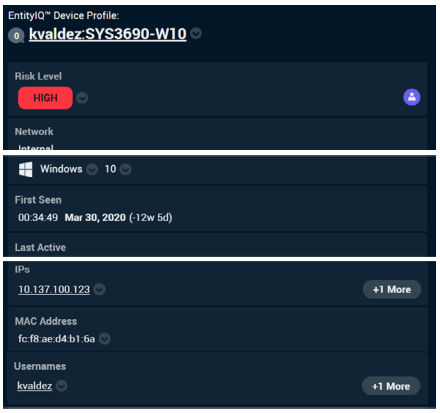
SentinelOne unites endpoint protection, detection, response and remediation. Software agents on the endpoints continuously monitor and collect data pertaining to all aspects of the managed device—how it's configured, what's running on it, where it reaches out to internally and externally, and more.

The platform uses AI engines to identify file-based malware, malicious scripts, weaponized documents, lateral movement, file-less malware, and even zero-days on the endpoints. When malicious activities are detected, the agent responds automatically to contain the threat.

How They Complement Each Other

With this integration, endpoint data from SentinelOne is automatically displayed in the Awake Security Platform. A security analyst investigating a threat is thus able to make effective risk management decisions with the benefit of network and endpoint context. The optimized and integrated workflow also reduces human errors and minimizes operational overheads from repeated context switches.

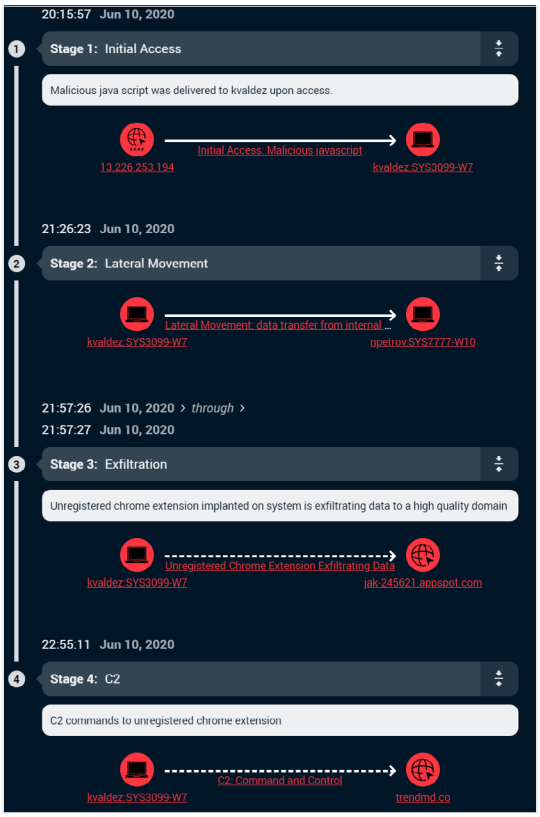
Awake's network visibility picks up devices, users and applications that SentinelOne doesn't see. For example, in a recent attack, Awake discovered an externally accessible IoT device that was compromised and then used for lateral movement to managed endpoints. The threat was discovered and quickly contained.



The Devil in the Details: An Integration Case Study

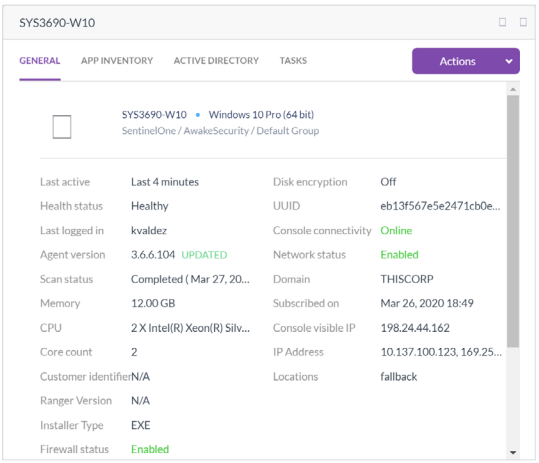
Automatically view a timeline of the breach.

Awake automatically constructs a forensic timeline showing the series of activities flagged for the device in question as well as the broader attack map that identifies the entire kill chain along with other devices, destinations and activities relevant to the investigation.



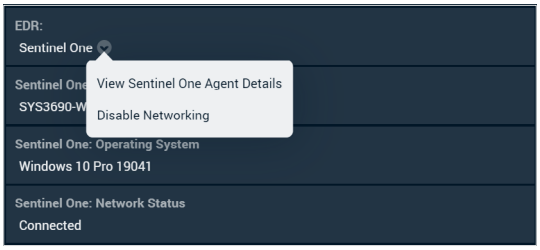
Pivot to SentinelOne.

With one click, view endpoint data such as process listings, registry information and other device specifics. The integration automatically tracks down the correct device in SentinelOne without requiring the analyst to manually search and match timestamps and IP addresses.



Isolate and remediate.

The integration enables one click remediation of endpoints to quarantine the device and prevent lateral movement, command and control and data exfiltration.



Get Started — Set Up the Integration to Get a Holistic View of Your Environment

Setup the integration in two quick steps:

1 Obtain an API key and URL for access to the SentinelOne platform.

2 Awake's customer success handles the rest to turn on the integration.

Pulse Supply
909 Ridgebrook Road.,Sparks,Maryland 21152,USA
TEL : +1-410-583-1701 FAX : +1-410-583-1704
E-mail: sales@pulsesupply.com
https://www.pulsesupply.com/datacom-systems