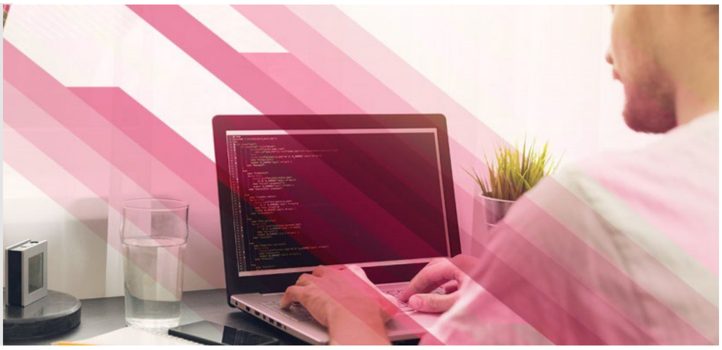
SMARTEVENT: FULL THREAT VISIBILITY

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 to prevent the next attack.



SmartEvent
Full Threat Visibility

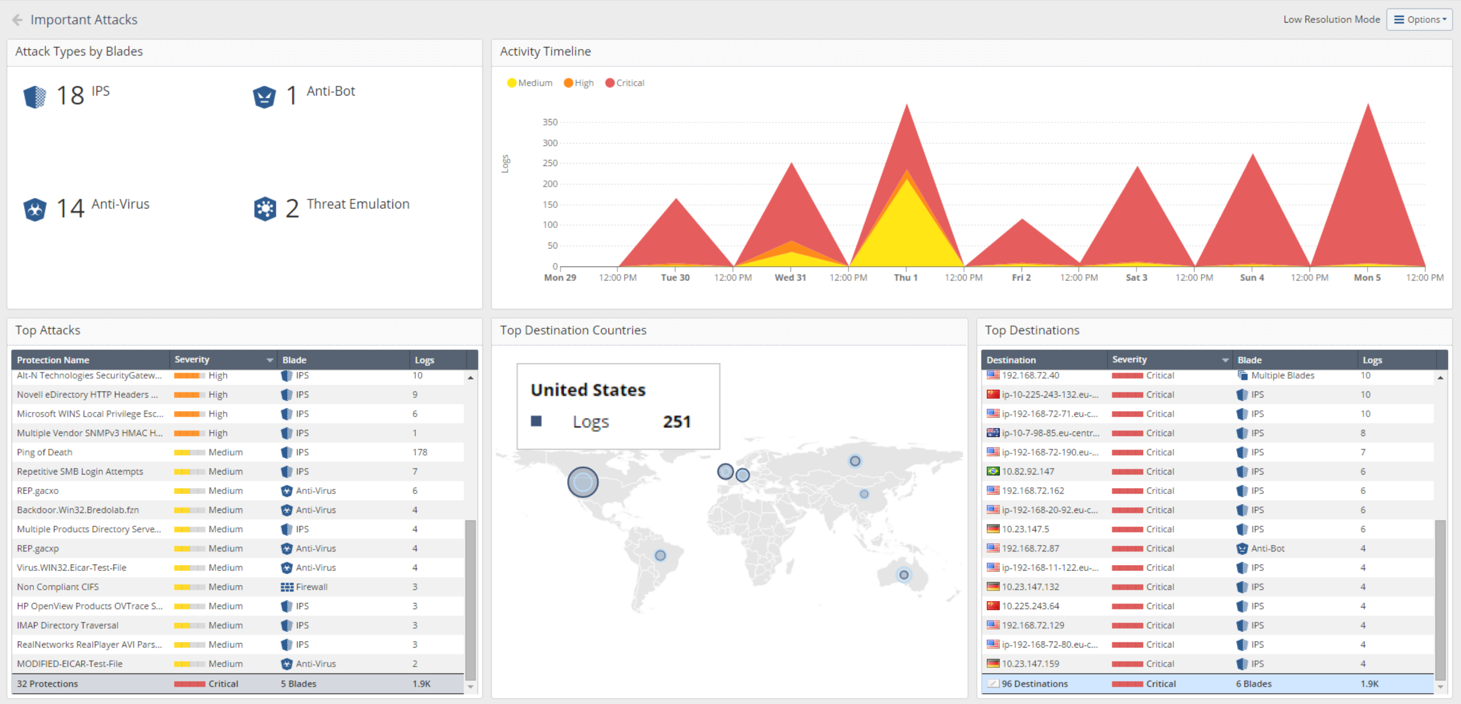
Key Features and Benefits

- **Instant Search Results**: Free text search, auto suggestion and search history favorites
- **Single View into Security Risk**: R81 integrated threat management and performance
- **Customizable Views and Reports**: Security events automatically alert on critical events

FULL THREAT VISIBILITY

REAL-TIME FORENSIC AND EVENT INVESTIGATION

COMMAND THE SECURITY EVENT



Attack Types by Blades

18 IPS	1 Anti-Bot
14 Anti-Virus	2 Threat Emulation

Top Attacks

Protection Name	Severity	Blade	Logs
Alt-N Technologies SecurityGatew...	High	IPS	10
Novell eDirectory HTTP Headers ...	High	IPS	9
Microsoft WINS Local Privilege Esc...	High	IPS	6
Multiple Vendor SNMPv3 HMAC H...	High	IPS	1
Ping of Death	Medium	IPS	178
Repetitive SMB Login Attempts	Medium	IPS	7
REP.gacxo	Medium	Anti-Virus	6
Backdoor.Win32.Bredolab.fzn	Medium	Anti-Virus	4
Multiple Products Directory Serve...	Medium	IPS	4
REP.gacxp	Medium	Anti-Virus	4
Virus.WIN32.Eicar-Test-File	Medium	Anti-Virus	4
Non Compliant CIFS	Medium	Firewall	3
HP OpenView Products OVTrace S...	Medium	IPS	3
IMAP Directory Traversal	Medium	IPS	3
RealNetworks RealPlayer AVI Pars...	Medium	IPS	3
MODIFIED-EICAR-Test-File	Medium	Anti-Virus	2
32 Protections	Critical	5 Blades	1.9K

