SECURONIX™
Security Analytics. Delivered.

Carbon Black.

SOLUTION BRIEF

# Enrich Endpoint Defense with Securonix and 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.

Built on big data, the 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.

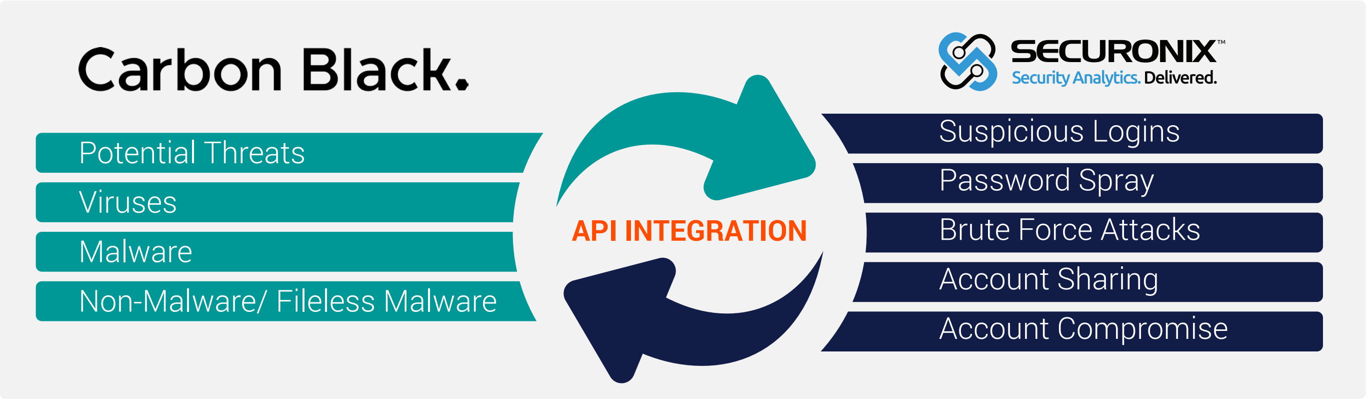
Cb Defense is a cloud-delivered endpoint security solution that combines next-generation antivirus and endpoint detection and response capabilities. Built on the Cb Predictive Security Cloud™ platform, Cb Defense also supports a variety of powerful endpoint security services through a single agent and unified console.

When you integrate Securonix and Cb Defense, they provide continuous protection and prevention in a single agent that proactively stops virus, malware, ransomware, and non-malware (otherwise known as fileless malware) attacks.

In order to provide this, Securonix analyzes intelligence from your endpoints gathered by Cb Defense and consumed via the Carbon Black's API. This information provides additional context used by the Securonix platform to assist threat detection and investigation. User behavior information from Cb Defense is also used to enrich behavioral analysis.

## Integration 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 and predictive analytics.

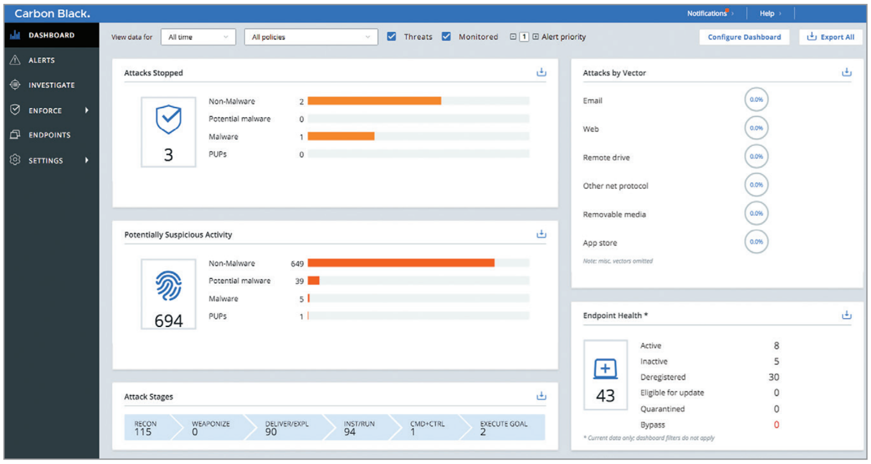

Carbon Black.

