SECURONIX
Security Analytics. Delivered.

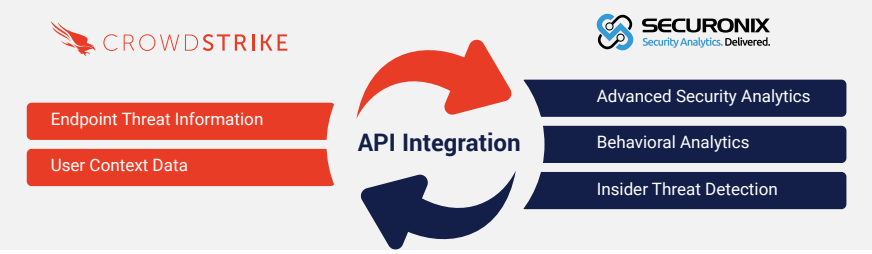
CROWDSTRIKE

SOLUTION BRIEF

Securonix and CrowdStrike Deliver Endpoint Visibility and Protection

The cyber security landscape continues to get more complex. Hackers continue to innovate, business technologies generate increasing amounts of data, and obsolete perimeter defenses struggle with modern insider and cyber threats. Built on big data, Securonix Security Analytics Platform combines log management, security incident and event management (SIEM), and user and entity behavior analytics (UEBA) into a complete, end-to-end platform that can be deployed in its entirety or in flexible, modular components. It collects massive volumes of data in real time, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response. CrowdStrike Falcon endpoint protection unifies the technologies required to successfully stop breaches, including next-generation antivirus, endpoint detection and response, IT hygiene, 24/7 threat hunting, and threat intelligence.

When integrated together, Securonix and CrowdStrike provide continuous breach prevention in a single agent and proactively detect virus, malware, ransomware, and other known and unknown threats. Securonix uses Crowdstrike's Falcon API to gather real-time intelligence from your endpoints. This provides additional context used to assist threat detection and investigation. User behavior information is also used to enrich behavioral analysis.



Endpoint Intelligence Enhanced Security Analytics Stop Unknown Threats

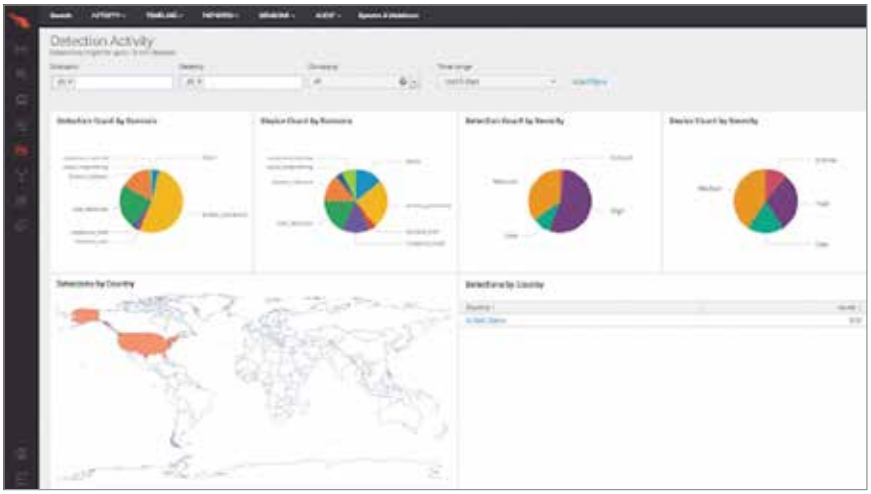
Internal threats are one of the greatest threats organizations face today. They can, knowingly or unknowingly, compromise your systems from the inside. CrowdStrike Falcon endpoint detection addresses the challenge of detecting security compromises due to user activities with their next-generation agent-based firewall combined with their centralized cloud-based platform. While the endpoint agent actively detects and prevents threats, the solution further hunts, anticipates, prepares, and protects systems from newly discovered threats.

Securonix uses CrowdStrike's Falcon API to collect security events in real time and enriches the event with additional data for further analysis. Securonix applies advanced security analytics and machine learning to detect and protect against advanced threats. Combined, Securonix and CrowdStrike provide visibility, analytics, and response protection to mitigate risks related to insider behavior activity.

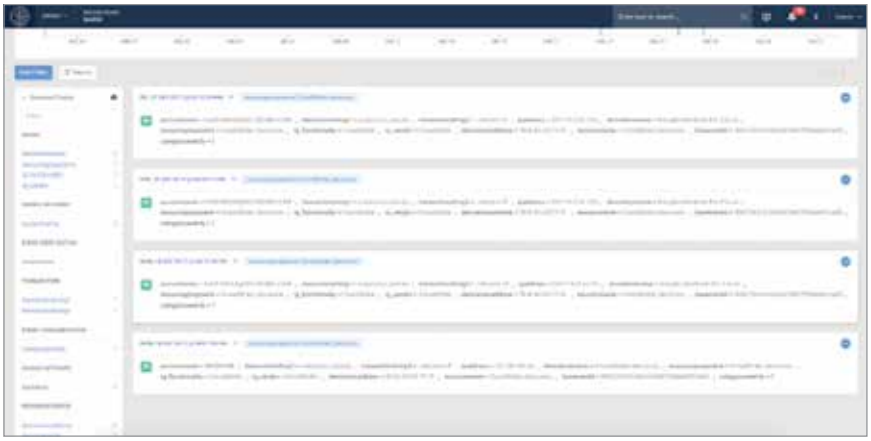
Integration Benefits

- Analyze endpoint threats in the wider context of the organization as a whole in order to identify advanced threats.
- Use endpoint user behavior data to enrich behavioral analysis and add additional depth to your analytics.
- Identify and mitigate risks related to insider behavior activity.
- Proactively detect virus, malware, ransomware, and other known and unknown threats.

By integrating Securonix and Crowdstrike, you gain visibility into endpoint cybersecurity threat patterns, suspicious behavior, malware, and virus detection. You can use automated playbook actions to respond automatically.



CrowdStrike Falcon agent detects a malicious threat on the user's computer and prevents further activity.



Securonix API integration with CrowdStrike Falcon API gathers and enriches the event details. Securonix assigns a risk score on the event and in context of the other user behavior elevates the risk score and can enact predefined threat playbook actions to further mitigate the threat.

How it Works

- Securonix uses the CrowdStrike Falcon API connection to receive security events in real time.
- Securonix behavior analytics uses self-learning to baseline normal behavior patterns in your endpoint data and detects anomalous threats.
- Threats with a risk score above a set threshold can trigger automated playbook responses.
- Securonix uses endpoint data to create data insights and visualize cybersecurity threats, risks, and compliance metrics.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

About CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence, the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. For more information visit www.crowdstrike.com.

SECURONIX
Security Analytics. Delivered.

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix