Check Point®
SOFTWARE TECHNOLOGIES LTD

Internet Web Access

Security Best Practices

ABSTRACT

This document aims to explain the Check Point approach to securing access to Internet. It provides architectural references for what, why and how organizations should consider when securing access to Internet in modern and effective way.

Contents

BUSINESS DRIVERS FOR SECURE WEB ACCESS

Today, the Internet has become an instrumental part of business operation. Being connected is essential to running a modern-day company. The evolution of web-applications has increased the complexity of our interactions with the internet; with this comes an increased security risk. Some of these include:

- Malware threats: Popular applications can be manipulated and weaponized against the users to propagate malware.
- Exploits: File-sharing programs, forums etc. are exploited by bad actors and used to propagate malware and pivot into networks.
- Bandwidth hogging: Applications that use a lot of bandwidth, such as streaming media, can limit the bandwidth that is available for alternate applications, which may be more crucial for business operation.

- Loss of Productivity: Employees are known to spend time on social networking sites, and other applications, which can seriously decrease business productivity. As employers are not aware of the extent of the misuse of company time, they are unable to effectively track how their business is affected by such practices.

An effective web access solution should fulfill the following requirements:

- High Security: Protect against known and unknown threats including sophisticated multi-vector cyber-attacks. Prevent infection and mitigate post-infection risk if necessary.

- Easy Administration: Simple and intuitive management consoles, unified policies, single point of logging and monitoring.

- User Interaction: Educate employees on proper Internet usage, and highlight inappropriate use and Internet dangers thought user feedback.

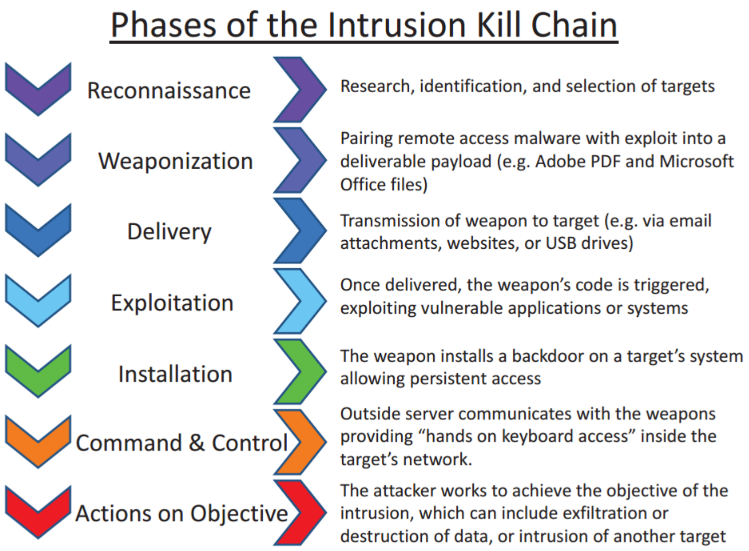
- Low TCO: Consolidated and automated security infrastructure will result in savings on both capital expenditure and operating expenses.

UNDERSTANDING THE CYBER KILL CHAIN

Unfortunately, there is no way to protect the entire network with a single product. In order to build an appropriate defense and choose a proper set of solutions, it is important to understand the “Cyber kill chain”, as coined by the Lockheed Martin Corporation. The kill chain model proposes that although attacks may occur in phases, each can be disrupted through strategically established controls.

Lockheed Martin illustrate a how a cyber threat impacts a network through a cyber-attack model, whereby the attack progresses through several stages; beginning with the initial infiltration and culminating in total data capture. The progression of the attack can be viewed as follows:

- Reconnaissance: The intruder selects a target, researches it, and attempts to identify vulnerabilities in their network.
- Weaponization: A remote access malware weapon is created, such as a virus or worm, tailored to capitalize on one or more vulnerabilities.
- Delivery: The weapon is transmitted to the target (e.g. via e-mail attachments, websites or USB drives).
- Exploitation: The weapon's program code is triggered and takes action on the target network to exploit its vulnerability.
- Installation: The malware weapon installs an access point (e.g. "backdoor") to be used by the intruder for persistent access to the target network.
- Command and Control: The intruder now has "hands on the keyboard" access, as a result of the communication and access provided by the malware weapon.
- Actions on Objective: The intruder is now free to successfully take action and achieve their intended goals; such as data exfiltration, data destruction, or encryption for ransom.



Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

The cyber kill chain along with our knowledge of user behaviour has lead organistaion to adopt a multi-point approach to protecting from internet-based threats and specifically threats presented to user. The following paper outlines some common best-practice architecture that aims to reduce the attack surface for user-egress traffic and limit the blast-radius of attacks should they be able to infect users.

Security professionals world-wide are aware of the threats posed by users and the intent; the following best-practice is the first line in protecting organisation where these dangers exist.

How to protect your business from today's cyber threats

In the current cyber environment, where multiple attack vectors are far too common, it is not enough to only rely on the security gateway.

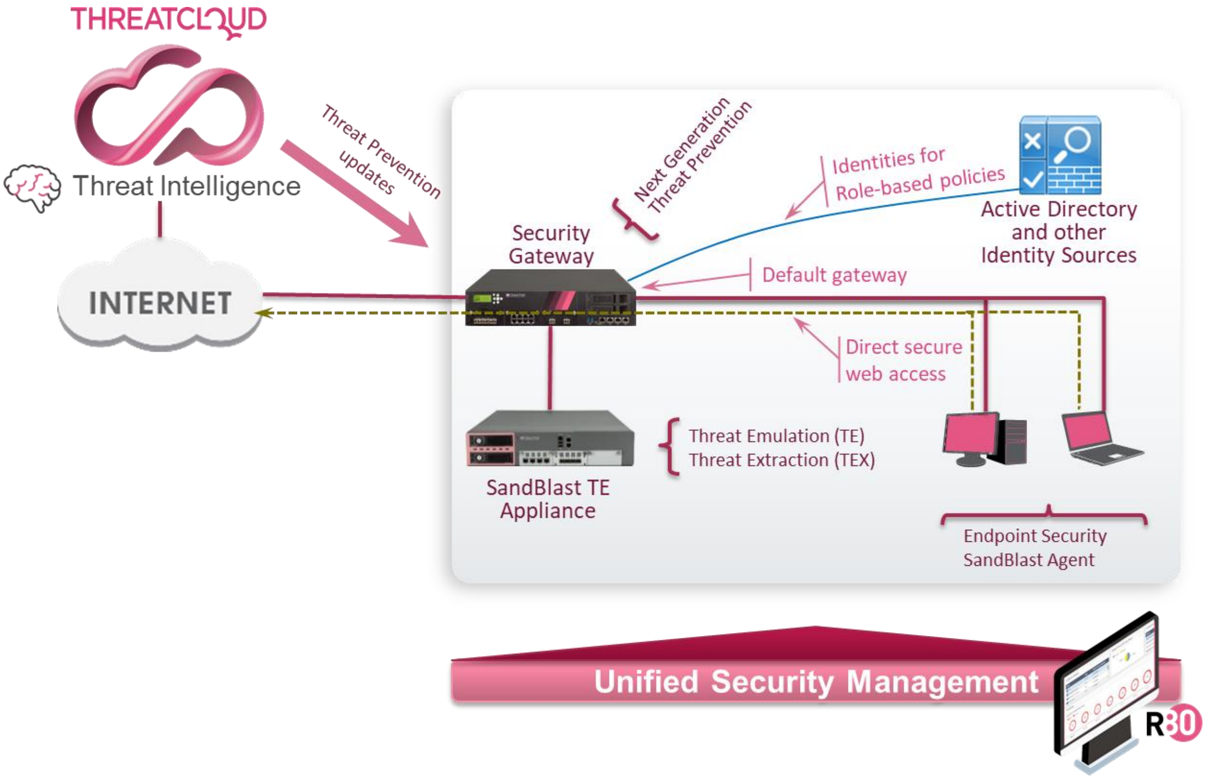
Defensive courses of action must be taken against the cyber kill chain:

- Detect: Determine whether an intruder has gained interest in the company network.
- Deny: Prevent information disclosure and unauthorized access.
- Disrupt: Stop or change outbound traffic (to the intruder).
- Degrade: Counter-attack unauthorized command and control.
- Deceive: Interfere with a command and control attack.
- Contain: Initiate network segmentation changes.

It is necessary to build a fully consolidated cyber security architecture that will provide protection against the latest and most advanced cyber-attacks at every stage, as well as future cyber threats across all networks, endpoint, cloud and mobile.

Check Point offers ultimate security architecture; designed to resolve the complexities of growing connectivity and inefficient security, and allow enterprises to integrate aligned security architecture into their current security strategy, rather than rely on point solutions.

This architecture is able to protect threats coming through networks, endpoint, cloud and mobile.