Potential Threats
Viruses
Malware
Non-Malware/ Fileless Malware

API INTEGRATION

SECURONIX™
Security Analytics. Delivered.

Suspicious Logins
Password Spray
Brute Force Attacks
Account Sharing
Account Compromise



Carbon Black.

Notifications › | Help ›

- DASHBOARD
- ALERTS
- INVESTIGATE
- ENFORCE ▸
- ENDPOINTS
- SETTINGS ▸

View data for: All time | All policies | ☑ Threats ☑ Monitored ⊟ 1 ⊞ Alert priority | Configure Dashboard | Export All

**Attacks Stopped** — 3

| | |
|---|---|
| Non-Malware | 2 |
| Potential malware | 0 |
| Malware | 1 |
| PUPs | 0 |

**Potentially Suspicious Activity** — 694

| | |
|---|---|
| Non-Malware | 649 |
| Potential malware | 39 |
| Malware | 5 |
| PUPs | 1 |

**Attack Stages**

| RECON | WEAPONIZE | DELIVER/EXPL | INST/RUN | CMD+CTRL | EXECUTE GOAL |
|---|---|---|---|---|---|
| 115 | 0 | 90 | 94 | 1 | 2 |

**Attacks by Vector**

| | |
|---|---|
| Email | 0.0% |
| Web | 0.0% |
| Remote drive | 0.0% |
| Other net protocol | 0.0% |
| Removable media | 0.0% |
| App store | 0.0% |

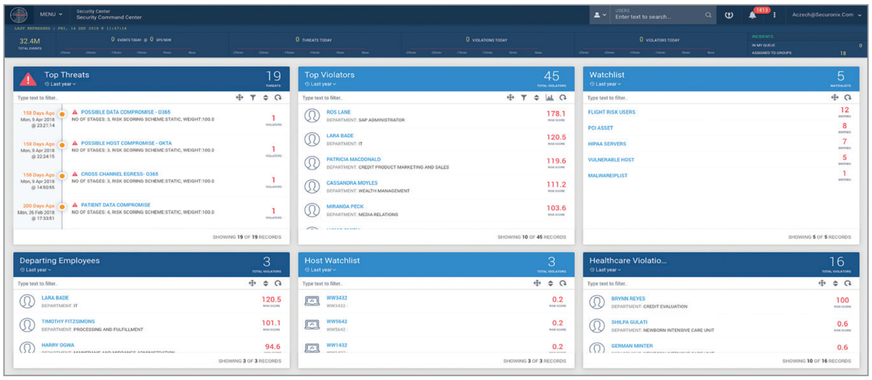
*Note: misc. vectors omitted*

**Endpoint Health *** — 43

| | |
|---|---|
| Active | 8 |
| Inactive | 5 |
| Deregistered | 30 |
| Eligible for update | 0 |
| Quarantined | 0 |
| Bypass | 0 |

** Current data only; dashboard filters do not apply*

Carbon Black's administrative portal provides an overview of malware types along with attacks that have been stopped as well as potential suspicious activity.



MENU | Security Center | Security Command Center

USERS: Enter text to search... | 1813 | Aczech@Securonix.Com

LAST REFRESHED : FRI, 14 SEP 2018 @ 11:47:14

32.4M TOTAL EVENTS | 0 EVENTS TODAY @ 0 EPS NOW | 0 THREATS TODAY | 0 VIOLATIONS TODAY | 0 VIOLATORS TODAY | INCIDENTS: IN MY QUEUE 0, ASSIGNED TO GROUPS 18

