Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SOLUTION DESCRIPTION

Check Point SmartLog transforms data into security intelligence with split-second searches that provide instant visibility into billions of log records over multiple time periods and domains all from Check Point's unified security management console.

Check Point SmartLog

included in the Logging and Status Software Blade

Transforms Data into Security Intelligence

YOUR CHALLENGE

Security systems track every activity within a network, and then generate log records that can be used like an audit trail to analyze real-time security events, or review in bulk later. Collecting log records provides visibility into what's happening in dynamic networks, enabling the ability to track suspicious behavior and prevent security incidents, support forensics analysis and meet compliance regulations. Security managers are under constant pressure to manage, sort and analyze an explosion of data (up to 100 gigabytes per day in large companies), searching for security events or breaches, all while monitoring the performance of the security system itself. But running queries and searching millions of log records can take hours from traditional log management systems. However without effective log management, companies ignore the intelligence provided by their own environments and ultimately expose their networks to unbridled security events.

OUR SOLUTION

SmartLog, part of the Logging and Status Software Blade and unified security management console, enables enterprises to centrally track log records and security activity across all Software Blades with split-second Google-like search results that provides instant visibility over billions of log records. The intuitive search box delivers real-time search results from any log field displaying top-down results, saving security administrators valuable time. Administrators can search multiple log files, time periods, gateways and domains, or search by action, user, time or geography for powerful granular security investigation. The Logging and Status Software Blade transforms data into security intelligence with real-time visibility over billions of log records from a single, integrated security management console.

SOLUTION HIGHLIGHTS

- SmartLog next generation log analyzer
- Simple and intuitive Google-like search experience
- Real-time visibility and troubleshooting ability
- Easy to deploy
- Powerful, easy to use queries
- Fully integrated with Check Point's unified security management console

SOLUTION BENEFITS

- Split-second search results from any log field
- Granular searches for any communication or traffic pattern
- Fast, easy-to-read top statistical results
- Tuned for large-scale environments
- Reduced troubleshooting time with real-time results
- No log limits—only limited by disk size

softwareblades™

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

COMPREHENSIVE LOG MANAGEMENT

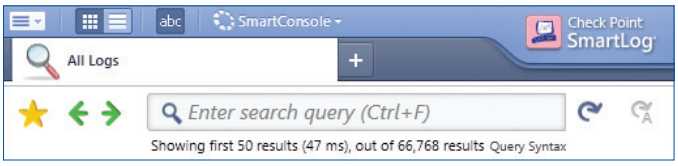
Check Point SmartLog transforms data into security intelligence with split-second searches that provide instant visibility into billions of log records with:

Next Generation Log Analyzer

SmartLog is a powerful, easy to use Log Management tool that reads logs generated by Check Point and OPSEC log-generating products and indexes them for split-second searches that provide instant visibility into billions of log records over multiple log files and types.

Simple and Intuitive Google-like Search Experience

SmartLog offers simple and intuitive Google-like searches that provide visibility into billions of log records. Text search is available from any log field with split-second results in top statistical display.



Simple and intuitive Google-like Search experience

Proactive Security Investigation

Search for any communication pattern over multiple log files, time periods, gateways and domains for proactive security investigation. Search results can be queried to a single log record and can be saved for future use to easily monitor suspicious behaviors.