Top Destinations

Destination	Severity	Blade	Logs
192.168.72.40	Critical	Multiple Blades	10
ip-10-225-243-132.eu-...	Critical	IPS	10
ip-192-168-72-71.eu-c...	Critical	IPS	10
ip-10-7-98-85.eu-centr...	Critical	IPS	8
ip-192-168-72-190.eu-...	Critical	IPS	7
10.82.92.147	Critical	IPS	6
192.168.72.162	Critical	IPS	6
ip-192-168-20-92.eu-c...	Critical	IPS	6
10.23.147.5	Critical	IPS	6
192.168.72.87	Critical	Anti-Bot	4
ip-192-168-11-122.eu-...	Critical	IPS	4
10.23.147.132	Critical	IPS	4
10.225.243.64	Critical	IPS	4
192.168.72.129	Critical	IPS	4
ip-192-168-72-80.eu-c...	Critical	IPS	4
10.23.147.159	Critical	IPS	4
96 Destinations	Critical	6 Blades	1.9K

> *“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

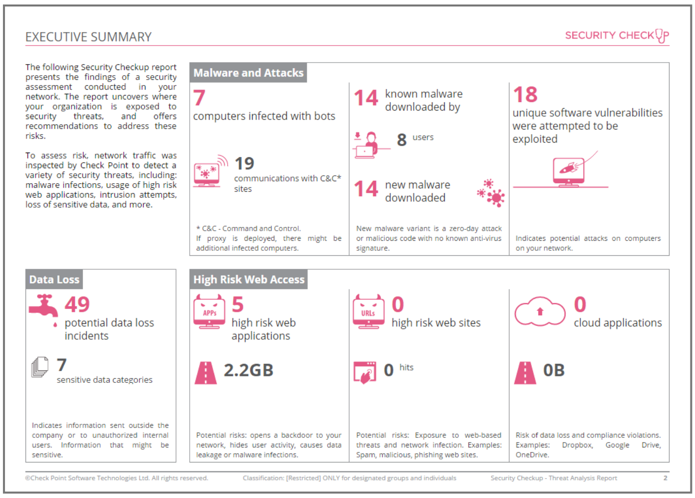
Check Point SOFTWARE TECHNOLOGIES LTD.

THREAT PREVENTION

Report

Feb 14, 2018 12:00 AM - Feb 21, 2018 6:15 PM

Threat Prevention


EXECUTIVE SUMMARY

SECURITY CHECKUP

The following Security Checkup report presents the findings of a security assessment conducted in your network. The report uncovers where your organization is exposed to security threats, and offers recommendations to address these risks.

To assess risk, network traffic was inspected by Check Point to detect a variety of security threats, including: malware infections, usage of high risk web applications, intrusion attempts, loss of sensitive data, and more.

Malware and Attacks

7 computers infected with bots

19 communications with C&C* sites

* C&C - Command and Control.
If proxy is deployed, there might be additional infected computers.

14 known malware downloaded by

8 users

14 new malware downloaded

New malware variant is a zero-day attack or malicious code with no known anti-virus signature.

18 unique software vulnerabilities were attempted to be exploited

Indicates potential attacks on computers on your network.

Data Loss

49 potential data loss incidents

7 sensitive data categories

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive.

High Risk Web Access

5 high risk web applications

2.2GB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

0 high risk web sites

0 hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

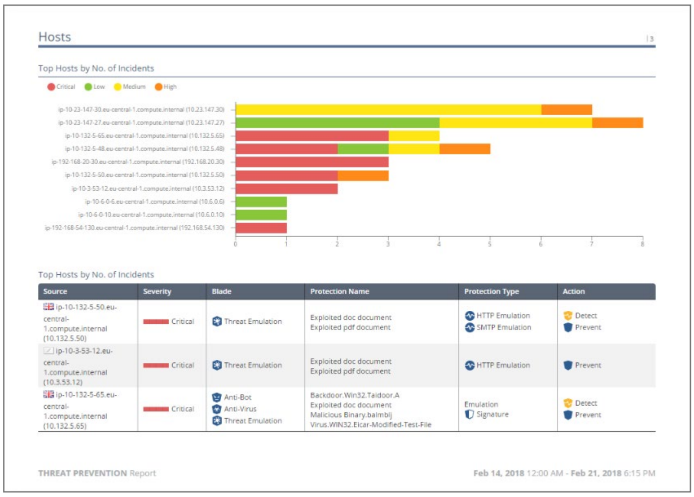
0 cloud applications

0B

Risk of data loss and compliance violations. Examples: Dropbox, Google Drive, OneDrive.

