

SECURITY CHECKUP

THREAT ANALYSIS REPORT

Date

Prepared for

Prepared by

Analysis duration

Analysis Network

Security Gateway version

Security device

Traffic inspected by the following Check Point Software Blades:

Industry

Company size

Country

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

5
computers infected with bots



48
communications
with C&C* sites

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

22 known malware
downloaded by



15 users

21 new malware
downloaded



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

52
unique software vulnerabilities
were attempted to be
exploited



Indicates potential attacks on computers on your network.

Data Loss



0
potential data loss
incidents



0
sensitive data
categories

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

High Risk Web Access



13
high risk web
applications



20.7GB

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



95
high risk web sites



2.4K hits

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



55
cloud applications



11.5GB

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




Table of Contents



EXECUTIVE SUMMARY



KEY FINDINGS

-  MALWARE & ATTACKS
-  HIGH RISK WEB ACCESS
-  DATA LOSS
-  BANDWIDTH ANALYSIS
-  MOBILE THREATS
-  ENDPOINTS



SOFTWARE-DEFINED PROTECTION

- ▶ CHECK POINT SOFTWARE-DEFINED PROTECTION
- ▶ ABOUT CHECK POINT












Key Findings

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.MSIL.Jaktinier.E	Jaktinier	3 Computers	 Slovakia (Slovak Republic)
Backdoor.Win32.Remcosrat.A	Remcosrat	2 Computers	 Slovakia (Slovak Republic)
cnc server.TC.ayuaq	Cnc server	1 Computer	 Israel  Slovakia (Slova..
Generic.TC.fmsilk	Generic	1 Computer	 Slovakia (Slova..  United States
Generic.TC.fsxpee	Generic	1 Computer	 Slovakia (Slova..  United States
Trojan.Win32.Emotet.ED	Emotet	1 Computer	 Slovakia (Slovak Republic)
Total: 6 Malware	5 Families	5 Computers	3 Countries

Command and Control locations



* 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.

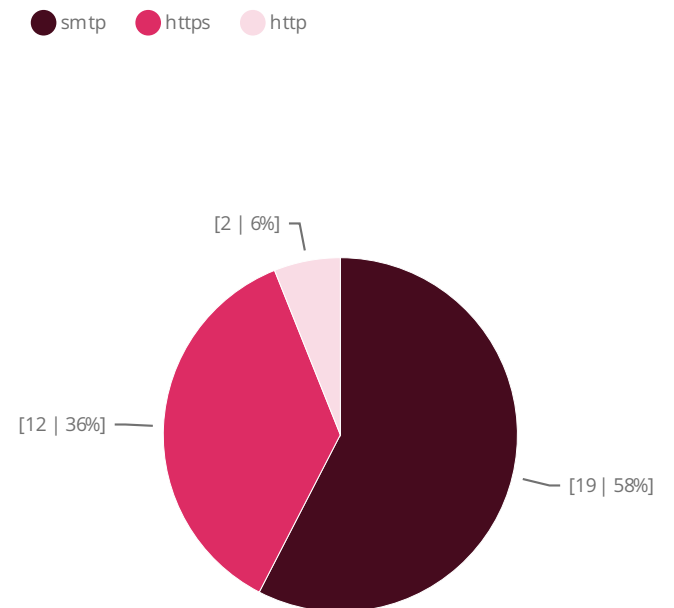
MALWARE DOWNLOADS (KNOWN MALWARE)

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. During the security analysis, a number of malware-related events which indicate malicious file downloads were detected. The following table summarizes downloads of known malware files detected in your network and the number of the downloading computers. Known malware refers to malware for which signatures exists and therefore should be blocked by an anti-virus system.

Malware downloads (top 20)

Infected File Name	Downloaded by	Protocol	MD5*
EU-Business-Register.pdf	5 Sources	smtp	03f7fb5b8f8f38ebf63902dbea785a2e197b0eb8a859caba95386d60a09b8015c43c1853de5c11829534660d82df680ed2b91e0dc9e4b55a5c912dc898c41326
Specified Styles.doc	2 Sources	smtp	2166d9c53c33771b5bd4f0e167945fc8
Isop.exe	1 Source	https	119bde97a29c1f21b5247e3e2a98fb5e
lazarus-2.0.6-fpc-3.0.4-win32.exe	1 Source	https	ceaa3da128ee3d05b60dbea922a7292b
Vendors form.doc	1 Source	smtp	
Payments for December.doc	1 Source	smtp	f6717cb6fd7fa760e77bfdd7cf8af809
PROFORMA INV# 646347319.xlsx	1 Source	smtp	8b9867bad3004154d6483a978b746172
Sales Order for November #20191113.doc	1 Source	smtp	494122226c417083bbc3a9c4c323bd13
itunes.exe	1 Source	http	4bcdc8e9d0ed23cba113890e4b6c3d95
fbevents.js	1 Source	https	b80a503b40d0f0f2efa062e39aa648d6

Downloads by protocol



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

KEY FINDINGS ▸ MALWARE AND ATTACKS

Infected File Name	Downloaded by	Protocol	MD5*
PDFCreator-3_2_1-Setup.exe	1 Source	https	37769973ad9968d8b11f77be35479c6a
Invoice copy.xlsx	1 Source	smtp	
UltraVNC_1_2_24.zip	1 Source	https	c08782b55da2d9d0f03e878f3d13fcd8
PAYMENT ADVISE.xlsx	1 Source	smtp	
Ref.No.ADIQUT19-0572.doc	1 Source	smtp	730b412459586597b952a7d04df99119
78.0.3904.108_78.0.3904.97_chrome_updater.exe	1 Source	http	b51d85b6aa4bfe3c62609e9cde1ec244
PAYMENT SLIP.doc	1 Source	smtp	46b9581c22c44c47bc98351faa666120
Purchase Order 23405 Bidding.doc	1 Source	smtp	f120ee8b6a0782c007d3ca2b67d5e3e2
pw11-free.exe	1 Source	https	75697a70f74dff19d0d39a817dfde286
125.c67f34a1c8d546f5900e.js	1 Source	https	e210647e35eca6666d2df354abee26d1
Total: 22 Files	15 Sources	3 Protocols	22 Files

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.