THREATCLOUD
Threat Intelligence
INTERNET
Threat Prevention updates
Next Generation Threat Prevention
Security Gateway
Identities for Role-based policies
Active Directory and other Identity Sources
Default gateway
Direct secure web access
Threat Emulation (TE)
Threat Extraction (TEX)
SandBlast TE Appliance
Endpoint Security SandBlast Agent
Unified Security Management
R80

Routed traffic inspection

Check Point's solution is simple, yet powerful and includes various technologies capable of stopping an attack at every stage of the kill chain. It also intends to combine protection at the network level and at the endpoint itself.

This holistic product is vital for forward thinking businesses, as Endpoint Security provides an extra layer of protection guarding beyond threats, which can be stopped at the perimeter using powerful security gateways, especially since the internet is not the only attack vector.

CHECK POINT PUT TO THE TEST

NSS Labs, Inc. released results for its 2019 Breach Prevention Systems (BPS) Group Test and recognized Check Point Next Generation Threat Prevention Appliance with Endpoint Security, as NSS Labs Recommended.

The NSS Labs BPS report significantly incorporates multiple solutions that enable a vendor to provide a breach prevention posture to its customers. Involving multiple solutions provides synergy between various security components that, when combined, effectively block attacks throughout the cyber kill chain. In Check Point's case, the solution involved a myriad of technologies such as SandBlast Network, SandBlast Agent, threat extraction, anti-bot and more.

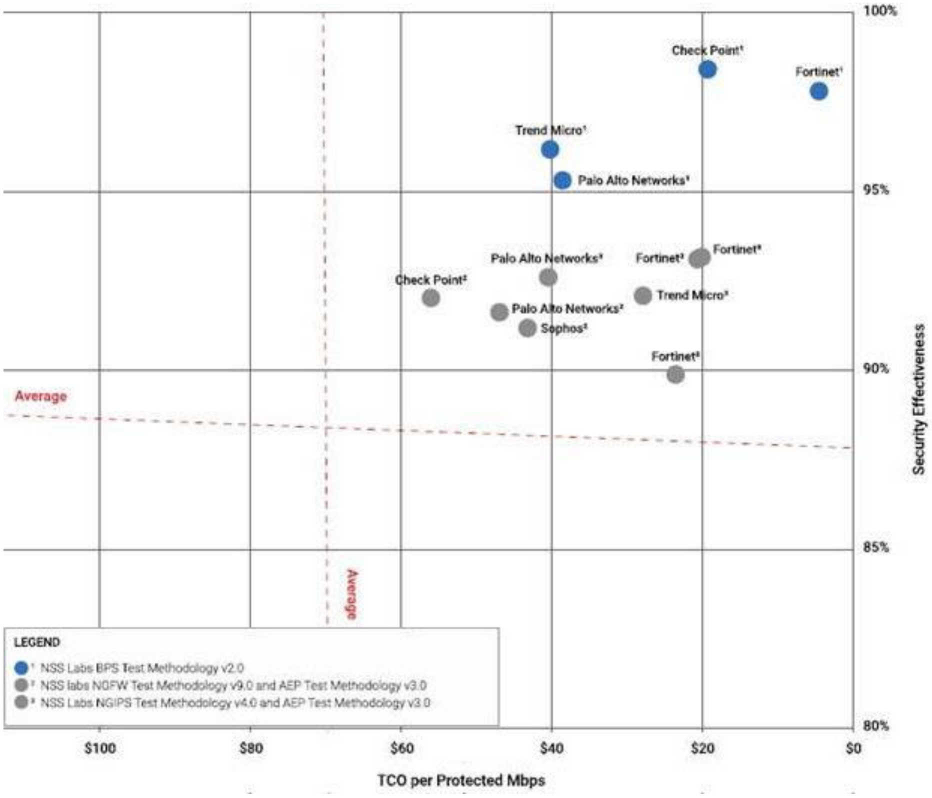
NSS LABS RECOMMENDED

In the introduction to its analysis of the BPS Security Value Map, NSS Labs wrote: “The Breach Prevention Systems (BPS) Security Value Map (SVM) is based upon data collected over thousands of hours of testing during NSS’ most recent tests including our Next Generation Firewall (NGFW), Next Generation Intrusion Prevention Systems (NGIPS), Breach Prevention Systems (BPS), and Advanced Endpoint Protection (AEP) Group Tests”.

These results mark Check Point’s third NSS Labs Recommended, in 2019, and the 20th NSS Labs Recommended rating since the company began testing with NSS in 2010.

Download the report and Security Value Map to learn more about the NSS Labs test and how Check Point performed:

- Clear #1 ranking in breach prevention posture
- #1 in NGFW + AEP combined
- Demonstrated significant added value when using network and endpoint protections together (Infinity)
- 100% block rate
- 100% malware PREVENTION, email and web
- 100% exploit resistance
- 100% catch rate in post infection
- 98.4% Overall Security Effectiveness
- 0% False positives

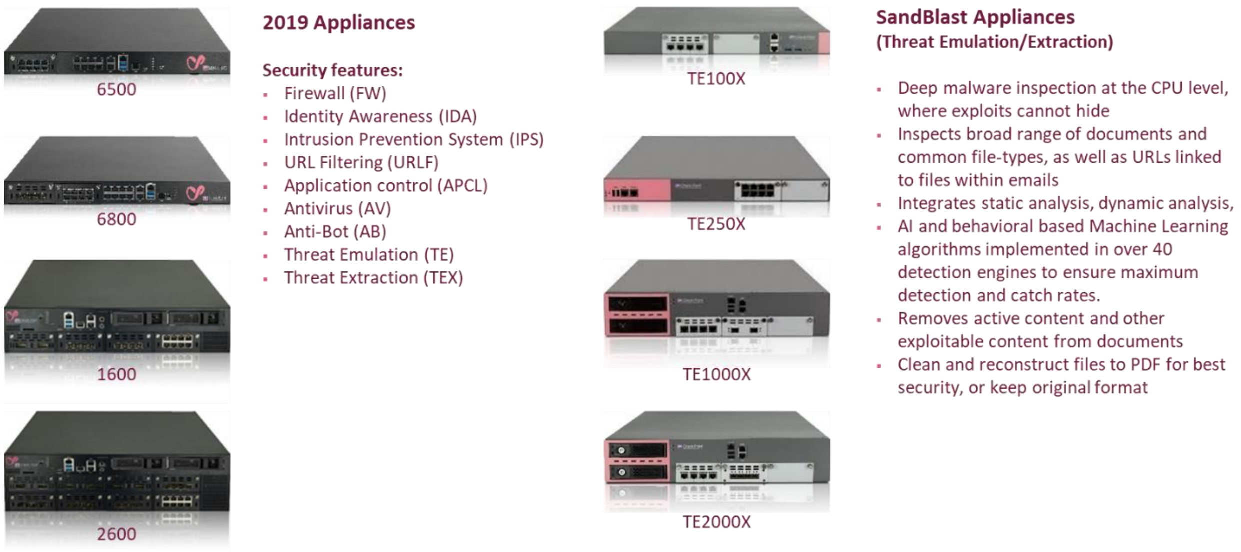


Security Value Map NSS Labs BPS

View Check Point’s other awards and recognitions: https://www.checkpoint.com/about-us/awards-and-recognition/

Check Point products and features

Network protection



2019 Appliances

Security features:

- Firewall (FW)
- Identity Awareness (IDA)
- Intrusion Prevention System (IPS)
- URL Filtering (URLF)
- Application control (APCL)
- Antivirus (AV)
- Anti-Bot (AB)
- Threat Emulation (TE)
- Threat Extraction (TEX)

SandBlast Appliances
(Threat Emulation/Extraction)

- Deep malware inspection at the CPU level, where exploits cannot hide
- Inspects broad range of documents and common file-types, as well as URLs linked to files within emails
- Integrates static analysis, dynamic analysis,
- AI and behavioral based Machine Learning algorithms implemented in over 40 detection engines to ensure maximum detection and catch rates.
- Removes active content and other exploitable content from documents
- Clean and reconstruct files to PDF for best security, or keep original format

Comprehensive threat protection is available in two simple packages for Check Point appliances:

- Next Generation Threat Prevention (NGTP): Includes multi-layered protection from known, signature-based threats including Antivirus, Anti-Bot, IPS, App Control, URL Filtering and Identity Awareness.
- Next Generation Threat Prevention & SandBlast™ (NGTX): Extends NGTP multi-layered protection with zero-day attacks protection using SandBlast Threat Emulation / SandBlast Threat Extraction.
- Threat Emulation and Treat Extraction: Protects against unknown zero-day attacks by detecting and blocking evasion-resistant malware, while rapidly delivering safe content to users. Delivered as a SandBlast appliance or as a cloud service.

Real-time security intelligence delivered from ThreatCloud:

- Leverage the industry's first collaborative network to fight cybercrime.
- Identify over 280 million addresses analyzed for bot discovery, over 12 million malware signatures and 1 million malicious websites.
- Dynamically update attack information from a worldwide network of sensors and the industry's best malware feeds.
- Combine information on remote operator hideouts, botnet communication patterns and attack behavior to accurately identify bot outbreaks.
- Receive up-to-the-minute bot intelligence from the ThreatCloud knowledgebase, including zero-day bot attacks discovered by Check Point Threat Emulation.