©Check Point Software Technologies Ltd. All rights reserved. Classification: [Restricted] ONLY for designated groups and individuals Security Checkup - Threat Analysis Report 2

Executive Summary


Hosts | 3

Top Hosts by No. of Incidents

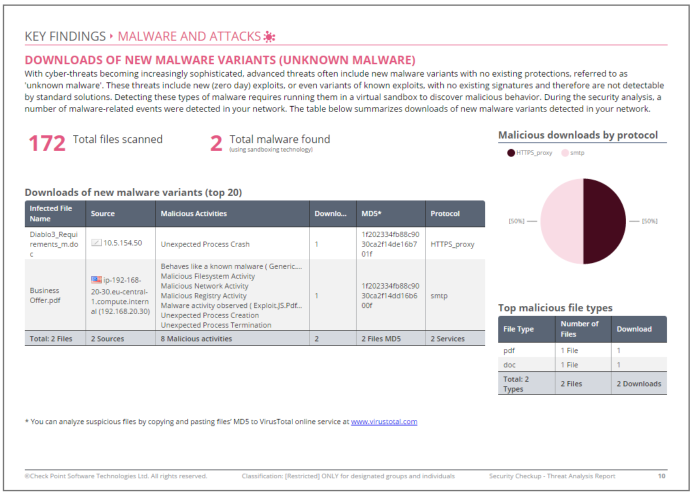
● Critical ● Low ● Medium ● High
ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)
ip-10-23-147-27.eu-central-1.compute.internal (10.23.147.27)
ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)
ip-10-132-5-48.eu-central-1.compute.internal (10.132.5.48)
ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)
ip-10-132-5-50.eu-central-1.compute.internal (10.132.5.50)
ip-10-3-53-12.eu-central-1.compute.internal (10.3.53.12)
ip-10-6-0-6.eu-central-1.compute.internal (10.6.0.6)
ip-10-6-0-10.eu-central-1.compute.internal (10.6.0.10)
ip-192-168-54-130.eu-central-1.compute.internal (192.168.54.130)
0 1 2 3 4 5 6 7 8

Top Hosts by No. of Incidents

Source	Severity	Blade	Protection Name	Protection Type	Action
ip-10-132-5-50.eu-central-1.compute.internal (10.132.5.50)	Critical	Threat Emulation	Exploited doc document Exploited pdf document	HTTP Emulation SMTP Emulation	Detect Prevent
ip-10-3-53-12.eu-central-1.compute.internal (10.3.53.12)	Critical	Threat Emulation	Exploited doc document Exploited pdf document	HTTP Emulation	Prevent
ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	Critical	Anti-Bot Anti-Virus Threat Emulation	Backdoor.Win32.Taidoor.A Exploited doc document Malicious Binary.balmbij Virus.WIN32.Eicar-Modified-Test-File	Emulation Signature	Detect Prevent

THREAT PREVENTION Report Feb 14, 2018 12:00 AM - Feb 21, 2018 6:15 PM

Hosts


KEY FINDINGS ‣ MALWARE AND ATTACKS

DOWNLOADS OF NEW MALWARE VARIANTS (UNKNOWN MALWARE)

With cyber-threats becoming increasingly sophisticated, advanced threats often include new malware variants with no existing protections, referred to as 'unknown malware'. These threats include new (zero day) exploits, or even variants of known exploits, with no existing signatures and therefore are not detectable by standard solutions. Detecting these types of malware requires running them in a virtual sandbox to discover malicious behavior. During the security analysis, a number of malware-related events were detected in your network. The table below summarizes downloads of new malware variants detected in your network.

172 Total files scanned

2 Total malware found (using sandboxing technology)

Downloads of new malware variants (top 20)

Infected File Name	Source	Malicious Activities	Downlo...	MD5*	Protocol
Diablo3_Requirements_m.doc	10.5.154.50	Unexpected Process Crash	1	1f202334fb88c9030ca2f14de16b701f	HTTPS_proxy
Business Offer.pdf	ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	Behaves like a known malware (Generic.... Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware activity observed (Exploit.JS.Pdf... Unexpected Process Creation Unexpected Process Termination	1	1f202334fb88c9030ca2f14dd16b600f	smtp
Total: 2 Files	2 Sources	8 Malicious activities	2	2 Files MD5	2 Services

Malicious downloads by protocol

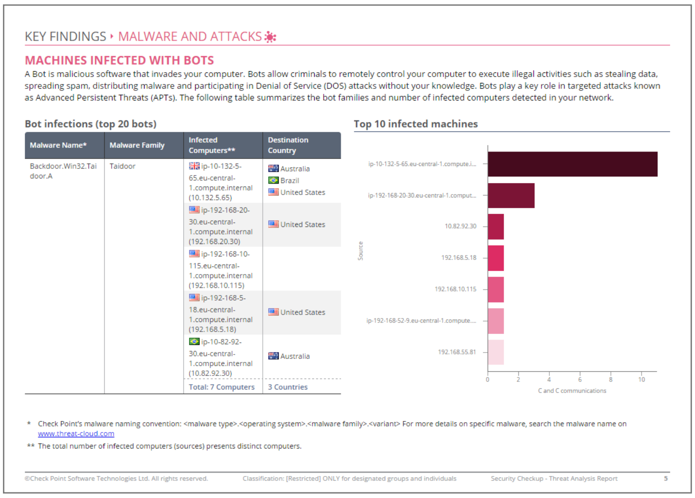
Top malicious file types

File Type	Number of Files	Download
pdf	1 File	1
doc	1 File	1
Total: 2 Types	2 Files	2 Downloads

* You can analyze suspicious files by copying and pasting files' MD5 to VirusTotal online service at www.virustotal.com

©Check Point Software Technologies Ltd. All rights reserved. Classification: [Restricted] ONLY for designated groups and individuals Security Checkup - Threat Analysis Report 10

Malwares and Attacks


KEY FINDINGS ‣ MALWARE AND ATTACKS

MACHINES INFECTED WITH BOTS

A Bot is malicious software that invades your computer. Bots allow criminals to remotely control your computer to execute illegal activities such as stealing data, spreading spam, distributing malware and participating in Denial of Service (DOS) attacks without your knowledge. Bots play a key role in targeted attacks known as Advanced Persistent Threats (APTs). The following table summarizes the bot families and number of infected computers detected in your network.