203.2K Total files scanned

19 Total malware found (using sandboxing technology)

Downloads of new malware variants (top 20)

Infected File Name	Malicious Activities	Downloads	MD5*	Protocol
EU-Business-Register.pdf	Behaves like a known malware (Generic.M... Behaves like a known malware (Generic.M... Behaves like a known malware (Generic.M... Malicious Network Activity Malware activity observed (HEUR:Trojan.PD.. Malware signature matched (Malicious Bina.	10	197b0eb8a859ca... c43c1853de5c118.. d2b91e0dc9e4b5...	smtp
Purchase Order 23405 Bidding.doc	Behaves like a known malware (Generic.M... Exploit.CVE-2012-0158.Gen) Malicious Filesystem Activity Malicious Network Activity Malware detected (Exploit.CVE-2012-0158.G. Malware signature matched (Malicious Bina.	8	f120ee8b6a0782c0 07d3ca2b67d5e3e 2	smtp

Top malicious file types

File Type	Number of Files	Download
pdf	3 Files	10
doc	2 Files	10
rtf	4 Files	7
rar	5 Files	6
xlsx	2 Files	4
exe	3 Files	3
Total: 6 Types	19 Files	40 Downloads

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

KEY FINDINGS ▶ MALWARE AND ATTACKS

Infected File Name	Malicious Activities	Downloads	MD5*	Protocol
Vadesi geçmiş fatura.pdf.gz.rar	A process created a hidden window Allocates read-write-execute memory (usually to unpack itself) Behaves like a known malware (Generic.MALWARE.5cf4) Changes read-write memory protection to read-execute (probably t.. Checks amount of memory in system, this can be used to detect vir... Command line console output was observed Creates executable files on the filesystem Creating a fake file extension, mostly common among phishing attem General registry locations that are typically written to by malware Generic detection methods (common) 11 more Malicious activities	2	bb0cf6e4d8f0037707ad906ca9d4e915	smtp
PROFORMA INV# 646347319.xlsx	Malicious embedded file detected: File Type: docm, File SHA-1: 6490.. Malware detected (Exploit.CVE-2017-0199.Gen)	2	8b9867bad3004154d6483a978b746172	smtp
Sales Order for November #20191113.doc.rtf	Behaves like a known malware (Generic.MALWARE.0c76) Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware activity observed (HEUR:Exploit.MSOffice.Generic) Unexpected Process Creation Unexpected Process Termination	2	494122226c417083bbc3a9c4c323bd13	smtp
Ref.No.ADIQUT19-0572.doc.rtf	Behaves like a known malware (Generic.MALWARE.0026) Exploit.CVE-2017-11882.Gen) Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware detected (Exploit.CVE-2017-11882.Gen Unexpected Process Creation Unexpected Process Termination	2	730b412459586597b952a7d04df99119	smtp
PAYMENT SLIP.doc.zip	Behaves like a known malware (Generic.MALWARE.5d70) Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware detected (VB:Trojan.Agent.EJPE) Unexpected Process Creation	2	46b9581c22c44c47bc98351faa666120	smtp

KEY FINDINGS ▶ MALWARE AND ATTACKS

Infected File Name	Malicious Activities	Downloads	MD5*	Protocol
Payments for December.doc.rtf	Attempted access to a known C and C site (http://jobmalawi.com/kk/... Behaves like a known malware (Generic.MALWARE.9f6e) Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware detected (Exploit.RTF-ObfsObjDat.Gen) Unexpected Process Creation	2	f6717cb6fd7fa760e77bfdd7cf8af809	smtp
TNT Shipment Documents.xlsx	Attempted access to a known C and C site (http://ribbonlogistics.com.. Behaves like a known malware (Generic.MALWARE.d029) CPU-Level Detection Event: Unexpected Process Crash Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malicious embedded file detected: File Type: unknown, File SHA-1: a.. Malware activity observed (HEUR:Exploit.MSOffice.Generic) Malware detected (Exploit.CVE-2017-11882.Gen) Unexpected Process Creation 1 more Malicious activity	2	43da9038d106fb0a9849e6ee99aaa9e8	smtp
MO Walcott International Development LLC Order 2019 pdf.rar	Allocates read-write-execute memory (usually to unpack itself) Changes read-write memory protection to read-execute (probably t.. Creating a fake file extension, mostly common among phishing attem Generic detection methods (common) Observe a program that accesses the CTF registry subkey Observe a program that creates a new process Observe a program that disables system error message boxes Observe a program that launches the Windows command prompt Observe a program that opens the ControlSet001 subkey The Injector is malware that injects malicious code into legitimate a... 10 more Malicious activities	1	05aeffb8ff2893550ecf90521cdffbf	smtp
TNT consignment number 114844306.doc.rtf	Behaves like a known malware (Generic.MALWARE.778d) Malicious Filesystem Activity Malicious Network Activity Malicious Registry Activity Malware activity observed (HEUR:Exploit.MSOffice.Generic)	1	45f8479d1cd68de04a316d7c38ac7406	smtp

KEY FINDINGS ▶ MALWARE AND ATTACKS

Infected File Name	Malicious Activities	Downloads	MD5*	Protocol
Banka hesabi.pdf.gz.rar	<p>A process created a hidden window</p> <p>Allocates read-write-execute memory (usually to unpack itself)</p> <p>Behaves like a known malware (Generic.MALWARE.5cf4)</p> <p>Changes read-write memory protection to read-execute (probably t..</p> <p>Checks amount of memory in system, this can be used to detect vir...</p> <p>Command line console output was observed</p> <p>Creates executable files on the filesystem</p> <p>Creating a fake file extension, mostly common among phishing attem</p> <p>General registry locations that are typically written to by malware</p> <p>Generic detection methods (common)</p> <p>11 more Malicious activities</p>	1	ce84b29e6b6f2c0eef11e4c9d c2de0a0	smtp
Order Package 14203355-1644699 OMWAVE GLOBAL\	<p>A potential heapspray has been detected. 122 megabytes was spraye.</p> <p>Allocates execute permission to another process indicative of possib.</p> <p>Allocates read-write-execute memory (usually to unpack itself)</p> <p>Attempted access to a known C and C site (DNS: sentab.tk)</p> <p>Attempted access to a known C and C site (http://sentab.tk/loki/Pane..</p> <p>AutoITCrypter is a packer written in Autoit scripting language.</p> <p>Checks for the Locally Unique Identifier on the system for a suspicio..</p> <p>Checks if process is being debugged by a debugger</p> <p>Collects information to fingerprint the system (MachineGuid, Digital...</p> <p>Common indicators for recognizing credentials and personal data h...</p> <p>11 more Malicious activities</p>	1	854baffb04fd3b6155116746d2 fd103b	smtp
itunes_3285353664.exe	<p>A potential heapspray has been detected. 87 megabytes was spraye...</p> <p>Allocates read-write-execute memory (usually to unpack itself)</p> <p>An installer bundle that offers additional third party applications tha...</p> <p>Attempts to stop active services</p> <p>Checks adapter addresses which can be used to detect virtual netwo.</p> <p>Checks amount of memory in system, this can be used to detect vir...</p> <p>Checks for the Locally Unique Identifier on the system for a suspicio..</p> <p>Checks the CPU name from registry, possibly for anti-virtualization</p> <p>Checks the version of Bios, possibly for anti-virtualization</p> <p>Collects information to fingerprint the system (MachineGuid, Digital...</p> <p>11 more Malicious activities</p>	1	4bcd8e9d0ed23cba113890e4 b6c3d95	http

