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–from the network which reveals the entire attack surface, like unmanaged IoT or contractor devices as well as managed endpoints that are often the end-target of the attack. The integration of network and endpoint security enables effective defenses against even the most advanced cyber threats.

The Awake Security Platform, the world's leading advanced network detection and response platform, integrates fully and easily with CrowdStrike Falcon Insight 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 both the managed and unmanaged infrastructure within the enterprise.

Better Together: The Benefits

- Visibility, detection and response for managed and unmanaged devices
- Investigations across the kill chain with endpoint and network context at your fingertips
- 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 NDR Security Division of ARISTA

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.

CROWDSTRIKE

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike® Falcon Insight™ solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

How They Complement Each Other

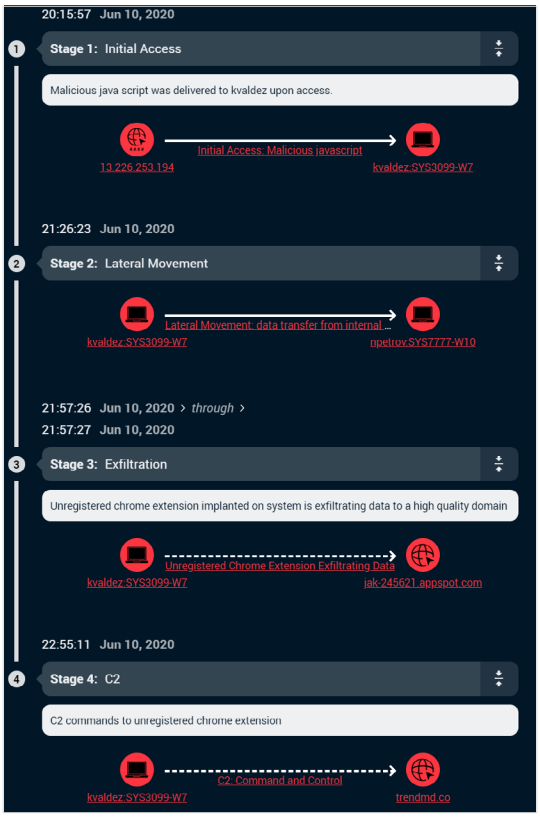
With this integration, endpoint data from Falcon Insight is automatically displayed in the Awake Security Platform. A security analyst investigating a threat is thus able to make effective risk management decisions with the benefit of network and endpoint context. The optimized and integrated workflow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

Awake's network visibility picks up devices, users and applications that are not managed by Falcon Insight. 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

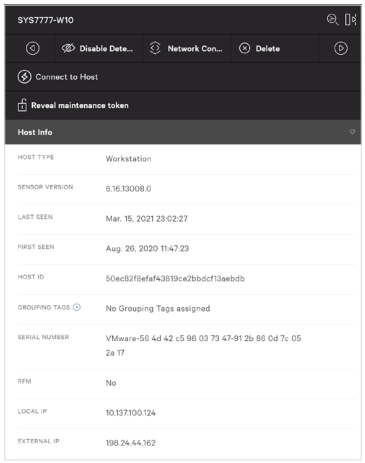
Automatically view a timeline of the breach.

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.



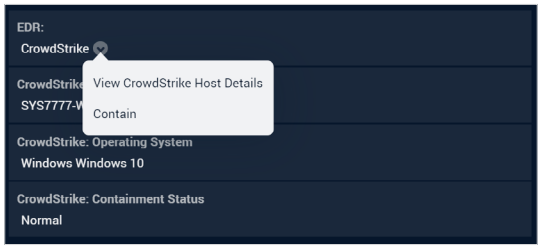
Pivot to Falcon Insight.

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 CrowdStrike 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 CrowdStrike platform.

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

Get Defense-in-Depth with Integrated Endpoint and Network Detection and Response

Schedule A Demo

5453 Great America Pkwy | Santa Clara, CA 95054 | (833) 292-5348 | https://awakesecurity.com