Bot infections (top 20 bots)

Malware Name*	Malware Family	Infected Computers**	Destination Country
Backdoor.Win32.Taidoor.A	Taidoor	ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)	Australia Brazil United States
		ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	United States
		ip-192-168-10-115.eu-central-1.compute.internal (192.168.10.115)	
		ip-192-168-5-18.eu-central-1.compute.internal (192.168.5.18)	United States
		ip-10-82-92-30.eu-central-1.compute.internal (10.82.92.30)	Australia
		Total: 7 Computers	3 Countries

Top 10 infected machines

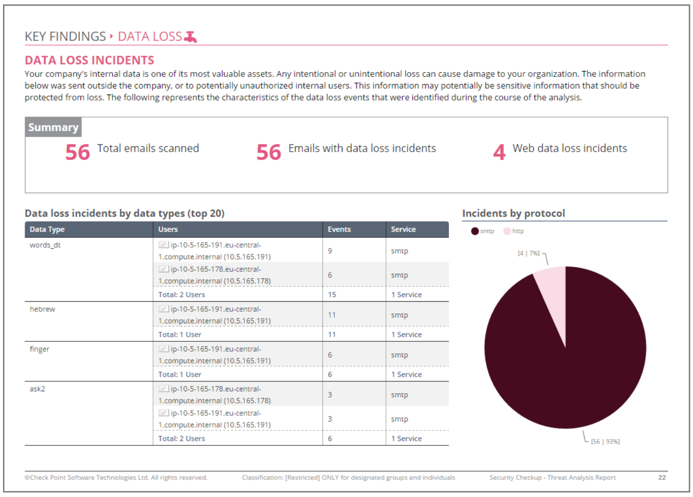
Source
ip-10-132-5-65.eu-central-1.compute.i...
ip-192-168-20-30.eu-central-1.comput...
10.82.92.30
192.168.5.18
192.168.10.115
ip-192-168-52-9.eu-central-1.compute....
192.168.55.81
0 2 4 6 8 10
C and C communications

* Check Point's malware naming convention: <malware type>.<operating system>.<malware family>.<variant> For more details on specific malware, search the malware name on www.threat-cloud.com

** The total number of infected computers (sources) presents distinct computers.

©Check Point Software Technologies Ltd. All rights reserved. Classification: [Restricted] ONLY for designated groups and individuals Security Checkup - Threat Analysis Report 5

Machines Infected with Bots


KEY FINDINGS ‣ DATA LOSS

DATA LOSS INCIDENTS

Your company's internal data is one of its most valuable assets. Any intentional or unintentional loss can cause damage to your organization. The information below was sent outside the company, or to potentially unauthorized internal users. This information may potentially be sensitive information that should be protected from loss. The following represents the characteristics of the data loss events that were identified during the course of the analysis.

Summary

56 Total emails scanned

56 Emails with data loss incidents

4 Web data loss incidents

Data loss incidents by data types (top 20)

Data Type	Users	Events	Service
words_dt	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	9	smtp
	ip-10-5-165-178.eu-central-1.compute.internal (10.5.165.178)	6	smtp
	Total: 2 Users	15	1 Service
hebrew	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	11	smtp
	Total: 1 User	11	1 Service
finger	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	6	smtp
	Total: 1 User	6	1 Service
ask2	ip-10-5-165-178.eu-central-1.compute.internal (10.5.165.178)	3	smtp
	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	3	smtp
	Total: 2 Users	6	1 Service

