

WELCOME TO THE FUTURE OF CYBER SECURITY

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.



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:**
R80.10 integrated threat management and performance
- **Customizable Views and Reports:**
Security events automatically alert on critical events



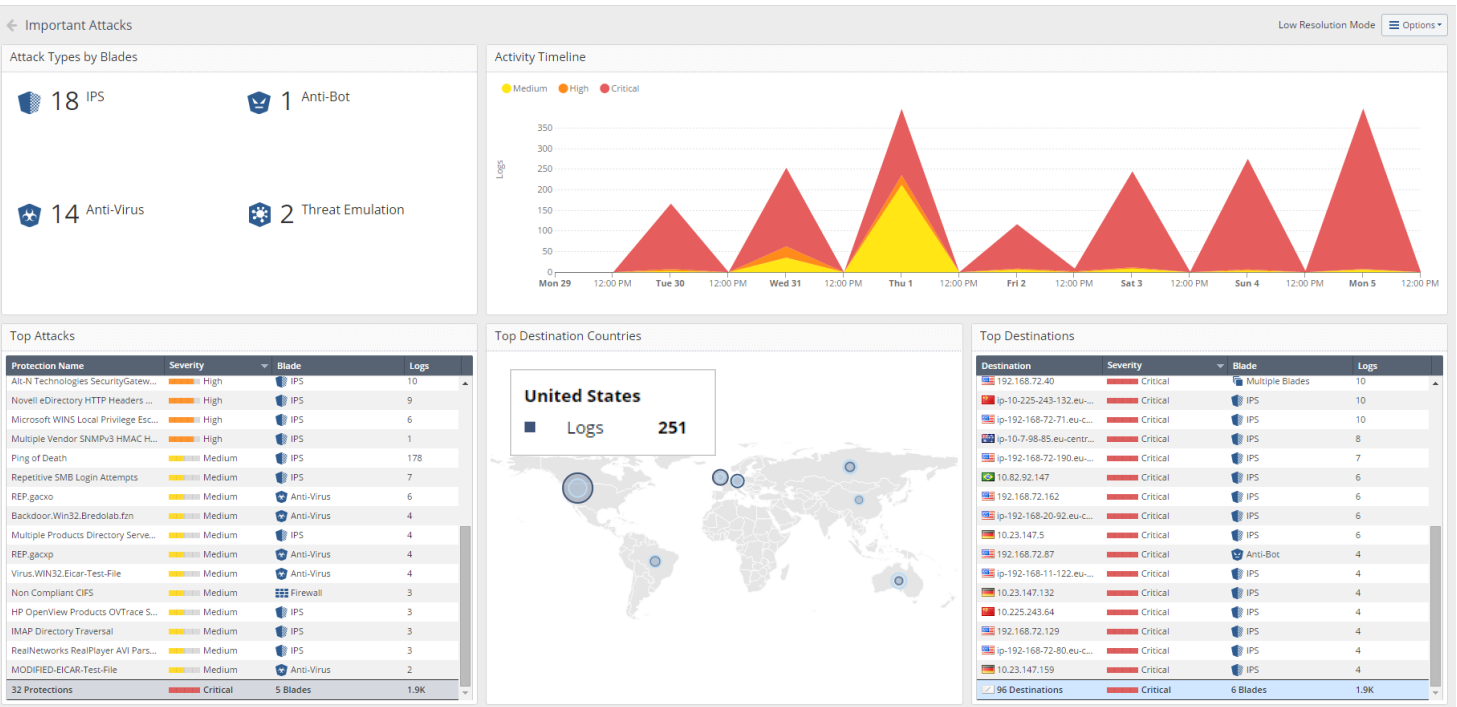
FULL THREAT VISIBILITY



REAL-TIME FORENSIC AND EVENT INVESTIGATION



COMMAND THE SECURITY EVENT



“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

WELCOME TO THE FUTURE OF CYBER SECURITY

TOP TIER REPORTING

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

14 known malware downloaded by

8 users

14 new malware downloaded

18 unique software vulnerabilities were attempted to be exploited

Data Loss

49 potential data loss incidents

7 sensitive data categories

High Risk Web Access

5 high risk web applications

2.2GB

0 high risk web sites

0 hits

0 cloud applications

0B

* C&C - Command and Control. If proxy is deployed, there might be additional infected computers. New malware variant is a zero-day attack or malicious code with no known anti-virus signature. Indicates potential attacks on computers on your network.