**Top Threats** — Last year — 19 THREATS

| | | |
|---|---|---|
| 158 Days Ago<br>Mon, 9 Apr 2018 @ 23:21:14 | POSSIBLE DATA COMPROMISE - O365<br>NO OF STAGES: 3, RISK SCORING SCHEME:STATIC, WEIGHT:100.0 | 1 VIOLATORS |
| 158 Days Ago<br>Mon, 9 Apr 2018 @ 22:24:15 | POSSIBLE HOST COMPROMISE - OKTA<br>NO OF STAGES: 3, RISK SCORING SCHEME:STATIC, WEIGHT:100.0 | 1 VIOLATORS |
| 158 Days Ago<br>Mon, 9 Apr 2018 @ 14:50:55 | CROSS CHANNEL EGRESS- O365<br>NO OF STAGES: 3, RISK SCORING SCHEME:STATIC, WEIGHT:100.0 | 1 VIOLATORS |
| 200 Days Ago<br>Mon, 26 Feb 2018 @ 17:33:51 | PATIENT DATA COMPROMISE<br>NO OF STAGES: 4, RISK SCORING SCHEME:STATIC, WEIGHT:100.0 | 1 VIOLATORS |

SHOWING 19 OF 19 RECORDS

**Top Violators** — Last year — 45 TOTAL VIOLATORS

| | |
|---|---|
| ROS LANE<br>DEPARTMENT: SAP ADMINISTRATOR | 178.1 RISK SCORE |
| LARA BADE<br>DEPARTMENT: IT | 120.5 RISK SCORE |
| PATRICIA MACDONALD<br>DEPARTMENT: CREDIT PRODUCT MARKETING AND SALES | 119.6 RISK SCORE |
| CASSANDRA MOYLES<br>DEPARTMENT: WEALTH MANAGEMENT | 111.2 RISK SCORE |
| MIRANDA PECK<br>DEPARTMENT: MEDIA RELATIONS | 103.6 RISK SCORE |

SHOWING 10 OF 45 RECORDS

**Watchlist** — Last year — 5 WATCHLISTS

| | |
|---|---|
| FLIGHT RISK USERS | 12 ENTITIES |
| PCI ASSET | 8 ENTITIES |
| HIPAA SERVERS | 7 ENTITIES |
| VULNERABLE HOST | 5 ENTITIES |
| MALWAREIPLIST | 1 ENTITIES |

SHOWING 5 OF 5 RECORDS

**Departing Employees** — Last year — 3 TOTAL VIOLATORS

| | |
|---|---|
| LARA BADE<br>DEPARTMENT: IT | 120.5 RISK SCORE |
| TIMOTHY FITZSIMONS<br>DEPARTMENT: PROCESSING AND FULFILLMENT | 101.1 RISK SCORE |
| HARRY OGWA | 94.6 |

SHOWING 3 OF 3 RECORDS

**Host Watchlist** — Last year — 3 TOTAL VIOLATORS

| | |
|---|---|
| WW3432<br>WW3432 : | 0.2 RISK SCORE |
| WW5642<br>WW5642 : | 0.2 RISK SCORE |
| WW1432 | 0.2 |

SHOWING 3 OF 3 RECORDS

**Healthcare Violatio...** — Last year — 16 TOTAL VIOLATORS

| | |
|---|---|
| BRYNN REYES<br>DEPARTMENT: CREDIT EVALUATION | 100 RISK SCORE |
| SHILPA GULATI<br>DEPARTMENT: NEWBORN INTENSIVE CARE UNIT | 0.6 RISK SCORE |
| GERMAN MINTER | 0.6 |

SHOWING 10 OF 16 RECORDS

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

## How it Works

- Cb Defense analyzes and identifies malicious activity on endpoints.
- Securonix uses Carbon Black's RESTful APIs  to gather information about real-time threats.
- Securonix behavior analytics uses self-learning to baseline normal behavior patterns in your endpoint data and detects anomalous threats.
- 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 Carbon Black

Carbon Black is a leading provider of next-generation endpoint security. Deployed via the cloud, on-premise, 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.

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