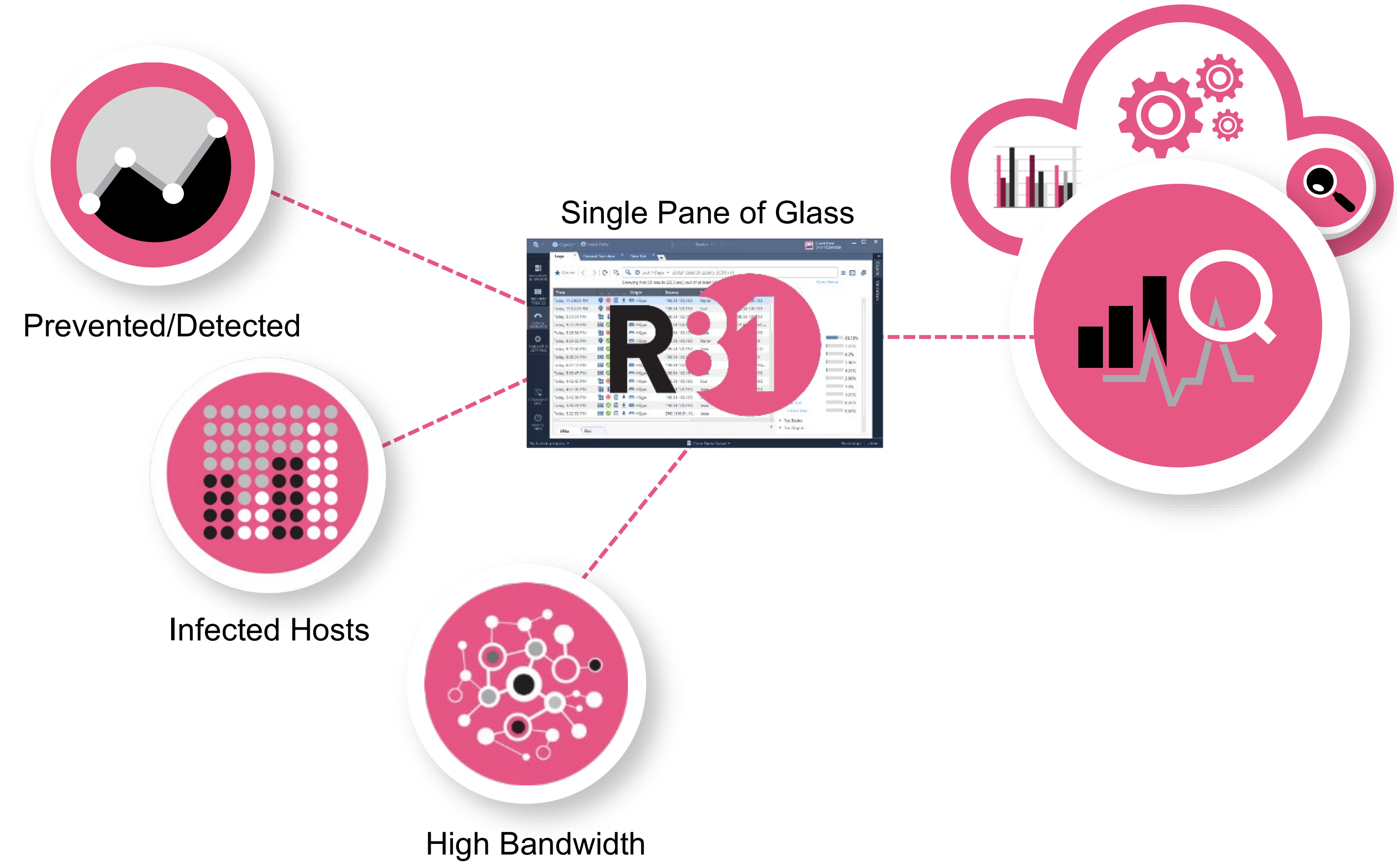
Incidents by protocol

©Check Point Software Technologies Ltd. All rights reserved. Classification: [Restricted] ONLY for designated groups and individuals Security Checkup - Threat Analysis Report 22

Key Findings: Data Loss

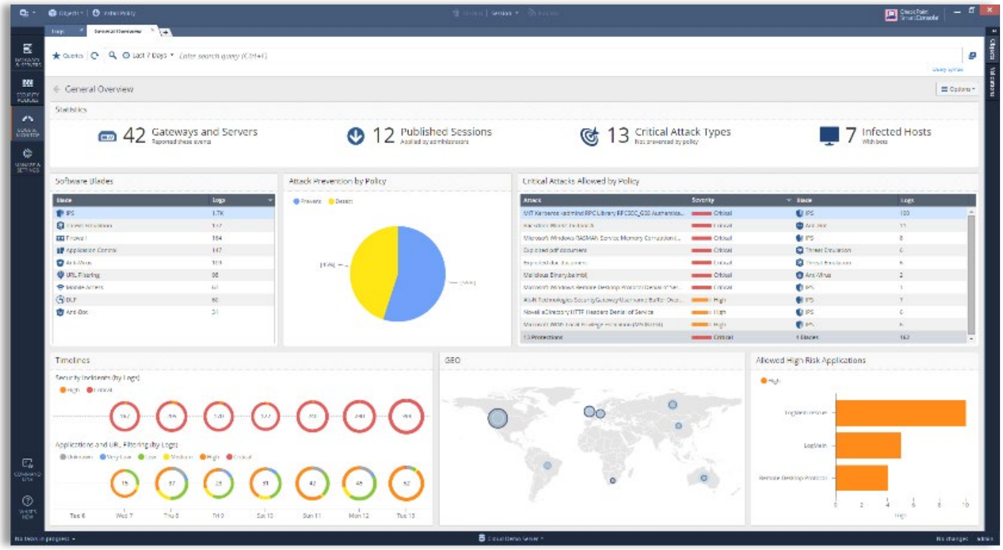
CORRELATION

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 plane 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.

SPOTLIGHT



General Overview

Statistics

42 Gateways and Servers
Reported these events

12 Published Sessions
Applied by administrators

13 Critical Attack Types
Not prevented by policy

7 Infected Hosts
With bots

Software Blades

Blade	Logs
IPS	1.7K
Threat Emulation	[illegible]
Firewall	164
Application Control	147
Anti-Virus	[illegible]
URL Filtering	98
Mobile Access	67
DLP	60
Anti-Bot	31