Protection from malicious downloads and applications:

- Identify websites delivering malware.
- Prevent malicious files from being downloaded.
- Acceleration technologies ensure high threat prevention performance.

– Enable specific applications while blocking risky or insecure applications.

Policy Enforcement

Firewall	Limits network access to only permitted services and allowed network segments
Identity Awareness	Limits access to users with the proper credentials i.e. only to those who have authorized access
Application Control	Limits access to approved applications and enable and educate users on safe use of the Internet
URL Filtering	Limits access to approved sites and enable safe use of the Internet

Threat Prevention

IPS	Enables virtual-patching of network services and applications that may be vulnerable to exploits
Antivirus	Prevents known malware
Anti-Bot	Detects and block bot behaviors and communications with known Command and Control servers
Anti-Spam	Detects and block known email sources of spam
Sandboxing	Inspects files for malicious content and behaviors
Threat Extraction	Delivers safe content to users while files are analyzed in the background

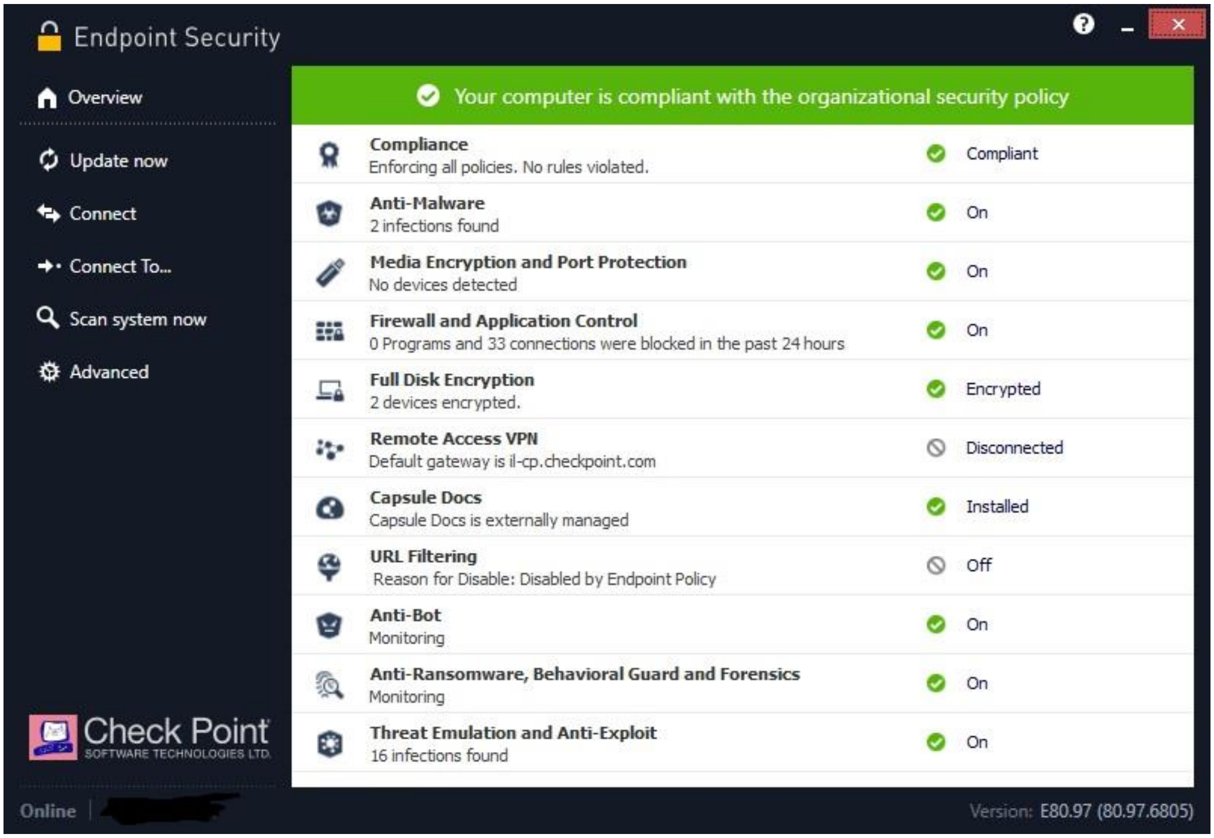
Data Protection

Content Awareness	Restricts the Data Types that users can upload or download
Data Loss Prevention	Protects personal healthcare information (PHI), personally identifiable information (PII), financial data and others

Additional Features

SSL Decryption	Performs analysis inside the encrypted traffic
User Check	Interacts with users in case of incidents, educate users on safe use of the Internet
Proxy	Supports legacy connection methods

Endpoint Protection



Endpoint Security

- Overview
- Update now
- Connect
- Connect To...
- Scan system now
- Advanced

Your computer is compliant with the organizational security policy

Compliance Enforcing all policies. No rules violated.	Compliant
Anti-Malware 2 infections found	On
Media Encryption and Port Protection No devices detected	On
Firewall and Application Control 0 Programs and 33 connections were blocked in the past 24 hours	On
Full Disk Encryption 2 devices encrypted.	Encrypted
Remote Access VPN Default gateway is il-cp.checkpoint.com	Disconnected
Capsule Docs Capsule Docs is externally managed	Installed
URL Filtering Reason for Disable: Disabled by Endpoint Policy	Off
Anti-Bot Monitoring	On
Anti-Ransomware, Behavioral Guard and Forensics Monitoring	On
Threat Emulation and Anti-Exploit 16 infections found	On

Check Point SOFTWARE TECHNOLOGIES LTD.

Online | [redacted]

Version: E80.97 (80.97.6805)

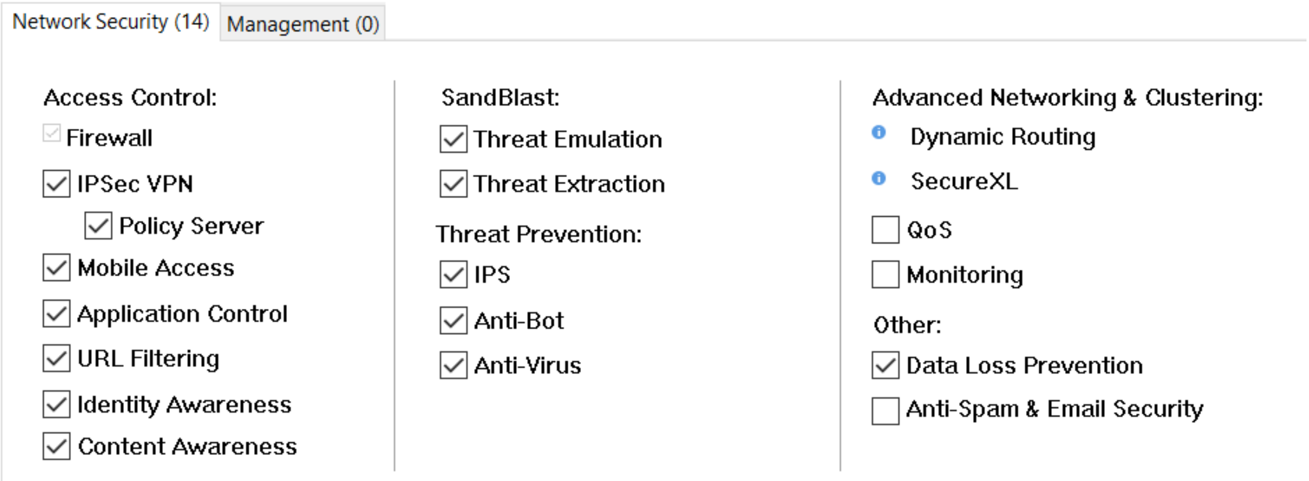
Endpoint Security Client + SandBlast Agent protections installed on the endpoints

Firewall and Compliance	Limits network access to only allowed services and allowed network segment building Zones
Anti-Bot	Detects and blocks bot behaviors and communications with known Command and Control servers
Antimalware	Detects and remediates all forms of malicious behavior including zero-day malware
Safe Browsing Anti-Ransomware Anti-Phishing	Prevents access to malicious websites Prevents cyber-extortion attacks and automatically reverses any damage done to files from the attack Detects and blocks malicious URLs sent to the device
Forensics	Monitors and records all endpoint events: files affected, processes launched, registry changes, network activity
Media Encryption	Enforces encryption of removable storage media
Full Disk Encryption	Secures all information on endpoint hard drives including user data and Operating System files

A combination of the Security Gateway and Endpoint protections ensures that a business is secure at every stage of the cyber kill chain and lets them maximize protection through unified management, monitoring and reporting.

HOW TO INTEGRATE NEW SOLUTIONS INTO EXISTING SYSTEMS

Check Point customers can easily enable additional features on their current Internet gateway[1].