Powerful, Easy to use Queries

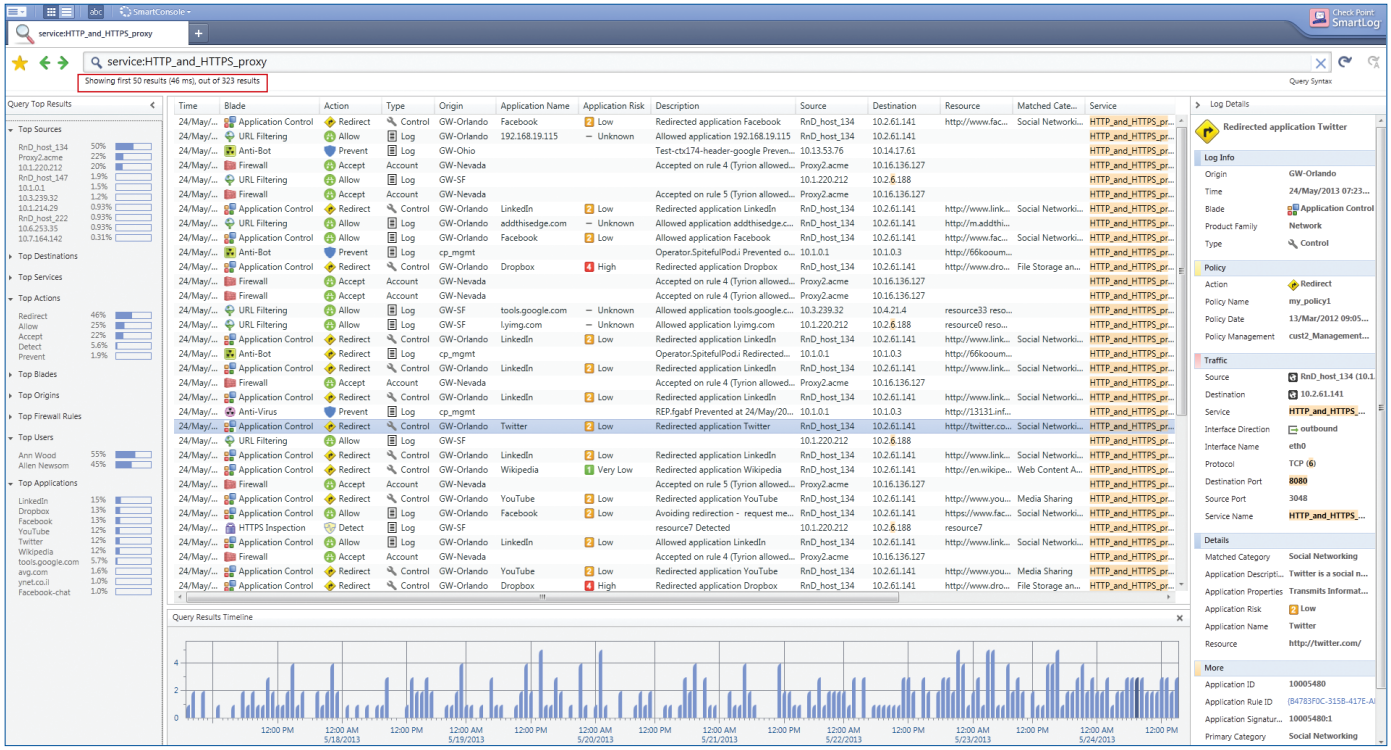
SmartLog comes with many predefined queries that are ready to run right out of the box. You can also create your own custom queries and save them for future use. SmartLog indexing enables queries to instantly analyze millions of logs and display the most relevant results in just one second.

Ease of Deployment

SmartLog is part of the SmartConsole suite, available at no extra charge with the Logging and Status Software Blade, R75.40 and later. No additional configuration is necessary—administrators simply enable SmartLog on their management or log server, saving time and reducing costs by leveraging existing security systems.

Integral Component of Check Point Security Management

SmartLog is an integral component of Check Point Security Management Systems. Check Point's unified security management system enables centralized tracking for all software blades from one console. SmartLog and the Logging and Status Software Blade can be easily activated on existing Check Point Security Gateways and Management Servers saving time and reducing costs by leveraging existing security infrastructure.

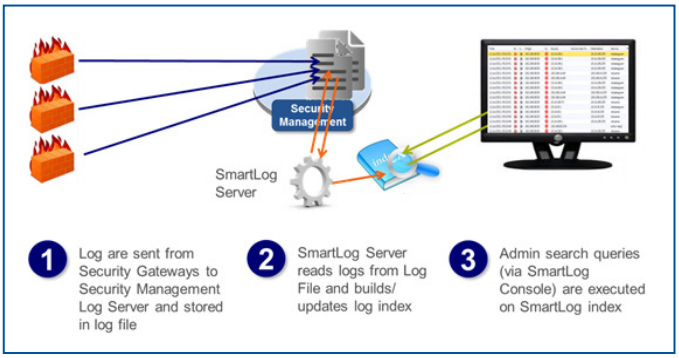


SmartLog displays split-second Search Results

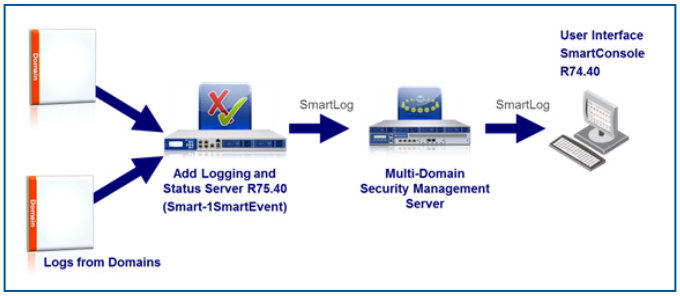
softwareblades™

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

How SmartLog Works



How SmartLog Works in Large Mulit-Domain Environments



SmartLog Sizing for Smart-1 Appliances

Sizing Guidelines - Logs per Day with 1 Month Retention

	Smart-1 5	Smart-1 25	Smart-1 50
Managed gateways	5-25	25-50	50-150
Device storage	500GB	2x1TB (RAID 1)	4x1TB (RAID 10)
Daily log capacity without SmartLog	2GB	12GB	25GB
Daily log capacity with SmartLog	3.6GB	21.6GB	45GB
SmartLog retention period*	1 Month	1 Month	1 Month

* Logging capacity refers to logs plus SmartLog indexes

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

October 15, 2013