Critical Attacks Allowed by Policy

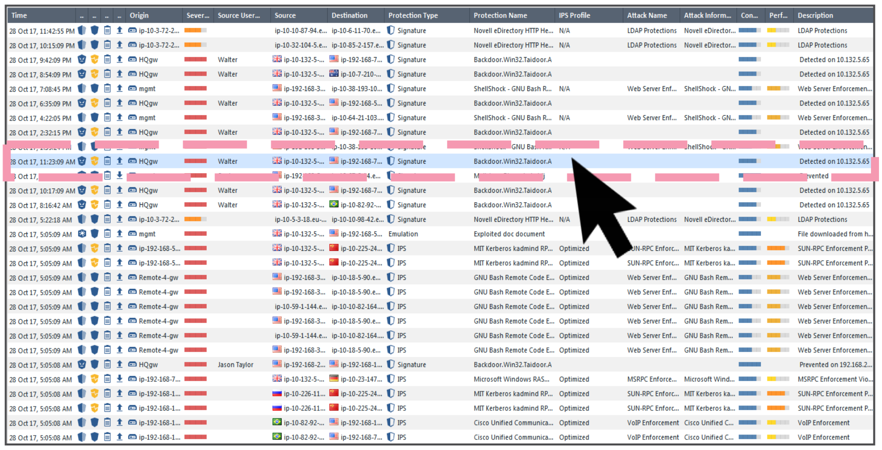
Attack	Severity	Blade	Logs
MIT Kerberos kadmind RPC Library RPCSEC_GSS Authentica...	Critical	IPS	100
Backdoor.Win32.Taidoor.A	Critical	Anti-Bot	11
Microsoft Windows RASMAN Service Memory Corruption (...	Critical	IPS	8
Exploited pdf document	Critical	Threat Emulation	6
Exploited doc document	Critical	Threat Emulation	6
Malicious Binary.[illegible]	Critical	Anti-Virus	2
Microsoft Windows Remote Desktop Protocol Denial of Ser...	Critical	IPS	1
Alt-N Technologies SecurityGateway Username Buffer Ove...	High	IPS	7
Novell eDirectory HTTP Headers Denial of Service	High	IPS	6
Microsoft WINS Local Privilege Escalation [illegible]	High	IPS	6
13 Protections	Critical	4 Blades	162

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.