KEY FINDINGS ▸ MALWARE AND ATTACKS

Infected File Name	Malicious Activities	Downloads	MD5*	Protocol
\\t102019PDF.z.rar	<p>A potential heap spray has been detected. 219 megabytes were sprayed.</p> <p>Allocates execute permission to another process indicative of possible execution.</p> <p>Allocates read-write-execute memory (usually to unpack itself)</p> <p>AutoITCrypter is a packer written in AutoIt scripting language.</p> <p>Changes read-write memory protection to read-execute (probably to bypass ASLR).</p> <p>Checks for the Locally Unique Identifier on the system for a suspicious process.</p> <p>Checks if process is being debugged by a debugger</p> <p>Collects information to fingerprint the system (MachineGuid, DigitalProductId, etc.)</p> <p>Common indicators for recognizing credentials and personal data hashes.</p> <p>Creates executable files on the filesystem</p> <p>11 more Malicious activities</p>	1	33eabad447888ec61d4d3fdb66f3c722	smtp
\\tLtd 09 decemberPDF.z.rar	<p>A potential heap spray has been detected. 122 megabytes were sprayed.</p> <p>Allocates execute permission to another process indicative of possible execution.</p> <p>Allocates read-write-execute memory (usually to unpack itself)</p> <p>Attempted access to a known C and C++ site (DNS: sentab.tk)</p> <p>Attempted access to a known C and C++ site (http://sentab.tk/loki/Panels)</p> <p>AutoITCrypter is a packer written in AutoIt scripting language.</p> <p>Checks for the Locally Unique Identifier on the system for a suspicious process.</p> <p>Checks if process is being debugged by a debugger</p> <p>Collects information to fingerprint the system (MachineGuid, DigitalProductId, etc.)</p> <p>Common indicators for recognizing credentials and personal data hashes.</p> <p>11 more Malicious activities</p>	1	854baffb04fd3b6155116746d2fd103b	smtp
Purchase Order No. 1352019 dtd. november\\r	<p>A potential heap spray has been detected. 219 megabytes were sprayed.</p> <p>Allocates execute permission to another process indicative of possible execution.</p> <p>Allocates read-write-execute memory (usually to unpack itself)</p> <p>AutoITCrypter is a packer written in AutoIt scripting language.</p> <p>Changes read-write memory protection to read-execute (probably to bypass ASLR).</p> <p>Checks for the Locally Unique Identifier on the system for a suspicious process.</p> <p>Checks if process is being debugged by a debugger</p> <p>Collects information to fingerprint the system (MachineGuid, DigitalProductId, etc.)</p> <p>Common indicators for recognizing credentials and personal data hashes.</p> <p>Creates executable files on the filesystem</p> <p>11 more Malicious activities</p>	1	33eabad447888ec61d4d3fdb66f3c722	smtp

KEY FINDINGS ▸ MALWARE AND ATTACKS

Infected File Name	Malicious Activities	Downloads	MD5*	Protocol
Isop.exe	Allocates read-write-execute memory (usually to unpack itself) Checks adapter addresses which can be used to detect virtual netwo. Checks amount of memory in system, this can be used to detect vir... Checks for the Locally Unique Identifier on the system for a suspicio.. Checks if process is being debugged by a debugger Checks the CPU name from registry, possibly for anti-virtualization Checks the version of Bios, possibly for anti-virtualization Collects information to fingerprint the system (MachineGuid, Digital... Creates a shortcut to an executable file Creates executable files on the filesystem 11 more Malicious activities	1	119bde97a29c1f21b5247e3e2a98fb5e	https
PDFescape_Desktop_Installer.exe		1	87d28b3d2df1cab3711bf8d3b5b520c2	http
Total: 19 Files	100 Malicious activities	40	19 Files MD5	3 Services

ACCESS TO SITES KNOWN TO CONTAIN MALWARE

Organizations can get infected with malware by accessing malicious web sites while browsing the internet, or by clicking on malicious links embedded in received email. The following summarizes events related to sites known to contain malware.

Top 10 accessed malicious sites












URL	Users	Hits
w3.org/tr/xhtml1/dtd/xhtml1-transitional.dtd w3.org/tr/xhtml1/dtd/xhtml1-strict.dtd w3.org/tr/rec-html40	8 Users	8
http://tracker.rareru.ru/match?bidder_id=adriver	2 Users	4
theblogchamp.com/calendar/dogeship_sunglade.html	1 User	1
santokatrin.com/calendar/multipointed_measuredly.html	1 User	1
http://deloplen.com/tag.min.js	1 User	1
http://www.driverscape.com/files/DriverToolkitInstaller.exe	1 User	1
http://deloplen.com/apu.php?zoneid=2899654&oo=1	1 User	1
http://deloplen.com/apu.php?zoneid=2899654&oo=1	1 User	1
http://deloplen.com/tag.min.js	1 User	1
thewildmeridian.com/calendar/addy_evenminded.html	1 User	1
	21 Users	29

* You can analyze suspicious URLs by copying and pasting them into VirusTotal online service at www.virustotal.com

ATTACKS AND EXPLOITED SOFTWARE VULNERABILITIES











During the security analysis, attacks and exploited software vulnerabilities on servers/clients were detected. Such incidents might indicate intrusion attempts, malware attacks, DoS attacks or attempts to bridge security by exploiting software vulnerabilities. The following summarizes these events.

Top attacks and exploited software vulnerabilities (top 20)

Attack / Exploit	Industry Reference	Severity	Events
Multiple Products Malformed GIF Image File Handling Buffer Overflow	CVE-2005-0243 CVE-2005-0399 CVE-2007-1071	 High	1.4K
VideoLAN VLC Media Player PNG Code Execution	CVE-2012-5470	 High	615
libpng png_decompress_chunk Integer Overflow	CVE-2011-3026	 Critical	116
Joomla Object Injection Remote Command Execution	CVE-2015-8562	 Critical	43
NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)	CVE-2018-20062	 Critical	40
WordPress portable-phpMyAdmin Plugin Authentication Bypass	CVE-2012-5469	 High	39
Oracle Java Runtime True Type Font IDEF Opcode Heap Buffer Overflow	CVE-2012-0499	 High	36
Radio Exploit Kit Landing Page	None	 Critical	24
D-Link DSL-2750B Remote Command Execution		 Critical	2.2K
JPEG Files Containing Suspicious Comments		 High	952
Masscan Port Scanner		 High	639

*For more information on specific CVE, search on MITRE's CVE search page (www.cve.mitre.org/cve/cve).