Network Security (14) | Management (0)

Access Control:
- ☑ Firewall
- ☑ IPSec VPN
  - ☑ Policy Server
- ☑ Mobile Access
- ☑ Application Control
- ☑ URL Filtering
- ☑ Identity Awareness
- ☑ Content Awareness

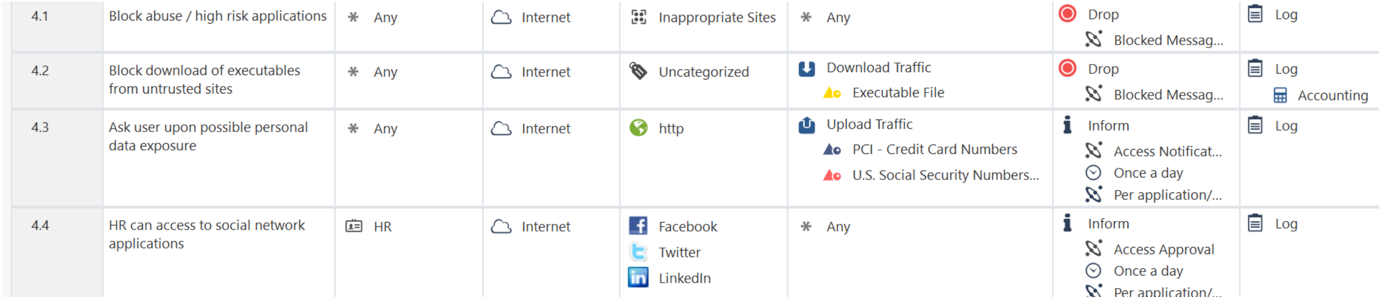
SandBlast:
- ☑ Threat Emulation
- ☑ Threat Extraction

Threat Prevention:
- ☑ IPS
- ☑ Anti-Bot
- ☑ Anti-Virus

Advanced Networking & Clustering:
- ● Dynamic Routing
- ● SecureXL
- □ QoS
- □ Monitoring

Other:
- ☑ Data Loss Prevention
- □ Anti-Spam & Email Security

Gateway security features

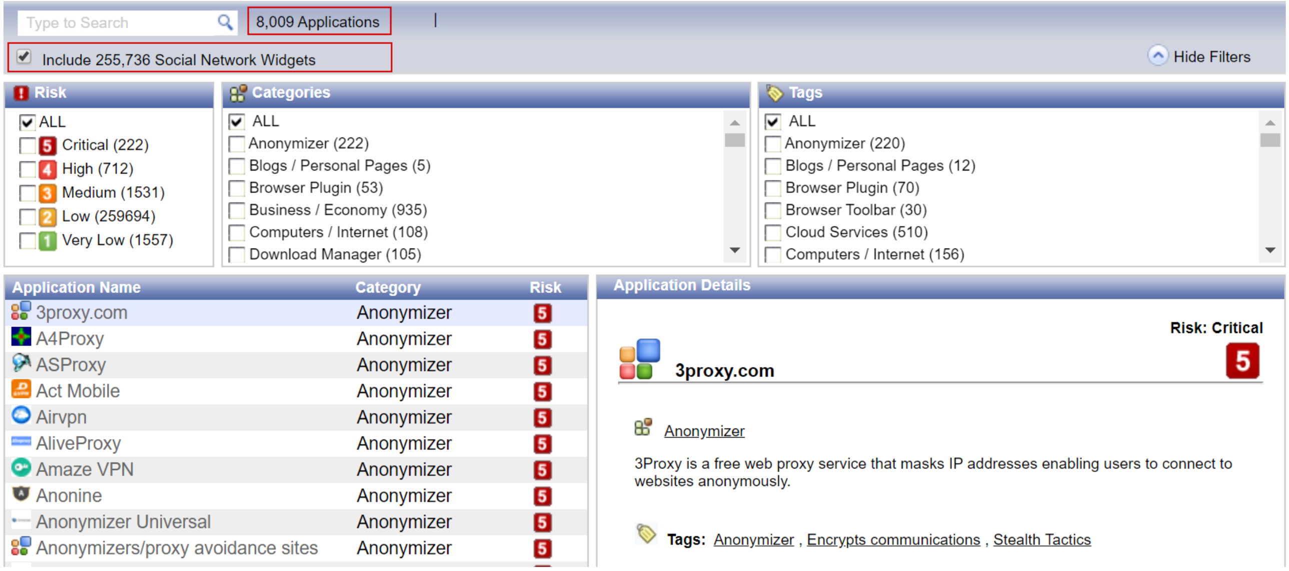


4.1	Block abuse / high risk applications	Any	Internet	Inappropriate Sites	Any	Drop Blocked Messag...	Log
4.2	Block download of executables from untrusted sites	Any	Internet	Uncategorized	Download Traffic Executable File	Drop Blocked Messag...	Log Accounting
4.3	Ask user upon possible personal data exposure	Any	Internet	http	Upload Traffic PCI - Credit Card Numbers U.S. Social Security Numbers...	Inform Access Notificat... Once a day Per application/...	Log
4.4	HR can access to social network applications	HR	Internet	Facebook Twitter LinkedIn	Any	Inform Access Approval Once a day Per application/...	Log

Access policy fragment

List of applications and social network widgets are available at AppWiki (https://appwiki.checkpoint.com/):

[1] Most features include a 30 days trial period. Please note that this may affect network performance and user accessibility.



Type to Search | 8,009 Applications

☑ Include 255,736 Social Network Widgets

Hide Filters

Risk

☑ ALL
□ 5 Critical (222)
□ 4 High (712)
□ 3 Medium (1531)
□ 2 Low (259694)
□ 1 Very Low (1557)

Categories

☑ ALL
□ Anonymizer (222)
□ Blogs / Personal Pages (5)
□ Browser Plugin (53)
□ Business / Economy (935)
□ Computers / Internet (108)
□ Download Manager (105)

Tags

☑ ALL
□ Anonymizer (220)
□ Blogs / Personal Pages (12)
□ Browser Plugin (70)
□ Browser Toolbar (30)
□ Cloud Services (510)
□ Computers / Internet (156)

Application Name	Category	Risk
3proxy.com	Anonymizer	5
A4Proxy	Anonymizer	5
ASProxy	Anonymizer	5
Act Mobile	Anonymizer	5
Airvpn	Anonymizer	5
AliveProxy	Anonymizer	5
Amaze VPN	Anonymizer	5
Anonine	Anonymizer	5
Anonymizer Universal	Anonymizer	5
Anonymizers/proxy avoidance sites	Anonymizer	5

Application Details

Risk: Critical 5

3proxy.com

Anonymizer

3Proxy is a free web proxy service that masks IP addresses enabling users to connect to websites anonymously.

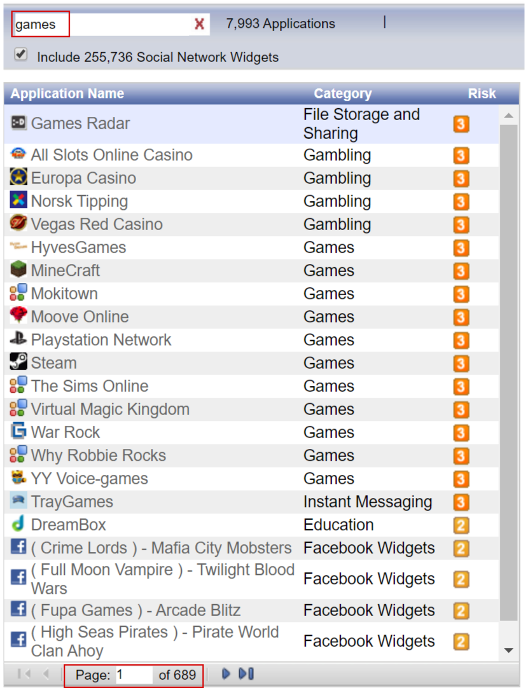
Tags: Anonymizer , Encrypts communications , Stealth Tactics

The application database is sizable (8000+ apps) and is grouped by multiple characteristics simplifying rule base creation. It also includes 250000+ social network widgets.

Typically, it is recommended to prohibit applications with critical risk for all users.

Administrators can block the Anonymizer category, which contains 200+ entries and automatically grows as the Check Point research team adds new anonymizers. This guarantees that users will be unable to bypass corporate policies, without extra effort from the administrator.

Furthermore, with a single rule administrators can block everything related to games, such as web sites, network games, social networks widgets and more. Categories are being updated automatically, so administrators need not be concerned when new games become available.