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections. Potential risks: Exposure to web-based threats and network infection. Examples: Spies, malicious, phishing web sites. 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 13

Top Hosts by No. of Incidents

● Critical ● Low ● Medium ● High

Source	Severity	Blade	Protection Name	Protection Type	Action
ip-10-23-147-30.eu-central-1.compute.internal (10.23.147.30)	Critical	Threat Emulation	Exploited doc document	HTTP Emulation	Detect
ip-10-23-147-27.eu-central-1.compute.internal (10.23.147.27)	Critical	Threat Emulation	Exploited pdf document	SMTP Emulation	Prevent
ip-10-132-5-48.eu-central-1.compute.internal (10.132.5.48)	Critical	Threat Emulation	Exploited doc document	HTTP Emulation	Prevent
ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)	Critical	Threat Emulation	Exploited pdf document	HTTP Emulation	Prevent
ip-10-132-5-50.eu-central-1.compute.internal (10.132.5.50)	Critical	Threat Emulation	Exploited doc document	HTTP Emulation	Prevent
ip-10-132-5-52.eu-central-1.compute.internal (10.132.5.52)	Critical	Threat Emulation	Exploited doc document	HTTP Emulation	Prevent
ip-10-6-4.eu-central-1.compute.internal (10.6.4.0)	Critical	Anti-Bot	Backdoor Win32.Tajdoor.A	Emulation	Detect
ip-192-168-130.eu-central-1.compute.internal (192.168.130.0)	Critical	Anti-Virus	Exploited doc document	Signature	Detect
ip-192-168-54-130.eu-central-1.compute.internal (192.168.54.130)	Critical	Threat Emulation	Malicious Binary (bat/maj)	Signature	Prevent
			Win32.Ecar.Modified.Test-File		

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

Malicious downloads by protocol

Infected File Name	Source	Malicious Activities	Downloads	MD5*	Protocol
Dialo3_Regul renets_m.doc	10.5.154.50	Unexpected Process Crash	1	1f0223349b8c90350ca2f14ee16a701f	HTTPS_proxy
Business Offer.pdf	ip-192-168-20-30.eu-central-1.compute.insern al (192.168.20.30)	Behaves like a known malware (Generic... Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware activity observed (Exploit).PDF... Unexpected Process Creation Unexpected Process Termination	1	1f0223349b8c90350ca2f14ee16a701f	smtp

Total: 2 Files, 2 Sources, 8 Malicious activities, 2 Downloads, 2 Files MD5, 2 Services

* You can analyze suspicious files by copying and pasting their 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 makes 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**	Distribution Country
Backdoor Win32.Tajdoor.A	Tajdoor	65	Australia, Brazil, United States
ip-10-132-5-65.eu-central-1.compute.internal (10.132.5.65)		10	United States
ip-192-168-20-30.eu-central-1.compute.internal (192.168.20.30)		10	United States
ip-192-168-10-115.eu-central-1.compute.internal (192.168.10.115)		10	United States
ip-192-168-5-18.eu-central-1.compute.internal (192.168.5.18)		10	United States
ip-10-82-82-30.eu-central-1.compute.internal (10.82.82.30)		10	Australia

* 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.mgsa-checkpoint.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
	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	15	1 Service
Total: 2 Users			
hebrew	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	11	smtp
	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	11	1 Service
Total: 1 User			
finger	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	6	smtp
	ip-10-5-165-191.eu-central-1.compute.internal (10.5.165.191)	6	1 Service
Total: 1 User			
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			