KEY FINDINGS ▸ MALWARE AND ATTACKS

Attack / Exploit	Industry Reference	Severity	Events
JavaScript Malicious Reverse Obfuscation Technique		 Critical	260
ZMap Security Scanner over HTTP		 High	165
Sophos Anti-Virus CAB Files Invalid typeCompress Parsing Heap Buffer Overflow		 High	164
Suspicious Executable Mail Attachment		 Critical	59
Google Chrome XSSAuditor Filter Security Policy Bypass		 High	53
PHP DIESCAN information disclosure		 High	45
SQL Servers SQL Injection Evasion Techniques - ver 2		 Critical	39
SQL Servers UNION Query-based SQL Injection		 Critical	38
Command Injection Over HTTP		 Critical	26
Total: 76 Attacks / Exploits	52 References	 Critical	7.1K

DDOS ATTACKS

Denial-of-service (DoS) attacks target networks, systems and individual services, and flood them with so much traffic that they either crash or are unable to operate which effectively denies the service to legitimate users. A DoS attack is launched from a single source to overwhelm and disable the target service, whereas a Distributed Denial-of-service (DDoS) attack is coordinated and simultaneously launched from multiple sources to overwhelm and disable a target service. During the security analysis, DDoS attacks were detected. The following summarizes these events.

Top 20 DDoS attacks

Summary

0

attack types

0

total attacks

0B

bandwidth utilization

Top source countries

No data found.

No data found.

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	VNC-encrypted	13 Sources	4 High	10.8GB
	VNC	6 Sources	4 High	8.2GB
	TeamViewer	10 Sources	4 High	1.5GB
	VNC-file transfer	4 Sources	4 High	197.5MB
	Total: 4 Applications	26 Sources	4 High	20.6GB
File Storage and Sharing	Dropbox	8 Sources	4 High	18.0MB
	Crashplan	1 Source	4 High	1.3MB
	ImageVenue	1 Source	4 High	8.8KB
	Macrium Reflect	1 Source	4 High	5.4KB
	Egnyte	1 Source	4 High	5.1KB
	Total: 5 Applications	11 Sources	4 High	19.3MB
Anonymizer	Tor	1 Source	5 Critical	4.6MB
	Hotspot Shield	1 Source	5 Critical	537.9KB
	Turbo VPN	1 Source	5 Critical	30.2KB
	Total: 3 Applications	2 Sources	5 Critical	5.2MB
Browser Plugin	Dashlane	1 Source	4 High	181.2KB
	Total: 1 Application	1 Source	4 High	181.2KB
Total: 4 Categories	13 Applications	36 Sources	5 Critical	20.7 GB

20.7GB

Total high risk web applications traffic

Top categories

Application Category	Traffic
Remote Administration	20.6GB
File Storage and Sharing	19.3MB
Anonymizer	5.2MB
Browser Plugin	181.2KB
Total: 4 Categories	20.7 GB

*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.

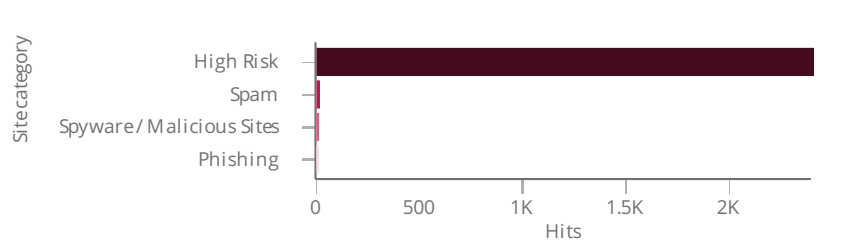
ACCESS TO HIGH RISK WEB SITES

Web use is ubiquitous in business today. But the dynamic, constantly evolving nature of the web makes it extremely difficult to protect and enforce web usage in a corporate environment. To make matters more complicated, web traffic has evolved to include not only URL traffic, but embedded URLs and applications as well. Identification of risky sites is more critical than ever. Access to the following risky sites was detected in your network, organized by category, number of users, then number of hits.

Top high risk web sites (top 10 sites per category)

Site Category	Site	Users	Hits
High Risk	ad.adriver.ru/cgi-bin/rle.cgi	81 Users	2.4K
	ad.novara.sk		
	adk.sk		
	ads.avocet.io/getuid		
	ads.undertone.com/u		
	adsinspidsp.com		
	affhit.com		
	afterdawn.fi		
	analyticstrackingopt.com		
	andreamarket.sk		
	79 more Sites		
Spam	blashco.me i16-tb.isnssdk.com isnssdk.com reimageplus.com	3 Users	6
Spyware / Malicious Sites	cdnrep.reimage.com	1 User	2
Phishing	client_monitor.isnssdk.com	1 User	1
Total: 4 Categories	95 Sites	84 Users	2.4 K

High risk web sites by category



Category	Browse Time (hh:mm:ss)	Traffic Total Bytes
Sex	1:33:57	120.5MB
Illegal / Questionable	0:04:06	39.0MB
Gambling	1:51:42	37.1MB
Total: 3 Categories	3:29:45	196.6MB

Web Access to non-business websites or to sites containing questionable content can expose an organization to possible productivity loss, compliance and business continuity risks.

Cloud based web applications (top 20)

Application Name	Application Category	Users	Traffic
iCloud	Media Sharing	6 Users	8.1GB
Ulozto	File Storage and Sharing	2 Users	955.2MB
Office365-Outlook-web	Email	9 Users	690.9MB
SoundCloud	Media Sharing	11 Users	516.4MB
Google Cloud Platform	Computers / Internet	12 Users	500.1MB
Google Analytics	Business / Economy	21 Users	449.0MB
Google Drive-web	File Storage and Sharing	37 Users	57.0MB
iCloud-email	Email	3 Users	42.5MB
Office365	Business / Economy	11 Users	29.5MB
Box	File Storage and Sharing	1 User	21.1MB
Dropbox	File Storage and Sharing	8 Users	18.0MB
Adobe Creative Cloud	Business / Economy	1 User	8.7MB
Zendesk	Business / Economy	52 Users	8.6MB
Microsoft Excel	Business / Economy	4 Users	7.7MB
Salesforce	Business / Economy	7 Users	5.8MB
Gmail	SMZ	30 Users	5.7MB
Windows Azure Cloud Services	Business / Economy	6 Users	3.3MB
GitHub	Business / Economy	7 Users	2.9MB
Salesforce Marketing Cloud	Business / Economy	8 Users	2.3MB
Skype for Business (Lync)	Business / Economy	2 Users	2.3MB
Total: 55 Applications	11 Categories	90 Users	11.5GB

BANDWIDTH UTILIZATION BY APPLICATIONS & WEBSITES

Organization's network bandwidth is usually utilized by a wide range of web applications and sites used by employees. Applications that use a lot of bandwidth, for example, streaming media, can limit the bandwidth that is available for important business applications. It is important to understand what is hogging the network's bandwidth in order to limit bandwidth consumption of non business related usage. The following summarizes the bandwidth usage of your organization sorted by consumed bandwidth.

