CHECK POINT NEXT GENERATION SMARTEVENT

CHECK POINT NEXT GENERATION SMARTEVENT

Complete threat visibility to better understand, prioritize and respond to critical security events

Product Benefits

- Quickly isolate real threats in real-time
- Minimizes amount of data to be reviewed
- Enables quick action to mitigate threats
- Constant monitoring helps improve security posture
- Helps keep stakeholders abreast of security status

Product Features

- Searches & analyzes millions of logs per second to identify critical events
- Correlates data from network and endpoint logs to catch suspicious activity
- Custom views and reports
- Enhanced, free text search
- Easy deployment

INSIGHTS

Today's security is complex, requiring multiple devices to cover the network. These devices generate voluminous amounts of logs. In a typical enterprise, an intrusion detection system alone can produce more than 500,000 messages a day and firewalls can generate millions of log records a day.

It is not humanly possible to scan all this data and even with automated log analysis, it is time-consuming to identify critical security incidents and to investigate them. To add to the challenge, data collected by different devices often do not provide a complete picture of one's security posture. What appears to be normal behavior when viewed on its own, may reveal evidence of abnormal activity when that data is cross-correlated and analyzed.

And given that everyone is a target these days, how do you know if you have been compromised? And what will you do if you are?

SOLUTION

By automating the aggregation and correlation of raw log data, we drastically reduce the amount of data you have to review so you can quickly isolate the real security threats. Because we aggregate data from all Check Point gateways and endpoints, we detect patterns that might otherwise go un-noticed.

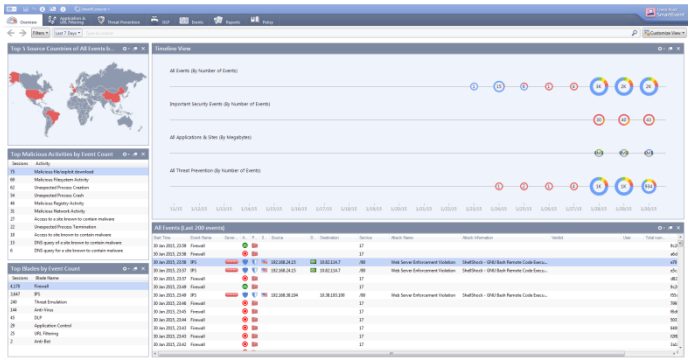
SmartEvent also consolidates monitoring, logging, reporting and event analysis functions within the same console. This means you can easily move from tracking trends to investigating and mitigating events with just a few clicks. If you are worried about a new malware that is making the rounds, our free-text search lets you quickly see if any instance of it was discovered on your network. Need to send reports to your manager or auditor? It's a breeze to set up custom reports in SmartEvent.

With SmartEvent, your security team can *focus* on the threats that pose the greatest risk to your business – rather than drown in data.

CUSTOMIZE YOUR SECURITY

Is there a real threat and what is the scope?

Next Generation SmartEvent allows you to create custom dashboards to monitor only what is relevant to your organization. Widgets and chart templates optimize visual display, making security data easy to understand at a glance.



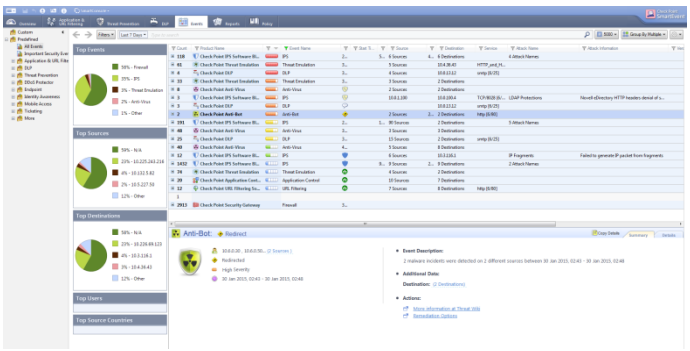
How do I stop it from happening again?

You can take advantage of pre-defined security events or customize them to prioritize events so automatic alerts are generated alerts for noteworthy, critical events.

EASILY INVESTIGATE EVENTS

Did that malware hit my network?

SmartEvent enables one-click exploration of security events. With one click, move from a high-level overview to specific details such as type of attack, timeline, application type and source. Free-text search allows you to enter specific search terms to retrieve results from millions of logs in seconds.



RESPOND & REMEDIATE ON THE SPOT

What do I do now to respond to that critical event?

With SmartEvent, once you have investigated an event, it's easy to act on it. Depending on the severity of the event, you can choose to ignore it, act on it later, or block it immediately. You can also easily toggle over to the rules associated with the event to refine your policy.

PERSONALIZED REPORTS

SmartEvent make it easy to customize reports for the different stakeholders in your company. Your CISO might need an overview of high risk events in the last month, while your HR Manager might need to know where employees are going online. With SmartEvent, your reports display only content that is relevant to each stakeholder.

COMPREHENSIVE DATA CORRELATION

SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously.

DEPLOY QUICKLY, MONITOR ANYWHERE

With a large number of pre-defined, but easily customizable security events, you can have SmartEvent up and running and detecting threats in a matter of hours.

And, you can stay on top of security while on the go. The Next Generation SmartEvent web portal provides access to reports and dashboard data via mobile phones and tablet devices.

SMART-1 EVENT APPLIANCES

Smart-1 Appliances	205	210	225	3050	3150
					
Managed Gateways	5	10	25	50	150+
Storage (HDD)	1 x 1 TB	1 x 2 TB	2 x 2 TB	4 x 2 TB	Up to 12 x 2 TB (default 6 x 2TB)
Event logs/Day	350K	650K	1.3M	4M	10M
Logs/Day (GB)	3.5	6.5	13	40	100
Maximum Users	900	1,600	3,000	10,000	25,000

Next Generation SmartEvent is also available as a software blade package on open servers.