SmartEvent: Full Threat Visibility

SmartEvent provides Full Threat Visibility with a single view into security risks. Take control and command the security event through real-time forensic and event investigation, compliance and reporting. Respond to security incidents immediately and gain network true insights.

Key Features and Benefits

- **Instant Search Results**: Free text search, auto suggestion and search history favorites
- **Single View into Security Risk**: R80.10 integrated threat management and performance
- **Customizable Views and Reports**: Security events automatically alert on critical events

---

“Check Point Solutions prevent threats of all kinds when users unknowingly access malicious resources, completely eliminating the very possibility of damage or data breach.

Check Point products stood out among the competitors for their ease of configuration, a user-friendly interface and the ability to prevent threats from entering the network.”

— Sergey Rysin, Security Advisor to STLC Director
TOP TIER REPORTING

Threat Prevention

Executive Summary

Malwares and Attacks

Key Findings: Data Loss

Machines Infected with Bots

Key Findings: Malware and Attacks

© 2018 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content
March 21, 2018
CORRELATION
Real-Time Forensic and Event Investigation

- SmartEvent correlates logs from all Check Point enforcement points, including endpoints, to identify suspicious activity, track trends and investigate/mitigate events – all through a single pane of glass.

- Real-time data analysis and custom event logs immediately notify administrators to allow for quick action and/or remediation. Take control of your security.

- Deploys quickly and monitors anywhere, SmartEvent is completely modular and customizable. Consisting of widgets, views and reports you can create your own or use any Check Point predefined reports.
SmartEvent: Full Threat Visibility

With one console, security teams can manage all aspects of security from policy to threat prevention – across the entire organization – on both physical and virtual environments. Consolidated management means increased operational efficiency.

Full Threat Visibility

Real Time Forensic and Threat Investigation

Correlation of millions of logs to identify significant events easily and understand your security status and trends.

From View to Action

Drill down directly from the event your viewing to the immediate rule in the policy. All through a single pane of glass.

Schedule Reports for any Audience

Take control and monitor all your gateways in real time. Add customized or predefined views to your reports, schedule anytime, and featuring one click export to PDF and Excel.

Step Up to 5th Generation Cyber Security

Gen V security leaves the patch work and best-of-breed deployments of the past behind. Instead, it’s characterized by an architecture that unifies all networks, cloud, and mobile, supported by automatic and immediate threat intelligence.

Integrated Threat Management

Utilize the power of R80.10 single management console – Nothing goes undetected.

KEY FINDINGS • HIGH RISK WEB ACCESS

<table>
<thead>
<tr>
<th>WEBSITE</th>
<th>Application Name</th>
<th>URL</th>
<th>Mobile</th>
<th>Internet</th>
<th>High Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>2322 Yahoo Search</td>
<td><a href="http://www.yahoo.com">www.yahoo.com</a></td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>Google</td>
<td>2330 Google Search</td>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>Facebook</td>
<td>2332 Facebook Login</td>
<td>login.facebook.com</td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>Amazon</td>
<td>2331 Amazon Home Page</td>
<td><a href="http://www.amazon.com">www.amazon.com</a></td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>Twitter</td>
<td>2333 Twitter Home Page</td>
<td><a href="http://www.twitter.com">www.twitter.com</a></td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
</tr>
</tbody>
</table>

3.6GB Total high risk web applications traffic

Top 5 high risk app sources

- Yahoo: 2322 Yahoo Search
- Google: 2330 Google Search
- Facebook: 2332 Facebook Login
- Amazon: 2331 Amazon Home Page
- Twitter: 2333 Twitter Home Page

*Risk level indicates an illegal top that can bypass security or fail detection. Be sure it indicates an application that can cause data manager or measure checking via how user knowledge.

© 2018 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content March 21, 2018
ORDERING DEDICATED SMART-1 SMARTEVENT APPLIANCES

<table>
<thead>
<tr>
<th>Smart-1 Appliances¹</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Smart-1 405</strong></td>
<td>CPAP-NGSM405-EVNT</td>
</tr>
<tr>
<td>Smart-1 405 Appliance, dedicated SmartEvent for 5 gateways (perpetual)</td>
<td></td>
</tr>
<tr>
<td><strong>Smart-1 410</strong></td>
<td>CPAP-NGSM410-EVNT</td>
</tr>
<tr>
<td>Smart-1 410 Appliance, dedicated SmartEvent for 10 gateways (perpetual)</td>
<td></td>
</tr>
<tr>
<td><strong>Smart-1 525</strong></td>
<td>CPAP-NGSM525-EVNT</td>
</tr>
<tr>
<td>Smart-1 525 Appliance, dedicated SmartEvent for 25 gateways (perpetual)</td>
<td></td>
</tr>
<tr>
<td><strong>Smart-1 5050</strong></td>
<td>CPAP-NGSM5050-EVNT</td>
</tr>
<tr>
<td>Smart-1 5050 Appliance, dedicated SmartEvent for 50 gateways (perpetual)</td>
<td></td>
</tr>
<tr>
<td><strong>Smart-1 5150</strong></td>
<td>CPAP-NGSM5150-EVNT</td>
</tr>
<tr>
<td>Smart-1 5150 Appliance, dedicated SmartEvent for 150 gateways (perpetual)</td>
<td></td>
</tr>
</tbody>
</table>

¹ SmartEvent for one year and extensions are available in the integrated Smart-1 Appliance policy management SKUs.

**SmartEvent perpetual dedicated server**, for customers who want a dedicated SmartEvent environment:
- Includes SmartEvent, Logs and correlation unit.
- Perpetual on Smart-1 and open servers.
- The dedicated SmartEvent server is licensed by the number of gateways it is analyzing logs from.
- Number of managed gateways on the dedicated SmartEvent server may be equal to or less than the number of managed gateways on the Security Management server.

**SPECIFICATIONS**

**Smart-1 SmartEvent Configuration**

<table>
<thead>
<tr>
<th>Appliances</th>
<th>Enterprise Grade</th>
<th>Ultra High End</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>405</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>410</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>525</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>5050</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5150</td>
<td></td>
</tr>
</tbody>
</table>

**Capacity & Performance**

- Managed Gateways: 5, 10, 25, 50, 150+ ¹
- Peak Indexed Logs per Sec: 400, 600, 1600, 7,500, 12,000
- Sustained Indexed Logs per Sec: 200, 300, 800, 3,750, 6,000
- Log Size per Day (GB): 0.36, 0.55, 1.5, 6.8, 11

**Hardware Specifications**

- Cores: 4, 4, 4, 16, 24
- Storage (HDD) Hot-Swappable: 1x 1 TB, 1x 2 TB, 2x 4 TB, 4x 4 TB (default 6x 4TB)
- RAID Type: - , 1
- Memory (RAM) Default/Max: 16 GB, 32 GB, 32/64 GB, 64/128 GB, 128/256 GB

¹ Manages up to 5000 Check Point 1400 Appliances