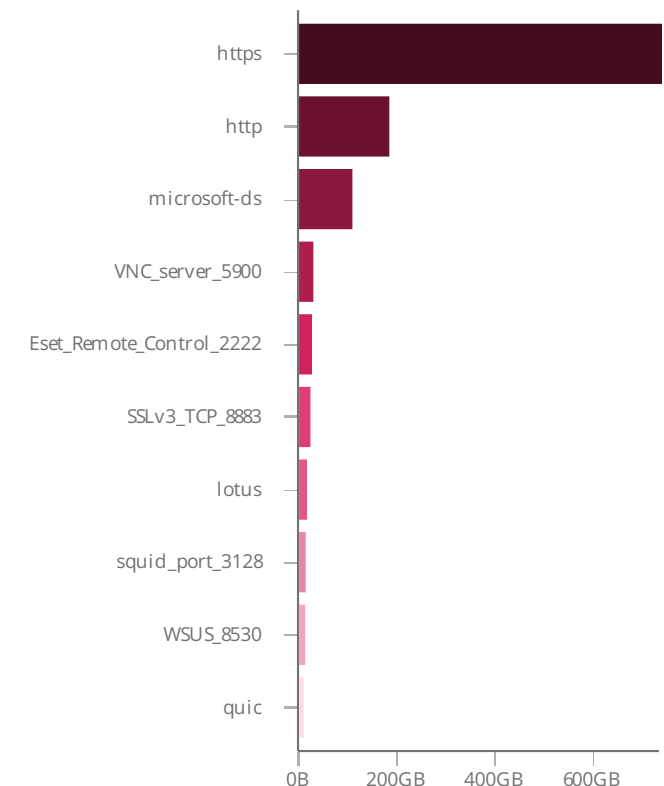
Top applications/sites (top 30)

Application / Site	Category	Risk Level	Sources	Traffic
SSL Protocol	Network Protocols	1 Very Low	22 Sources	202.7GB
Windows Update	Software Update	1 Very Low	30 Sources	186.3GB
YouTube	Media Streams	2 Low	113 Sources	137.9GB
Facebook	Social Networking	2 Low	109 Sources	134.9GB
Server Message Block v1 (SMBv1)	Network Protocols	2 Low	17 Sources	100.3GB
HTTP/2 over TLS	Network Protocols	1 Very Low	21 Sources	42.9GB
Google Play	Search Engines / Portals	2 Low	22 Sources	33.6GB
Apple Services	Web Services Provider	2 Low	11 Sources	30.2GB
Instagram	Social Networking	2 Low	65 Sources	25.8GB
bestfm.sk	Business / Economy	— Unknown	1 Source	23.8GB
Google Services	Computers / Internet	2 Low	19 Sources	14.9GB
dbankcdn.com	Computers / Internet	— Unknown	3 Sources	12.0GB
IBM Lotus Notes and Domino	Business / Economy	2 Low	10 Sources	11.8GB
VNC-encrypted	Remote Administration	4 High	13 Sources	10.8GB
Office on Demand	Business / Economy	2 Low	13 Sources	8.2GB
















1.1TB

Total traffic scanned

Traffic by protocol



KEY FINDINGS ▸ BANDWIDTH ANALYSIS


Application / Site	Category	Risk Level	Sources	Traffic
VNC	Remote Administration	 High	6 Sources	8.2GB
iCloud	Media Sharing	 Low	6 Sources	8.1GB
iosapps.itunes.apple.com	Computers / Internet	 Unknown	2 Sources	7.3GB
Microsoft Services	Computers / Internet	 Low	27 Sources	6.6GB
smzjelsava.sk	Computers / Internet	 Unknown	9 Sources	6.1GB
cdn-apple.com	Computers / Internet	 Unknown	2 Sources	6.0GB
TM_bypass_URL	Custom Application/Site	 Unknown	28 Sources	5.9GB
muscdn.com	Computers / Internet	 Unknown	2 Sources	5.7GB
VNC-clipboard	Remote Administration	 Medium	6 Sources	5.6GB
Google Ads	Web Advertisements	 Medium	45 Sources	5.4GB
adc.eamobile.com	Computers / Internet	 Unknown	1 Source	4.7GB
stream.atv.hu	News / Media	 Unknown	2 Sources	4.4GB
Server Message Block (SMB)	Network Protocols	 Very Low	5 Sources	3.8GB
Netflix-streaming	Media Streams	 Low	2 Sources	3.6GB
eset.com	Computers / Internet	 Unknown	23 Sources	3.5GB
Total: 3424 Applications / Sites	70 Categories	6 Risks	161 Sources	1.1TB


KEY FINDINGS ▸ SCADA COMMUNICATIONS

SCADA (Supervisory Control and Data Acquisition) is a type of industrial control system (ICS) that monitors and controls industrial processes. It operates with coded signals over communication channels so as to provide control of remote equipment. SCADA networks are usually separated from the organizational IT network for security purposes. SCADA protocols detected on the IT network might indicate a security risk with a potential for a security breach. The following SCADA protocols were detected on your network.

SCADA Communications

17
Sources


14
Destinations


59
Commands


3
Ports


Top SCADA commands (top 20)

Protocol & Command	Transactions	Traffic
S7 Protocol - CPU functions-Message service	22	356.2KB
S7 Protocol - CPU functions-Read SZL	22	136.4KB
S7 protocol	22	53.2MB
S7 Protocol - read var	15	183.6MB
S7 Protocol - setup communication	12	26.3KB
S7 Protocol - block functions-list blocks of type DB	7	6.8KB
S7 Protocol - block functions-List blocks	7	95.5KB
IENA Protocol	7	500B
S7 Protocol - block functions-list blocks of type	7	2.1KB
S7 Protocol - write var	7	44.0MB
S7 Protocol - Programmer command Forces	7	44.4KB
S7 Protocol - Block functions-get OB block info	6	832.7KB
S7 Protocol - request download DB block	6	9.6MB
Total: 59 Protocols & Commands	361 Transactions	771.7 MB

The following section focuses on mobile threats and uncovers where your organization is exposed to them, 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: mobile malware infections, usage and downloads of high risk mobile apps, download of malicious mobile applications, outdated mobile operating systems, and more.