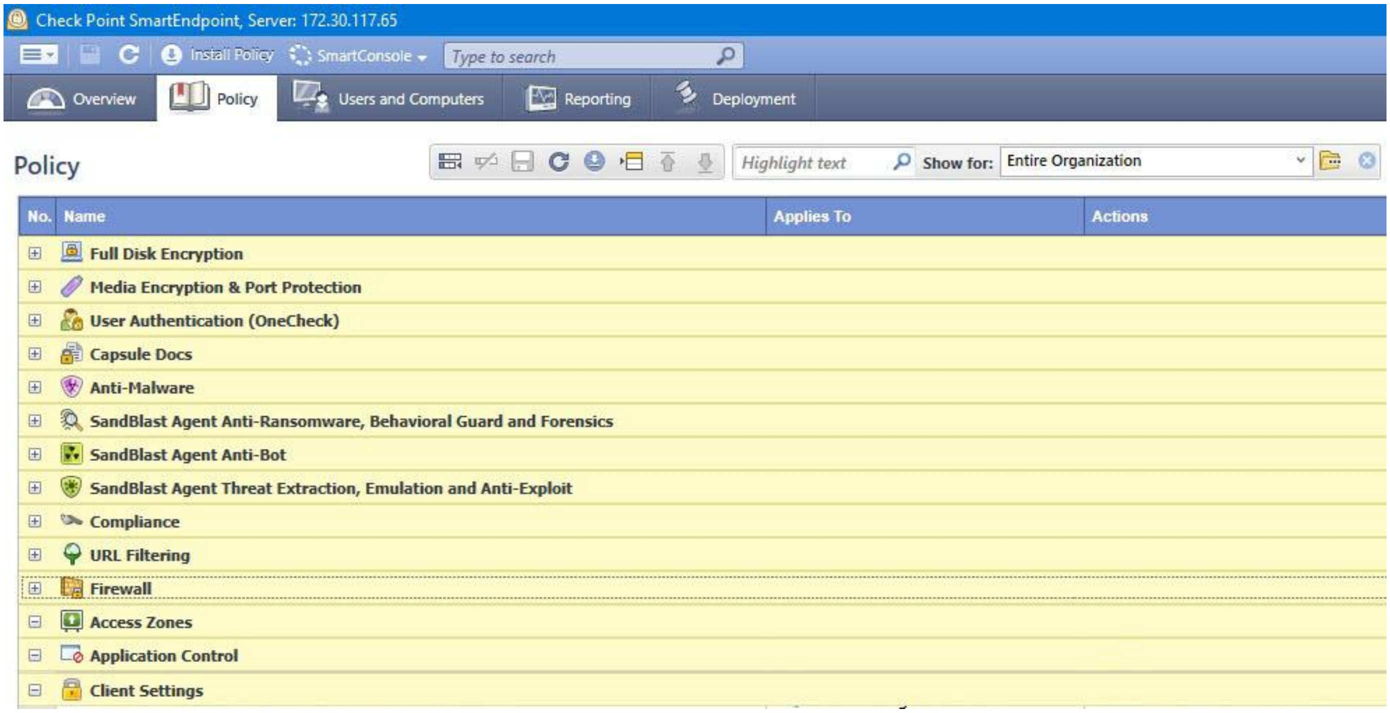
games | 7,993 Applications

☑ Include 255,736 Social Network Widgets

Application Name	Category	Risk
Games Radar	File Storage and Sharing	3
All Slots Online Casino	Gambling	3
Europa Casino	Gambling	3
Norsk Tipping	Gambling	3
Vegas Red Casino	Gambling	3
HyvesGames	Games	3
MineCraft	Games	3
Mokitown	Games	3
Moove Online	Games	3
Playstation Network	Games	3
Steam	Games	3
The Sims Online	Games	3
Virtual Magic Kingdom	Games	3
War Rock	Games	3
Why Robbie Rocks	Games	3
YY Voice-games	Games	3
TrayGames	Instant Messaging	3
DreamBox	Education	2
(Crime Lords) - Mafia City Mobsters	Facebook Widgets	2
(Full Moon Vampire) - Twilight Blood Wars	Facebook Widgets	2
(Fupa Games) - Arcade Blitz	Facebook Widgets	2
(High Seas Pirates) - Pirate World Clan Ahoy	Facebook Widgets	2

Page: 1 of 689

Games to block



No.	Name	Applies To	Actions
⊞	Full Disk Encryption		
⊞	Media Encryption & Port Protection		
⊞	User Authentication (OneCheck)		
⊞	Capsule Docs		
⊞	Anti-Malware		
⊞	SandBlast Agent Anti-Ransomware, Behavioral Guard and Forensics		
⊞	SandBlast Agent Anti-Bot		
⊞	SandBlast Agent Threat Extraction, Emulation and Anti-Exploit		
⊞	Compliance		
⊞	URL Filtering		
⊞	Firewall		
⊟	Access Zones		
⊟	Application Control		
⊟	Client Settings		

Endpoint Security Management Console (collapsed sections)

Check Point offers a consolidated security solution across both network and endpoint. This includes a unified Management Server for managing both the Network environment (gateways) and the endpoint environment (desktops / laptops / servers) from a single location.

Benefits:

- A single Management Server and a single SmartConsole assures easier administration and decreases time to deployment.
- The single Security Events Management platform provides near real time security monitoring across all layers. Having the relevant attack diagnostics and visibility enables organizations to respond quickly and remediate their systems in case of a security breach.
- Reduces hardware and licenses costs, as well as operational IT maintenance costs.

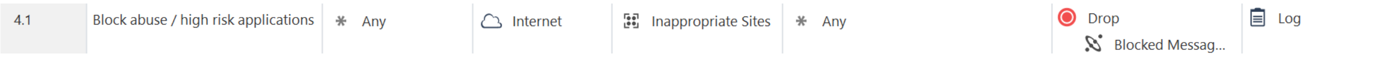
BEST PRACTICES FOR CONFIGURATION

1. Activate security blades on the Internet gateway in the SmartConsole

Use Access control (Application Control, URL Filtering, Identity Awareness, Content Awareness) as well as Threat Prevention and Sandblast (IPS, Anti-Bot, Anti-Virus, Threat Emulation Threat Extraction).

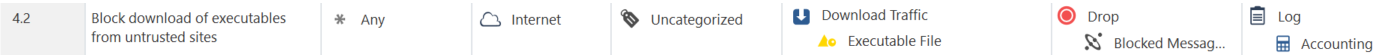
2. Build Network Security policy

- Block abuse/high risk applications.



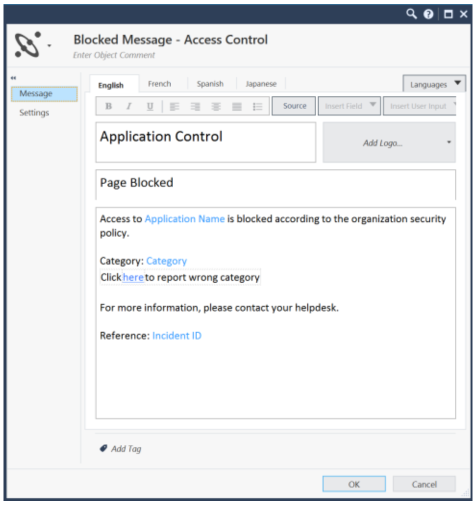
4.1	Block abuse / high risk applications	✱ Any	Internet	Inappropriate Sites	✱ Any	Drop Blocked Messag...	Log

– Block the download of executables (i.e. from untrusted sites).



4.2	Block download of executables from untrusted sites	Any	Internet	Uncategorized	Download Traffic Executable File	Drop Blocked Messag...	Log Accounting

– Inform users about block reason using the Blocked Message (User Check).



Blocked Message - Access Control

Enter Object Comment

Application Control

Page Blocked

Access to Application Name is blocked according to the organization security policy.

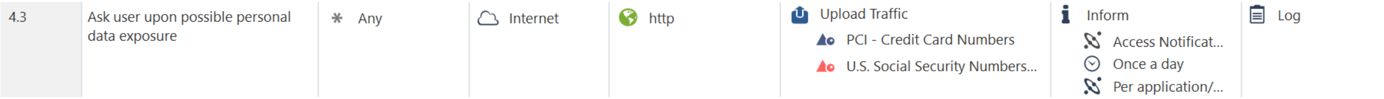
Category: Category

Click here to report wrong category

For more information, please contact your helpdesk.

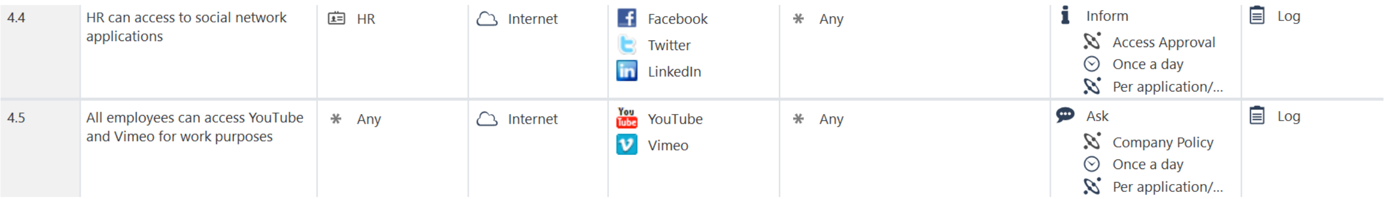
Reference: Incident ID

– Control user uploads to avoid confidential information leakage.



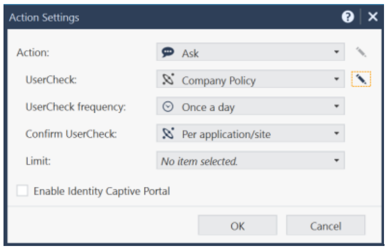
4.3	Ask user upon possible personal data exposure	Any	Internet	http	Upload Traffic PCI - Credit Card Numbers U.S. Social Security Numbers...	Inform Access Notificat... Once a day Per application/...	Log

– Create rules according to user roles (groups).