Incidents by protocol

● smtp ● http

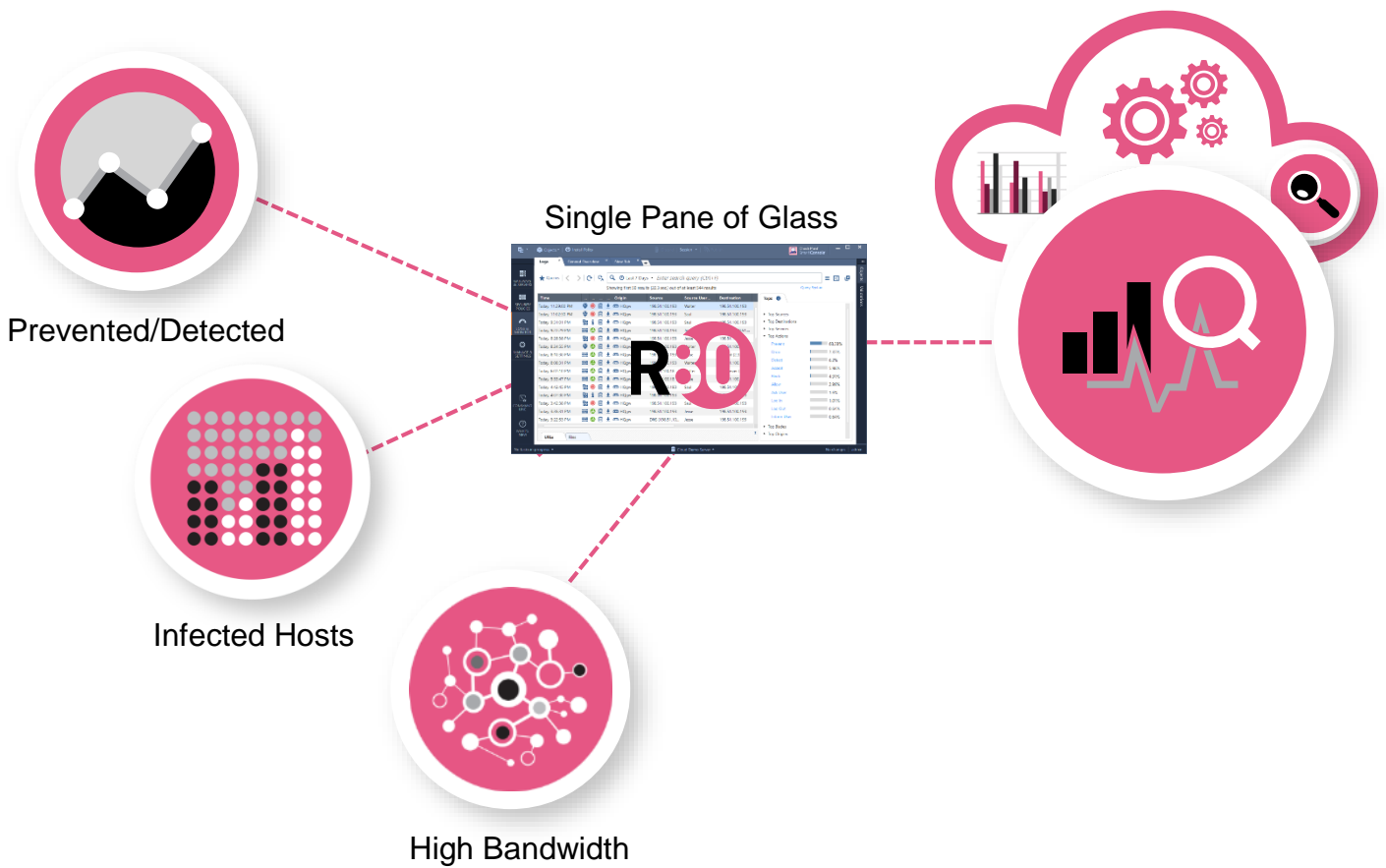
©Check Point Software Technologies Ltd. All rights reserved. Classification (Restricted) ONLY for designated groups and individuals. Security Checkup - Threat Analysis Report 22

Key Findings: Data Loss

WELCOME TO THE FUTURE OF CYBER SECURITY

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.

WELCOME TO THE FUTURE OF CYBER SECURITY

ORDERING DEDICATED SMART-1 SMARTEVENT APPLIANCES

Smart-1 Appliances ¹	SKU
Smart-1 405	
Smart -1 405 Appliance, dedicated SmartEvent for 5 gateways (perpetual)	CPAP-NGSM405-EVNT
Smart-1 410	
Smart-1 410 Appliance, dedicated SmartEvent for 10 gateways (perpetual)	CPAP-NGSM410-EVNT
Smart-1 525	
Smart-1 525 Appliance, dedicated SmartEvent for 25 gateways (perpetual)	CPAP-NGSM525-EVNT
Smart-1 5050	
Smart-1 5050 Appliance, dedicated SmartEvent for 50 gateways (perpetual)	CPAP-NGSM5050-EVNT
Smart-1 5150	
Smart-1 5150 Appliance, dedicated SmartEvent for 150 gateways (perpetual)	CPAP-NGSM5150-EVNT






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

	Enterprise Grade			Ultra High End	
Appliances	405	410	525	5050	5150
					
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	up to 12x 4TB (default 6x 4TB)
RAID Type	-	-	1	5, 10	5, 6, 10, 50, 60
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

CONTACT US

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