Mobile Devices

7

Android devices

3

iOS devices

22.8GB

total mobile traffic

Mobile devices detected on corporate network (number of devices is based on source IP addresses).

Cloud Mobile Apps

4

cloud base mobile apps

2.5MB

traffic

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

High Risk Apps

0

high risk mobile apps

0B

traffic

High risk mobile apps are legitimate apps that can be used to monitor and control mobile devices.

Access to High Risk Sites

4

high risk web sites

5

hits

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

Malware

0

downloads of malicious apps and malware

0

infected devices

Download of malicious content such as malicious apps, malware and adware and infected devices communicating with Command and Control servers.

Top 10 accessed malicious sites

Protection Name	Malicious URL	Malware Family	Mobile sources	Hits
Rough_adnetwork.TC.a	http://sdk.appsflyer.tk/op?platform=1&os_version=7.0&package_name=com.xrom.intl.appcenter&app_version_name=5.1.010-201807191...		1 Mobile user	1
Total: 1 Protection		0 Families	1 Mobile user	1

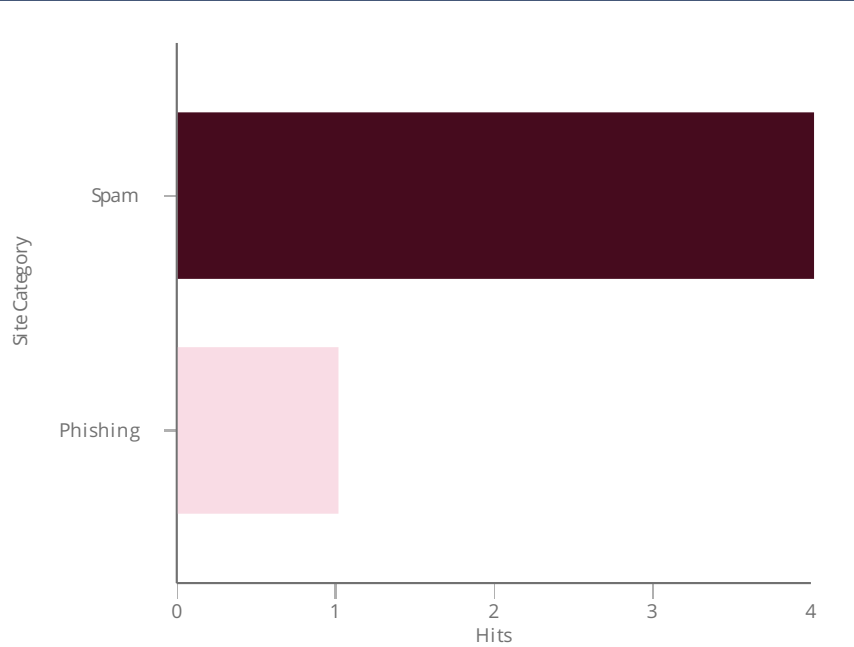
HIGH RISK MOBILE APPS AND WEB SITES

Mobile apps are essential to the productivity of every organization, but they also create degrees of vulnerability in its security posture. Web is also ubiquitous in business today. But the dynamic, constantly evolving nature of the web makes it extremely difficult to protect and enforce web usage in a corporate environment. Identification of risky apps and sites is more critical than ever. The following risky mobile apps and risky sites accessed by mobile devices were detected in your network.

Top high risk web applications (top 5 apps per category)

Application Category	App/Site Name	Source	Applicati... Risk*	Traffic
Spam	blashco.me	1 Source	4 High	183.6KB
	isnssdk.com	1 Source	4 High	10.6KB
	i16-tb.isnssdk.com	1 Source	4 High	5.9KB
	Total: 3 Applications	2 Sources	4 High	200.0KB
Phishing	client_monitor.isnssdk.com	1 Source	4 High	6.4KB
	Total: 1 Application	1 Source	4 High	6.4 KB
Total: 2 Categories	4 Applications	2 Sources	4 High	206.4 KB

High risk web sites by category



*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.

For more information on specific application, search the application name on Check Point App Wiki (<http://appwiki.checkpoint.com/>).

CLOUD-BASED STORAGE AND SHARING APPLICATIONS

Cloud-based storage and sharing applications can be essential to productivity and the routine operation of an organization, but they also create degrees of vulnerability in its security posture. Usage of such applications can lead to data leakage and loss of control over sensitive data which can end up in the hands of unauthorized and ill-intentioned strangers.

Top applications (top 20)

Application name	Application Category	Mobile Devices	Traffic
SoundCloud	Media Sharing	1 Device	1.9MB
Google Cloud Platform	Computers / Internet	1 Device	447.8KB
Windows Azure Cloud Services	Business / Economy	1 Device	100.2KB
Google App Engine	Web Services Provider	1 Device	5.5KB
Total: 4 Applications	4 Categories	2 Devices	2.5MB

4 sources running Android versions 4.x or below

Android OS versions 4.x and below are considered outdated versions containing many security vulnerabilities*.

Android mobile devices and OS versions (showing up to 30)











Device model and OS version**	Source IPs
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.4; SM-G357FZ Build/KTU84P)	3 Sources
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.2; EVOLVEO StrongPhone D2 Mini Build/KOT49H)	2 Sources
Other: Dalvik/1.6.0 (Linux; U; Android 4.2.2; GT-S7580 Build/JDQ39)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.4; E2003 Build/25.0.A.2.35)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.2.2; A3-A10 Build/JDQ39)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.2; K010 Build/KOT49H)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.1.2; PMP7170B3G_DUO Build/JZO54K)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.2; Lenovo A3500-FL Build/KOT49H)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.1.2; sk; MT8377 Build/JZO54K; FW PMP7170B3G_DUO_20140303_V1.0.10)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.0.3; Slider SL101 Build/IML74K)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.1.2; sk; PMP7170B3G_DUO Build/JZO54K; FW PMP7170B3G_DUO_20140303_V1.0.10)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.2; C6903 Build/14.3.A.0.757)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.3; MediaPad 7 Youth 2 Build/HuaweiMediaPad)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.2; SM-G800F Build/KOT49H)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-I9100P Build/JZO54K)	1 Source
Other: AndroidDownloadManager/4.2.2 (Linux; U; Android 4.2.2; A3-A10 Build/JDQ39)	1 Source

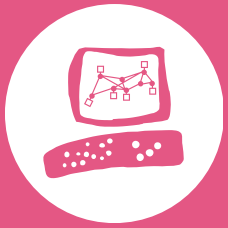
* For further information about security vulnerabilities on Android versions: <http://www.cvedetails.com/version-list/1224/19997/1/Google-Android.html>