4.4	HR can access to social network applications	HR	Internet	Facebook Twitter LinkedIn	Any	Inform Access Approval Once a day Per application/...	Log
4.5	All employees can access YouTube and Vimeo for work purposes	Any	Internet	YouTube Vimeo	Any	Ask Company Policy Once a day Per application/...	Log

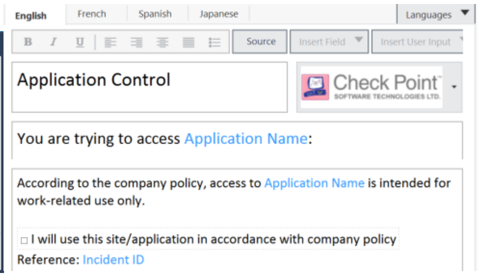
– Educate users on proper Internet usage.



Action Settings

Action:	Ask
UserCheck:	Company Policy
UserCheck frequency:	Once a day
Confirm UserCheck:	Per application/site
Limit:	No item selected.

□ Enable Identity Captive Portal



Application Control

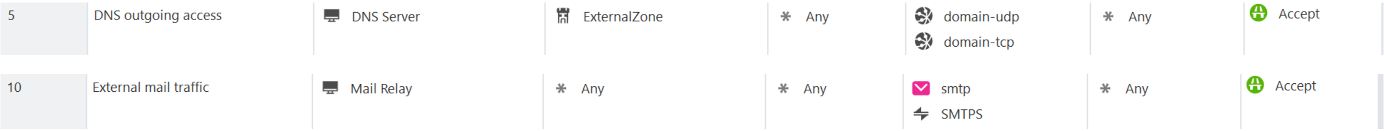
You are trying to access Application Name:

According to the company policy, access to Application Name is intended for work-related use only.

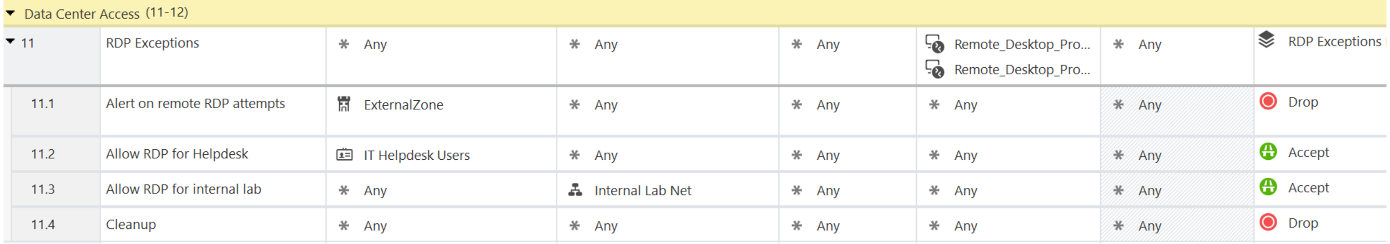
□ I will use this site/application in accordance with company policy

Reference: Incident ID

– In addition to outgoing web access, create other network access rules including Internet/DMZ, LAN and Data Center – all in the same console.



5	DNS outgoing access	DNS Server	ExternalZone	Any	domain-udp domain-tcp	Any	Accept
10	External mail traffic	Mail Relay	Any	Any	smtp SMTPS	Any	Accept

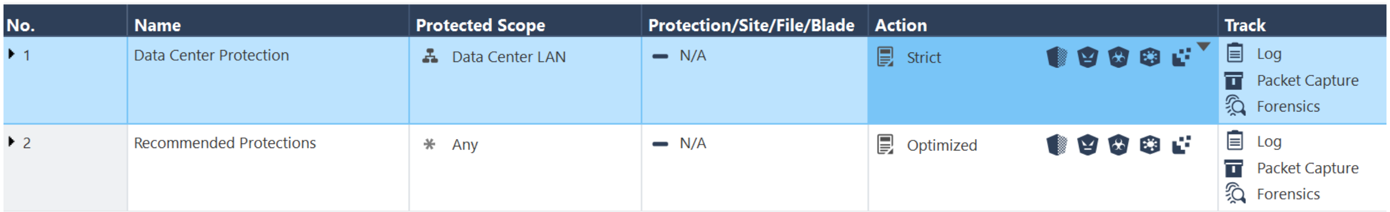


▼ Data Center Access (11-12)

▼ 11	RDP Exceptions	✻ Any	✻ Any	✻ Any	Remote_Desktop_Pro... Remote_Desktop_Pro...	✻ Any	RDP Exceptions
11.1	Alert on remote RDP attempts	ExternalZone	✻ Any	✻ Any	✻ Any	✻ Any	Drop
11.2	Allow RDP for Helpdesk	IT Helpdesk Users	✻ Any	✻ Any	✻ Any	✻ Any	Accept
11.3	Allow RDP for internal lab	✻ Any	Internal Lab Net	✻ Any	✻ Any	✻ Any	Accept
11.4	Cleanup	✻ Any	✻ Any	✻ Any	✻ Any	✻ Any	Drop

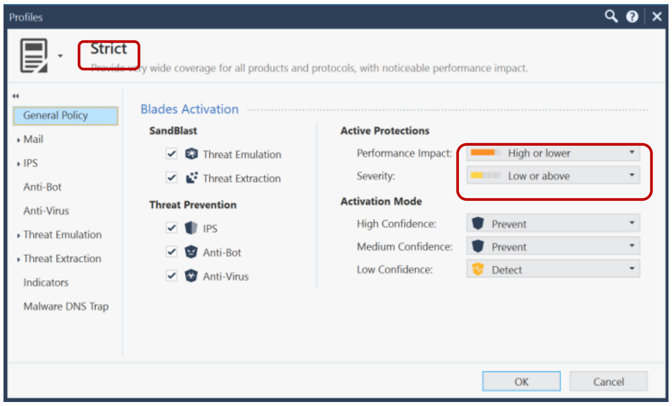
3. Build a Threat Prevention policy

   – Create rules for different scopes (the data center may require extra protections).



No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track
▸ 1	Data Center Protection	Data Center LAN	— N/A	Strict	Log Packet Capture Forensics
▸ 2	Recommended Protections	✻ Any	— N/A	Optimized	Log Packet Capture Forensics

   – Configure security profiles.



Profiles

Strict

Provide very wide coverage for all products and protocols, with noticeable performance impact.

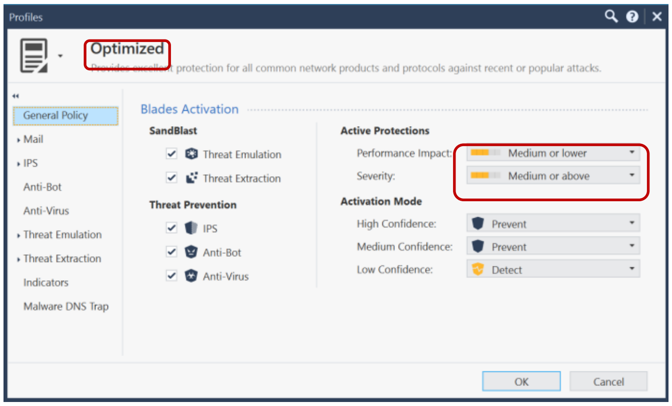
Blades Activation

SandBlast
- ☑ Threat Emulation
- ☑ Threat Extraction

Threat Prevention
- ☑ IPS
- ☑ Anti-Bot
- ☑ Anti-Virus

Active Protections
- Performance Impact: High or lower
- Severity: Low or above

Activation Mode
- High Confidence: Prevent
- Medium Confidence: Prevent
- Low Confidence: Detect



Profiles

Optimized

Provides excellent protection for all common network products and protocols against recent or popular attacks.

Blades Activation

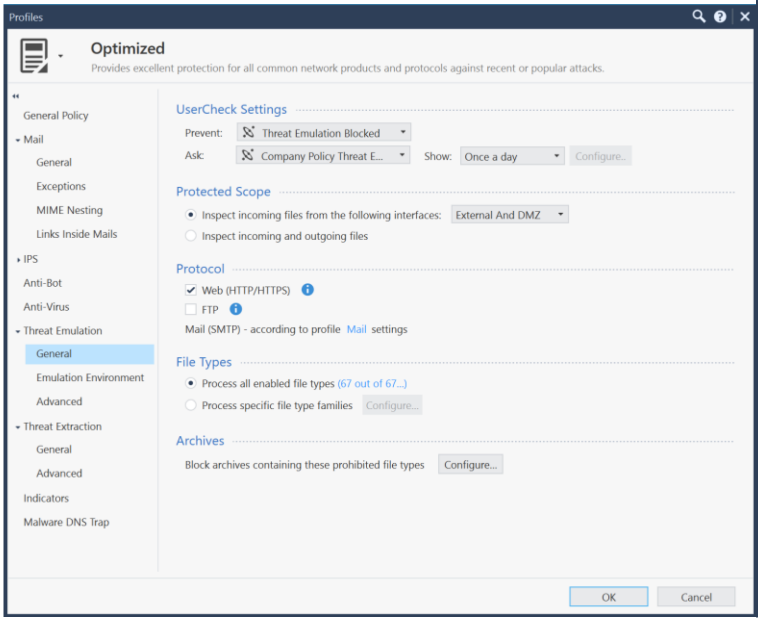
SandBlast
- ☑ Threat Emulation
- ☑ Threat Extraction

Threat Prevention
- ☑ IPS
- ☑ Anti-Bot
- ☑ Anti-Virus

Active Protections
- Performance Impact: Medium or lower
- Severity: Medium or above

Activation Mode
- High Confidence: Prevent
- Medium Confidence: Prevent
- Low Confidence: Detect

   – Configure Threat Emulation and Threat Extraction.