Real Time Forensic and Threat Investigation

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



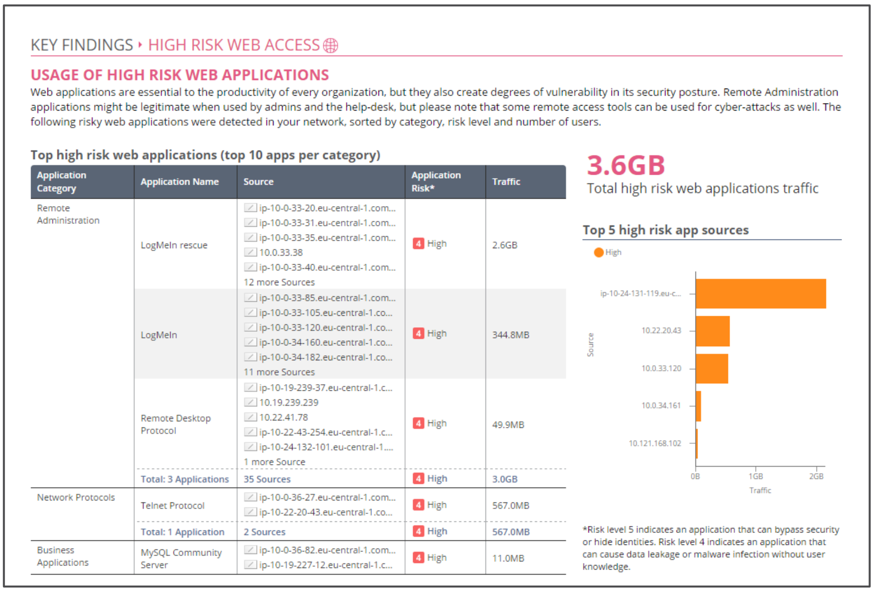
Time	..	..	..	..	Origin	Sever...	Source User...	Source	Destination	Protection Type	Protection Name	IPS Profile	Attack Name	Attack Inform...	Con...	Perf...	Description
28 Oct 17, 11:42:55 PM					ip-10-3-72-2...			ip-10-10-87-94.e...	ip-10-6-11-70.e...	Signature	Novell eDirectory HTTP He...	N/A	LDAP Protections	Novell eDirector...			LDAP Protections
28 Oct 17, 10:15:09 PM					ip-10-3-72-2...			ip-10-32-104-5.e...	ip-10-85-2-157.e...	Signature	Novell eDirectory HTTP He...	N/A	LDAP Protections	Novell eDirector...			LDAP Protections
28 Oct 17, 9:42:09 PM					HQgw		Walter	ip-10-132-5-...	ip-192-168-7...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
28 Oct 17, 8:54:09 PM					HQgw		Walter	ip-10-132-5-...	ip-10-7-210-...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
28 Oct 17, 7:08:45 PM					mgmt			ip-192-168-3...	ip-10-38-193-10...	Signature	ShellShock - GNU Bash R...	N/A	Web Server Enf...	ShellShock - GN...			Web Server Enforcemen...
28 Oct 17, 6:35:09 PM					HQgw		Walter	ip-10-132-5-...	ip-192-168-5...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
28 Oct 17, 4:22:05 PM					mgmt			ip-192-168-3...	ip-10-64-21-103....	Signature	ShellShock - GNU Bash R...	N/A	Web Server Enf...	ShellShock - GN...			Web Server Enforcemen...
28 Oct 17, 2:32:15 PM					HQgw		Walter	ip-10-132-5-...	ip-192-168-7...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
[illegible]					[illegible]			[illegible]	ip-10-38-1[illegible]	[illegible]	[illegible] GNU Ba[illegible]	[illegible]	[illegible]	[illegible]hellShoc[illegible]			[illegible]
28 Oct 17, 11:23:09 AM					HQgw		Walter	ip-10-132-5-...	ip-192-168-7...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
[illegible] Oct 17, [illegible]					[illegible]		[illegible]	ip-192[illegible]	[illegible]4.e...	[illegible]	M[illegible]j	[illegible]	[illegible]	[illegible]			[illegible]vented
28 Oct 17, 10:17:09 AM					HQgw		Walter	ip-10-132-5-...	ip-192-168-7...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
28 Oct 17, 8:16:42 AM					HQgw		Walter	ip-10-132-5-...	ip-10-82-92-...	Signature	Backdoor.Win32.Taidoor.A						Detected on 10.132.5.65
28 Oct 17, 5:22:18 AM					ip-10-3-72-2...			ip-10-5-3-18.eu-...	ip-10-10-98-42.e...	Signature	Novell eDirectory HTTP He...	N/A	LDAP Protections	Novell eDirector...			LDAP Protections
28 Oct 17, 5:05:09 AM					mgmt			ip-10-132-5-...	ip-192-168-5...	Emulation	Exploited doc document						File downloaded from h...
28 Oct 17, 5:05:09 AM					ip-192-168-5...			ip-10-132-5-...	ip-10-225-24...	IPS	MIT Kerberos kadmind RP...	Optimized	SUN-RPC Enforc...	MIT Kerberos ka...			SUN-RPC Enforcement P...
28 Oct 17, 5:05:09 AM					ip-192-168-5...			ip-10-132-5-...	ip-10-225-24...	IPS	MIT Kerberos kadmind RP...	Optimized	SUN-RPC Enforc...	MIT Kerberos ka...			SUN-RPC Enforcement P...
28 Oct 17, 5:05:09 AM					Remote-4-gw			ip-192-168-3...	ip-10-18-5-90.e...	IPS	GNU Bash Remote Code E...	Optimized	Web Server Enf...	GNU Bash Rem...			Web Server Enforcemen...
28 Oct 17, 5:05:09 AM					Remote-4-gw			ip-192-168-3...	ip-10-18-5-90.e...	IPS	GNU Bash Remote Code E...	Optimized	Web Server Enf...	GNU Bash Rem...			Web Server Enforcemen...
28 Oct 17, 5:05:09 AM					Remote-4-gw			ip-10-59-1-144.e...	ip-10-10-82-164....	IPS	GNU Bash Remote Code E...	Optimized	Web Server Enf...	GNU Bash Rem...			Web Server Enforcemen...
28 Oct 17, 5:05:09 AM					Remote-4-gw			ip-192-168-3...	ip-10-18-5-90.e...	IPS	GNU Bash Remote Code E...	Optimized	Web Server Enf...	GNU Bash Rem...			Web Server Enforcemen...
28 Oct 17, 5:05:09 AM					Remote-4-gw			ip-10-59-1-144.e...	ip-10-10-82-164....	IPS	GNU Bash Remote Code E...	Optimized	Web Server Enf...	GNU Bash Rem...			Web Server Enforcemen...
28 Oct 17, 5:05:09 AM					Remote-4-gw			ip-192-168-3...	ip-10-18-5-90.e...	IPS	GNU Bash Remote Code E...	Optimized	Web Server Enf...	GNU Bash Rem...			Web Server Enforcemen...
28 Oct 17, 5:05:08 AM					HQgw		Jason Taylor	ip-192-168-2...	ip-192-168-1...	Signature	Backdoor.Win32.Taidoor.A						Prevented on 192.168.2...
28 Oct 17, 5:05:08 AM					ip-192-168-7...			ip-10-132-5-...	ip-10-23-147...	IPS	Microsoft Windows RAS...	Optimized	MSRPC Enforce...	Microsoft Wind...			MSRPC Enforcement Vio...
28 Oct 17, 5:05:08 AM					ip-192-168-1...			ip-10-226-11...	ip-10-225-24...	IPS	MIT Kerberos kadmind RP...	Optimized	SUN-RPC Enforc...	MIT Kerberos ka...			SUN-RPC Enforcement P...
28 Oct 17, 5:05:08 AM					ip-192-168-1...			ip-10-226-11...	ip-10-225-24...	IPS	MIT Kerberos kadmind RP...	Optimized	SUN-RPC Enforc...	MIT Kerberos ka...			SUN-RPC Enforcement P...
28 Oct 17, 5:05:08 AM					ip-192-168-1...			ip-10-82-92-...	ip-192-168-1...	IPS	Cisco Unified Communica...	Optimized	VoIP Enforcement	Cisco Unified C...			VoIP Enforcement
28 Oct 17, 5:05:08 AM					ip-192-168-1...			ip-10-82-92-...	ip-192-168-7...	IPS	Cisco Unified Communica...	Optimized	VoIP Enforcement	Cisco Unified C...			VoIP Enforcement

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.



KEY FINDINGS › HIGH RISK WEB ACCESS

USAGE OF HIGH RISK WEB APPLICATIONS

Web applications are essential to the productivity of every organization, but they also create degrees of vulnerability in its security posture. Remote Administration applications might be legitimate when used by admins and the help-desk, but please note that some remote access tools can be used for cyber-attacks as well. The following risky web applications were detected in your network, sorted by category, risk level and number of users.