** For more visual display of devices and OS versions, copy and paste the each record above into the user-agent string search box at the bottom of this portal: <https://faisalman.github.io/ua-parser-js>

KEY FINDINGS ▸ OUTDATED ANDROID VERSIONS

Device model and OS version**	Source IPs
Other: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-I8262 Build/JZO54K)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.1.2; LG-E460 Build/JZO54K) [FBAN/Orca-Android;FBAV/77.0.0.27.71;FBPN/com.facebook.orca	1 Source
Other: AndroidDownloadManager/4.4.4 (Linux; U; Android 4.4.4; SM-G357FZ Build/KTU84P)	1 Source
Other: com.google.android.apps.maps/1016200132 (Linux; U; Android 4.4.4; sk_SK; E2003; Build/25.0.A.2.35; Cronet/76.0.3809.111)	1 Source
Other: com.google.android.youtube/5.1.10(Linux; U; Android 4.1.2; sk_SK; PMP7170B3G_DUO Build/JZO54K) gzip	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.2; E39 Build/KOT49H)	1 Source
Other: Dalvik/1.6.0 (Linux; U; Android 4.4.4; G620S-L01 Build/HuaweiG620S-L01)	1 Source
Other: nokeepalive Cerberus 3.6 - Android 28 - ONEPLUS A6003 - 9 - ONEPLUS A6003_22_190911	1 Source
Total: 24 Models and OS versions	4 Sources

Endpoints Involved in High Risk Web Access and Data Loss Incidents		Endpoints Involved in Malware and Attack Incidents		
<div></div> <div>36</div> <div>running high risk applications</div>	<div></div> <div>84</div> <div>accessed high risk web sites</div>	<div></div> <div>5</div> <div>infected with malware</div>	<div></div> <div>15</div> <div>downloaded malware</div>	<div></div> <div>0</div> <div>received email containing link to malicious site</div>
<div></div> <div>32</div> <div>users accessed questionable, nonbusiness related web sites</div>	<div></div> <div>0</div> <div>users involved in potential data loss incidents</div>	<div></div> <div>21</div> <div>accessed a site known to contain malware</div>	<div></div> <div>2.7K</div> <div>attacked sources <small>(Source IP addresses of IPS events)</small></div>	<div></div> <div>110</div> <div>attacked destinations <small>(Destination IP addresses of IPS events)</small></div>



Software-Defined Protection

SOFTWARE-DEFINED PROTECTION

In a world with high-demanding IT infrastructures and networks, where perimeters are no longer well defined, and where threats grow more intelligent every day, we need to define the right way to protect enterprises in the ever changing threat landscape.

There is a wide proliferation of point security products; however these products tend to be reactive and tactical in nature rather than architecturally oriented. Today's corporations need a single architecture that combines high performance network security devices with real-time proactive protections. A new paradigm is needed to protect organizations proactively.

Software-defined Protection is a new, pragmatic security architecture and methodology. It offers an infrastructure that is modular, agile and most importantly, SECURE.

Such architecture must protect organizations of all sizes at any location: headquarters networks, branch offices, roaming through smartphones or mobile devices, or when using cloud environments.

Protections should automatically adapt to the threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations. These protections must integrate seamlessly into the larger IT environment, and the architecture must

provide a defensive posture that collaboratively leverages both internal and external intelligent sources.

The Software Defined Protection (SDP) architecture partitions the security infrastructure into three interconnected layers:

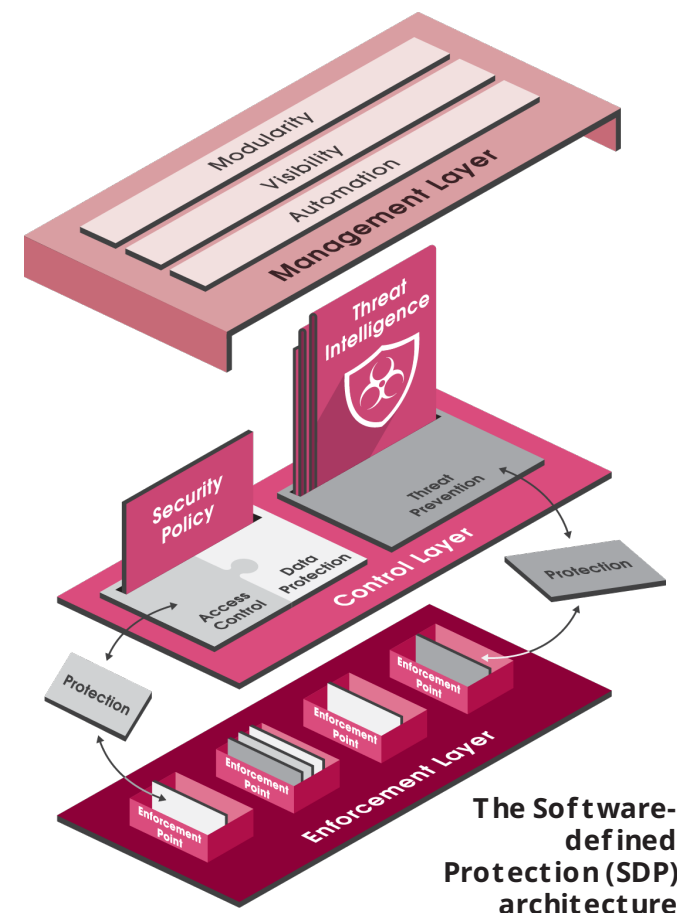
► **An Enforcement Layer that** is based on physical, virtual and host-based security enforcement points and that segments the network as well as executes the protection logic in high-demand environments.

► **A Control Layer that** analyzes different sources of threat information and generates protections and policies to be executed by the Enforcement Layer.

► **A Management Layer that** orchestrates the infrastructure and brings the highest degree of agility to the entire architecture.

By combining the high performance Enforcement Layer with the fast-evolving and dynamic softwarebased Control Layer, the SDP architecture provides not only operational resilience, but also proactive incident prevention for an ever-changing threat landscape.

Designed to be forward-looking, the SDP architecture supports traditional network security and access control policies requirements as well as the threat prevention needed by modern enterprises that



embrace new technologies such as mobile computing and Software-defined Networks (SDN).

Check Point Software-defined Protection

Check Point provides all the right components needed to implement a complete SDP architecture with the best management and the best security.

Check Point software-defined protections provide the flexibility needed to cope with new threats and embrace new technologies. Our solutions generate new and updated protections for known and unknown threats and proactively distribute this knowledge through the cloud. Implementing Check Point security solutions based on sound architectural security design empowers enterprises to embrace leading-edge information system solutions with confidence.



