SECURONIX™ | vmware® Carbon Black

SOLUTION BRIEF

Enrich Endpoint Defense with Securonix and VMware Carbon Black

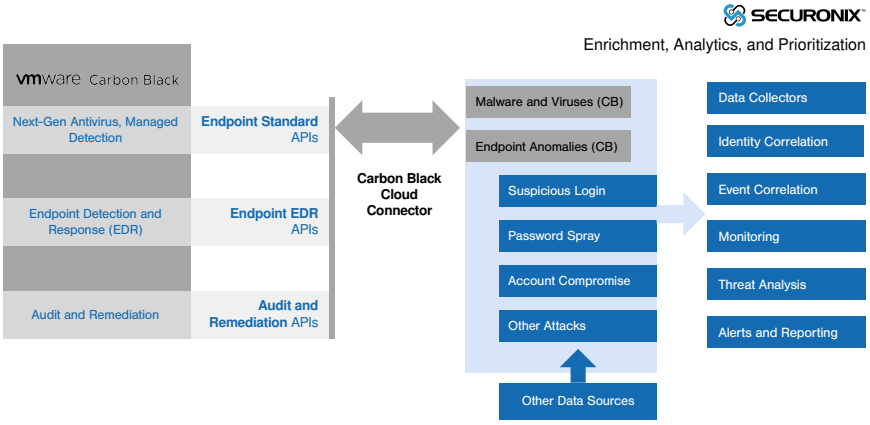
Your security team faces unique challenges in today's data-heavy landscape. Separating insights from noise, handling insider threats, battling alert fatigue, and standardizing incident response procedures all weigh heavily on your security analyst's mind.

Securonix delivers unlimited scale, powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases your security through improved visibility, actionability, and security posture, while reducing management and analyst burden.

Carbon Black Endpoint Detection and Response (EDR) is a comprehensive endpoint security and response solution that combines next-generation antivirus and endpoint detection and response capabilities. Utilizing the threat intelligence available on the VMware Carbon Black Cloud platform, Carbon Black EDR also supports a variety of powerful endpoint security services through a single solution and unified console.

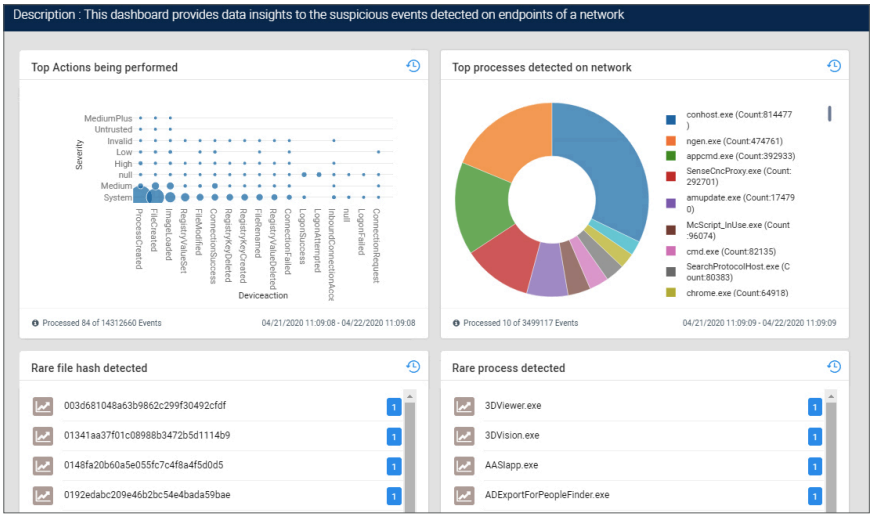
When integrated, Securonix and Carbon Black EDR provides continuous protection and prevention in a single solution. It proactively stops viruses, malware, ransomware, and other non-malware attacks using file heuristics and event correlation to connect related events.

Securonix analyzes intelligence from endpoints gathered by Carbon Black EDR and consumed via Carbon Black APIs. This information provides additional context used by the Securonix platform to perform threat detection and investigation. User behavior information from Carbon Black Defense is also used to enrich behavioral analysis.



Solution Benefits

- Improved protection from known and unknown attacks.
- Full visibility into endpoints to close security gaps.
- Clear alerting of potential threats.
- Easier investigation into security incidents.
- Use endpoint user behavior data to enrich behavioral analysis and add additional depth to predictive analytics.



Securonix provides a real-time updated list of top threats, top violators, watchlists, and more. This provides the security analyst a single pane of glass view of pertinent security threats at their fingertips.

The platform allows the analyst to drilldown into each individual event, providing event information enriched with additional context.

How it Works

- Carbon Black EDR analyzes and identifies malicious activity on endpoints.
- Securonix uses Carbon Black APIs and cloud connectors to gather information about real-time threats.
- Securonix behavior analytics uses self-learning to baseline normal behavior patterns in your endpoint data and detect anomalous threats.
- Securonix uses endpoint data to create data insights and visualize cybersecurity threats, risks, and compliance metrics.

About VMware Carbon Black

VMware Carbon Black is a leading provider of next-generation endpoint security. Deployed via the cloud, on-premises, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information visit www. carbonblack.com.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

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