Top high risk web applications (top 10 apps per category)

Application Category	Application Name	Source	Application Risk*	Traffic
Remote Administration	LogMeIn rescue	ip-10-0-33-20.eu-central-1.com... ip-10-0-33-31.eu-central-1.com... ip-10-0-33-35.eu-central-1.com... 10.0.33.38 ip-10-0-33-40.eu-central-1.com... 12 more Sources	4 High	2.6GB
	LogMeIn	ip-10-0-33-85.eu-central-1.com... ip-10-0-33-105.eu-central-1.co... ip-10-0-33-120.eu-central-1.co... ip-10-0-34-160.eu-central-1.co... ip-10-0-34-182.eu-central-1.co... 11 more Sources	4 High	344.8MB
	Remote Desktop Protocol	ip-10-19-239-37.eu-central-1.c... 10.19.239.239 10.22.41.78 ip-10-22-43-254.eu-central-1.c... ip-10-24-132-101.eu-central-1.... 1 more Source	4 High	49.9MB
	Total: 3 Applications	35 Sources	4 High	3.0GB
Network Protocols	Telnet Protocol	ip-10-0-36-27.eu-central-1.com... ip-10-22-20-43.eu-central-1.co...	4 High	567.0MB
	Total: 1 Application	2 Sources	4 High	567.0MB
Business Applications	MySQL Community Server	ip-10-0-36-82.eu-central-1.com... ip-10-19-227-12.eu-central-1.c...	4 High	11.0MB

3.6GB
Total high risk web applications traffic

*Risk level 5 indicates an application that can bypass security or hide identities. Risk level 4 indicates an application that can cause data leakage or malware infection without user knowledge.

Integrated Threat Management

Utilize the power of R81 single management console – Nothing goes undetected.

ORDERING DEDICATED SMART-1 SMARTEVENT APPLIANCES

Smart-1 Appliances[1]	SKU
Smart-1 600-S	
Smart-1 600-S Base SmartEvent appliance for 5 gateways (perpetual)	CPAP-NGSM600S-BASE-EVNT
Smart-1 600-S Plus SmartEvent dedicated appliance for 10 gateways (perpetual) including SmartEvent, SmartEvent	CPAP-NGSM600S-PLUS-EVNT
Smart-1 600-M	
Smart-1 600-M Base SmartEvent dedicated appliance for 25 gateways (perpetual)	CPAP-NGSM600M-BASE-EVNT
Smart-1 600-M Plus SmartEvent dedicated appliance for 50 gateways (perpetual)	CPAP-NGSM600M-PLUS-EVNT
Smart-1 6000-L	
Smart-1 6000-L Base SmartEvent appliance for 75 gateways (perpetual), 96 GB RAM, 24 TB HDD, 2x AC PSUs, LOM	CPAP-NGSM6000L-BASE-EVNT
Smart-1 6000-L Base Multi-Log appliance for 75 gateways and 10 domains (perpetual), 96 GB RAM, 24 TB HDD, 2x AC PSUs, LOM	CPAP-NGSM6000L-BASE-MLOG-10
Smart-1 6000-L Plus SmartEvent appliance for 150 gateways (perpetual), 192 GB RAM, 24 TB HDD, 2x AC PSUs, LOM	CPAP-NGSM6000L-PLUS-EVNT
Smart-1 6000-L Plus Multi-Log appliance for 150 gateways and 10 domains (perpetual), 192 GB RAM, 24 TB HDD, 2x AC PSUs, LOM	CPAP-NGSM6000L-PLUS-MLOG-10
Smart-1 6000-XL	
Smart-1 6000-XL Base appliance SmartEvent for 200 Gateways (perpetual), 192 GB RAM, 24 TB SSD, 2x AC PSUs, LOM	CPAP-NGSM6000XL-BASE-EVNT
Smart-1 6000-XL Base Multi-Log appliance for 200 Gateways and 10 domains (perpetual), 192 GB RAM, 24 TB SSD, 2x AC PSUs, LOM	CPAP-NGSM6000XL-BASE-MLOG10
Smart-1 6000-XL Plus SmartEvent appliance for 400 gateways (perpetual), 384 GB RAM, 24 TB SSD, 2x AC PSUs, LOM	CPAP-NGSM6000XL-PLUS-EVNT
Smart-1 6000-XL Plus Multi-Log appliance for 400 gateways and 10 domains (perpetual), 384 GB RAM, 24 TB SSD, 2x AC PSUs, LOM	CPAP-NGSM6000XL-PLUS-MLOG10

[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 to equal or less than the number of managed gateways on the Security Management server.

SPECIFICATIONS

Smart-1 SmartEvent Configuration

	Enterprise Grade		Ultra High End	
Appliances	**600-S**	**600-M**	**6000-L**	**6000-XL**
Capacity & Performance				
Managed Gateways	5/10	25/50	75/150	200/400 [1]
Peak Indexed Logs per Sec	6,000[2]	8,000[2]	40,000[2]	67,500[2]
Sustained Indexed Logs per Sec	2,000[2]	4,000[2]	23,000[2]	40,000[2]
GB per Day of Logs	50[2]	105[2]	38[2]	65[2]
Hardware Specifications				
Cores	6	12	16	32
Storage (HDD) Hot-Swappable	1x 2TB HDD	2x 4TB HDD	up to 12x 4TB HDD	up to 12x 4TB SSD
RAID Type	-	1	5, 6, 10, 50, 60 (5, 6, 50 for 6 disks)	5, 6, 10, 50, 60 (5, 6, 50 for 6 disks)
Memory (RAM) Default/Max	16/32 GB	32/64 GB	96/192 GB	192/384 GB

1. Manages up to 5000 Check Point 1500, 1600, 1800 firewalls when divided into multiple domains using MDM or using SmartProvisioning
2. 600-S and 600-M tested with SmartLog and SmartEvent configuration, 6000-L/6000-XL tested with dedicated SmartEvent configuration