CHECK POINT SDP ENFORCEMENT LAYER

To secure the boundaries of each segment, Check Point offers a wide range of enforcement points. These include high-performance network security appliances, virtual gateways, endpoint host software and mobile device applications (Check Point Capsule) which enables you to extend security from the corporate network, and apply it to your mobile devices. Check Point provides enterprises with all the building blocks needed to engineer segmented, consolidated and secure systems and networks.

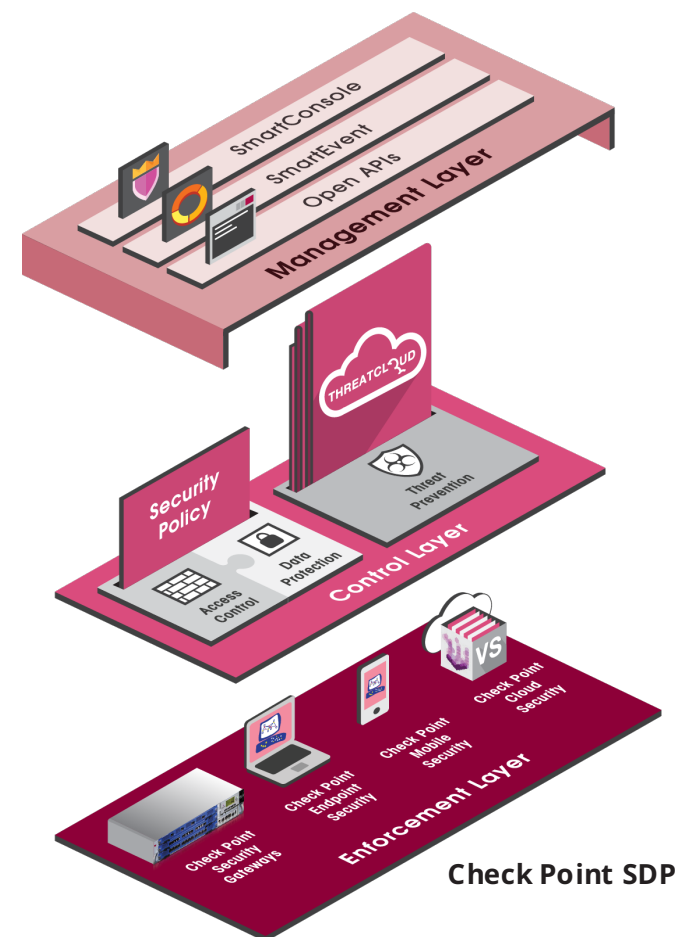


CHECK POINT SDP CONTROL LAYER

Check Point SDP control layer is based on Check Point Software Blade Architecture that provides customers with flexible and effective security solutions to match their exact needs. With a choice of over 20 Software Blades, the modular nature of the Software Blade Architecture allows customers to build a relevant security solution per enforcement point and to expand their security infrastructure over time.

Next Generation Threat Prevention

Check Point efficiently delivers controls to counter many of the known and unknown threats. The Check Point Threat prevention solution includes: Integrated Intrusion Prevention System (IPS) to proactively prevent intrusions, network based Antivirus to identify and block malware, Anti-bot to detect and prevent bot damage, Threat Emulation Threat Emulation malware sandboxing to detect and block unknown and zero-day attacks. Check Point built a unique cloud-based threat intelligence big data and protection generator, Check Point ThreatCloud™. Check Point ThreatCloud enables a collaborative way to fight cybercrime, delivering real-time security threat intelligence converted into security indicators to the control layer.



Check Point SDP

Next Generation Firewall and Secure Web Gateway

Check Point access control is based on multiple software blades which enable a unified contextbased security policy: Firewall to securely control access to clients, servers, applications and connection types. Application Control to control usage of Web 2.0 applications and prevent high-risk applications usage. URL Filtering to control access to millions of web sites and prevent access to websites hosting malware. And Identity Awareness for granular visibility of users, groups and machines and creation of accurate, identity-based policies.

Next Generation Data Protection

Next Generation Data Protection solutions encompass all facets of protecting content from getting into the wrong hands. Data Loss Prevention (DLP) is an integral part of a data protection solution helping businesses to pre-emptively protect sensitive information from unintentional loss, educating users on proper data handling policies and empowering them to remediate incidents in real-time. DLP controls sensitive information from leaving the company and it also inspects and controls sensitive emails between departments with Microsoft Exchange support. In addition, Check Point provides protection for data at rest and in storage with encryption technologies. These technologies can be implemented on all

enforcement points protecting sensitive documents and confidential data from being accessed or transferred to removable media or by unauthorized users.

Check Point Capsule: Extending Corporate Security Policy to Mobile Devices

Check Point Capsule enables you to extend Check Point's security from the corporate network, and apply it to your mobile devices. This way both your network and your employees' mobile devices enforce the same protections against internal and external threats. With Check Point Capsule you are able to access corporate email, documents, and internal directories and assets from within a secure business environment. Personal data and applications are segregated from business data, enabling secure use of business assets while protecting employee's personal information and applications. Business documents are protected everywhere they go with Check Point Capsule. Security is established at document creation, and travels with the document everywhere it goes, ensuring that corporate security guidelines are always enforced.



CHECK POINT SDP MANAGEMENT LAYER

All Check Point protections and enforcement points are managed from a single unified security management console. Check Point security management is highly scalable, providing the ability to manage tens of millions of objects while maintaining super-fast user interface response times.

Check Point Modular / Layered Policy Management

Check Point Security Management support the enterprise segmentation, allowing administrators to define security policy for each segment while enforcing segregation of duties with a new concept called Layers and Sub Layers. Policies can be defined for each segment. Access control policies can be defined using separate layers, which can be assigned to different administrators. Multiple administrators can then work on the same policy simultaneously.

Automation and Orchestration

Check Point Security Management provides CLIs and Web Services APIs that allow organizations to integrate with other systems such as network management, CRM, trouble ticketing, identity management and cloud orchestrators.

Visibility with Check Point

SmartEvent

Check Point SmartEvent performs big data analysis and real-time security event correlation. It offers the ability to provide a consolidated and correlated view of an incident based on multiple sources of information. Security event analysis creates actionable intelligence in the form of threat indicators that can be distributed via ThreatCloud to block threats in real-time.

Learn more about Check Point Software-defined Protection and how it can help your security infrastructure keep pace with today's rapidly changing threat landscape.

Visit:

www.checkpoint.com/sdp

About Check Point

Check Point Software Technologies' mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point has extended its IT security innovation with the development of our Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Check Point develops markets and supports a wide range of software, as well as combined hardware and software products and services for IT security. We offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified

security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is supported by, and reinforced with, real-time security updates.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

www.checkpoint.com