Profiles

Optimized

Provides excellent protection for all common network products and protocols against recent or popular attacks.

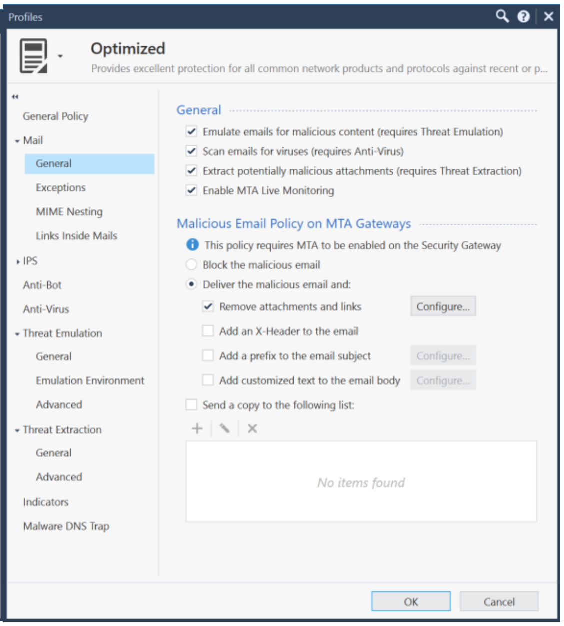
UserCheck Settings
- Prevent: Threat Emulation Blocked
- Ask: Company Policy Threat E... Show: Once a day Configure...

Protected Scope
- ● Inspect incoming files from the following interfaces: External And DMZ
- ○ Inspect incoming and outgoing files

Protocol
- ☑ Web (HTTP/HTTPS)
- □ FTP
- Mail (SMTP) - according to profile Mail settings

File Types
- ● Process all enabled file types (67 out of 67...)
- ○ Process specific file type families Configure...

Archives
- Block archives containing these prohibited file types Configure...



Profiles

Optimized

Provides excellent protection for all common network products and protocols against recent or p...

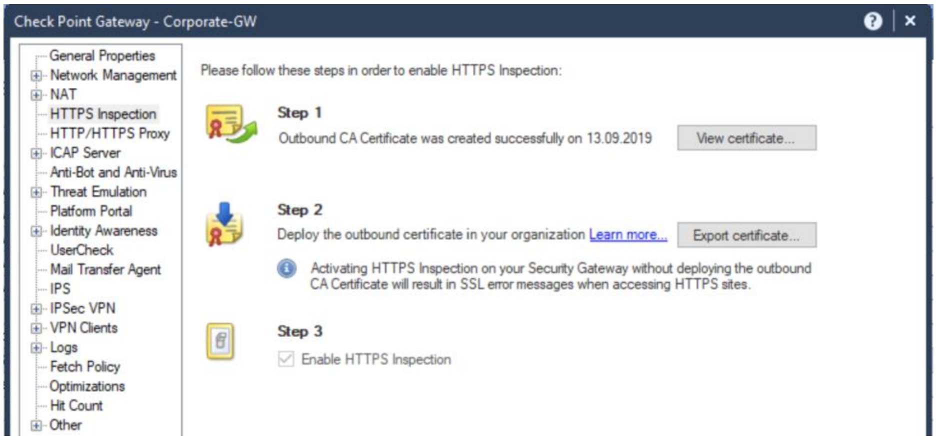
General
- ☑ Emulate emails for malicious content (requires Threat Emulation)
- ☑ Scan emails for viruses (requires Anti-Virus)
- ☑ Extract potentially malicious attachments (requires Threat Extraction)
- ☑ Enable MTA Live Monitoring

Malicious Email Policy on MTA Gateways
- This policy requires MTA to be enabled on the Security Gateway
- ○ Block the malicious email
- ● Deliver the malicious email and:
  - ☑ Remove attachments and links Configure...
  - □ Add an X-Header to the email
  - □ Add a prefix to the email subject Configure...
  - □ Add customized text to the email body Configure...
- □ Send a copy to the following list:

No items found

4. Activate Outgoing SSL Inspection to control encrypted traffic

- Choose relevant gateways.



Please follow these steps in order to enable HTTPS Inspection:

Step 1

Outbound CA Certificate was created successfully on 13.09.2019

Step 2

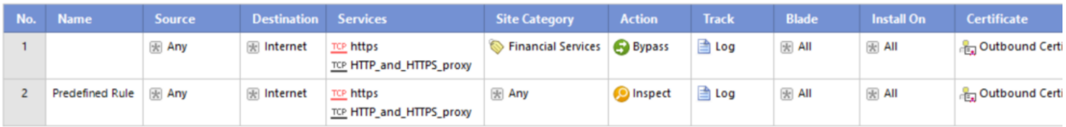
Deploy the outbound certificate in your organization Learn more...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

☑ Enable HTTPS Inspection

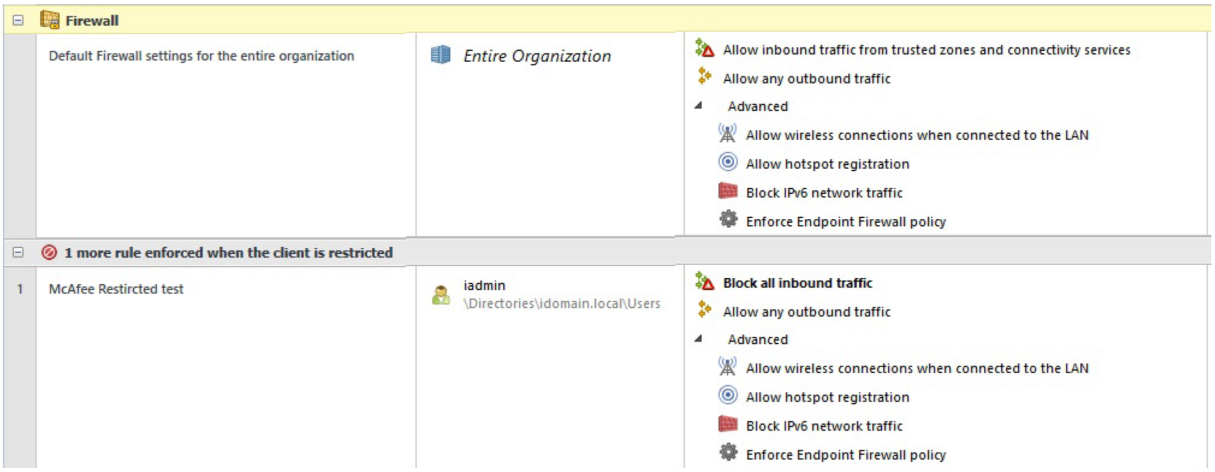
- Create exceptions if needed (for example, ‘do not inspect financial services to comply with legislation/privacy requirements’).



No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificate
1		Any	Internet	https HTTP_and_HTTPS_proxy	Financial Services	Bypass	Log	All	All	Outbound Certi
2	Predefined Rule	Any	Internet	https HTTP_and_HTTPS_proxy	Any	Inspect	Log	All	All	Outbound Certi

5. Configure Endpoint Security

- Access rules including NAC integration with 3rd party solutions.



Firewall

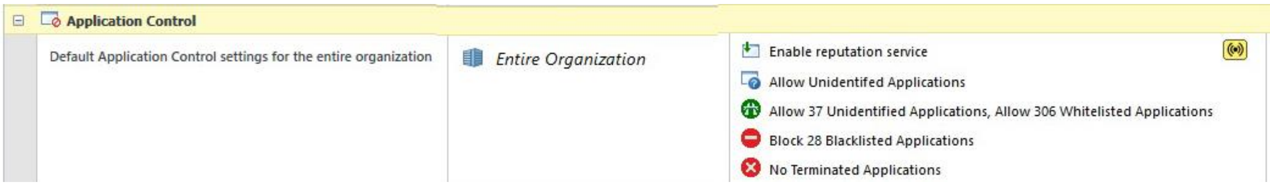
Default Firewall settings for the entire organization — *Entire Organization*

- Allow inbound traffic from trusted zones and connectivity services
- Allow any outbound traffic
- Advanced
  - Allow wireless connections when connected to the LAN
  - Allow hotspot registration
  - Block IPv6 network traffic
  - Enforce Endpoint Firewall policy

1 more rule enforced when the client is restricted

1 McAfee Restircted test — iadmin \Directories\idomain.local\Users

- **Block all inbound traffic**
- Allow any outbound traffic
- Advanced
  - Allow wireless connections when connected to the LAN
  - Allow hotspot registration
  - Block IPv6 network traffic
  - Enforce Endpoint Firewall policy

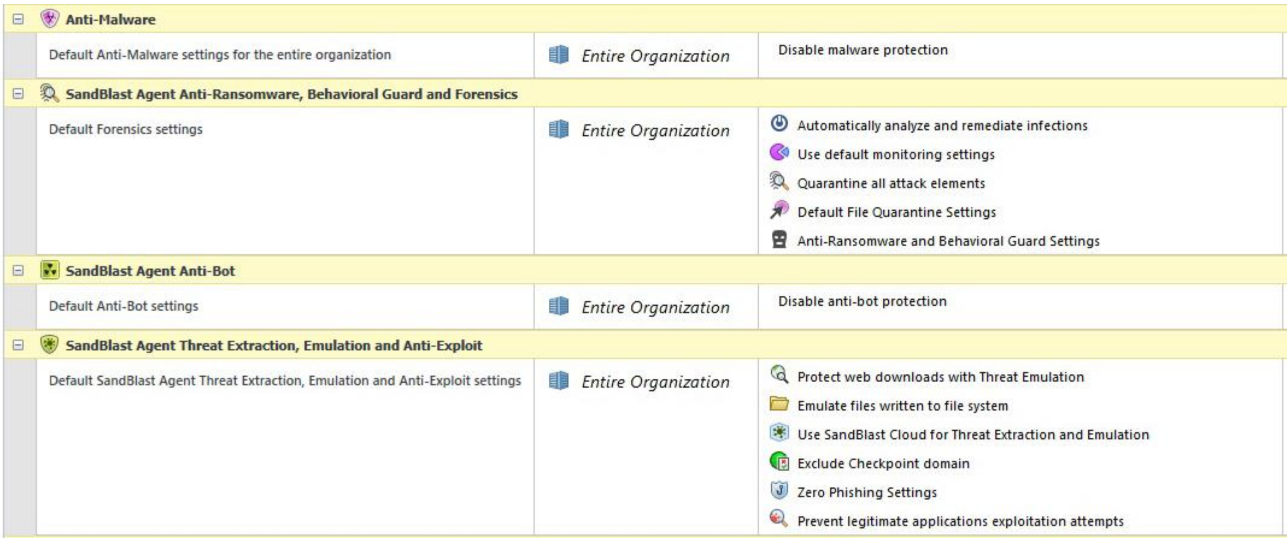


Application Control

Default Application Control settings for the entire organization — *Entire Organization*

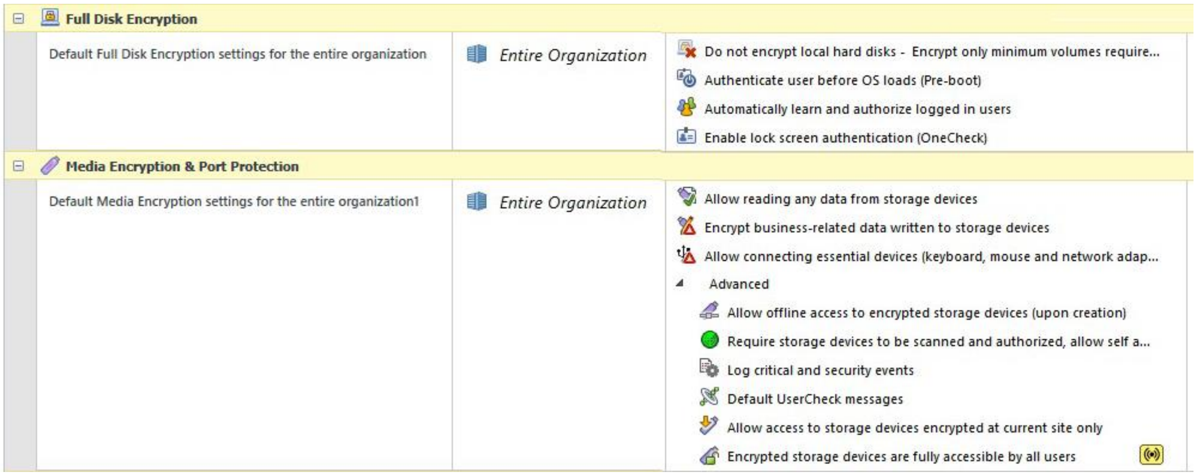
- Enable reputation service
- Allow Unidentifed Applications
- Allow 37 Unidentified Applications, Allow 306 Whitelisted Applications
- Block 28 Blacklisted Applications
- No Terminated Applications

- Threat Prevention blades.



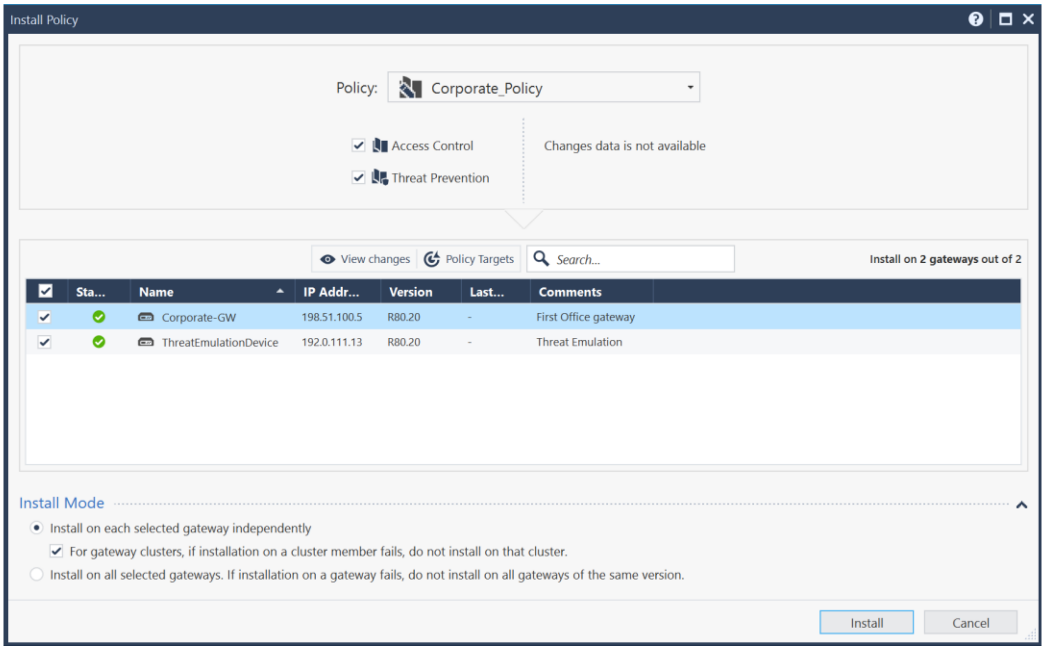
Anti-Malware		
Default Anti-Malware settings for the entire organization	*Entire Organization*	Disable malware protection
SandBlast Agent Anti-Ransomware, Behavioral Guard and Forensics		
Default Forensics settings	*Entire Organization*	Automatically analyze and remediate infections Use default monitoring settings Quarantine all attack elements Default File Quarantine Settings Anti-Ransomware and Behavioral Guard Settings
SandBlast Agent Anti-Bot		
Default Anti-Bot settings	*Entire Organization*	Disable anti-bot protection
SandBlast Agent Threat Extraction, Emulation and Anti-Exploit		
Default SandBlast Agent Threat Extraction, Emulation and Anti-Exploit settings	*Entire Organization*	Protect web downloads with Threat Emulation Emulate files written to file system Use SandBlast Cloud for Threat Extraction and Emulation Exclude Checkpoint domain Zero Phishing Settings Prevent legitimate applications exploitation attempts

– Add additional components if needed.



Full Disk Encryption		
Default Full Disk Encryption settings for the entire organization	*Entire Organization*	Do not encrypt local hard disks - Encrypt only minimum volumes require... Authenticate user before OS loads (Pre-boot) Automatically learn and authorize logged in users Enable lock screen authentication (OneCheck)
Media Encryption & Port Protection		
Default Media Encryption settings for the entire organization1	*Entire Organization*	Allow reading any data from storage devices Encrypt business-related data written to storage devices Allow connecting essential devices (keyboard, mouse and network adap... Advanced Allow offline access to encrypted storage devices (upon creation) Require storage devices to be scanned and authorized, allow self a... Log critical and security events Default UserCheck messages Allow access to storage devices encrypted at current site only Encrypted storage devices are fully accessible by all users

6. Publish and install the policy on all relevant gateways



Install Policy

Policy: Corporate_Policy

☑ Access Control
☑ Threat Prevention

Changes data is not available

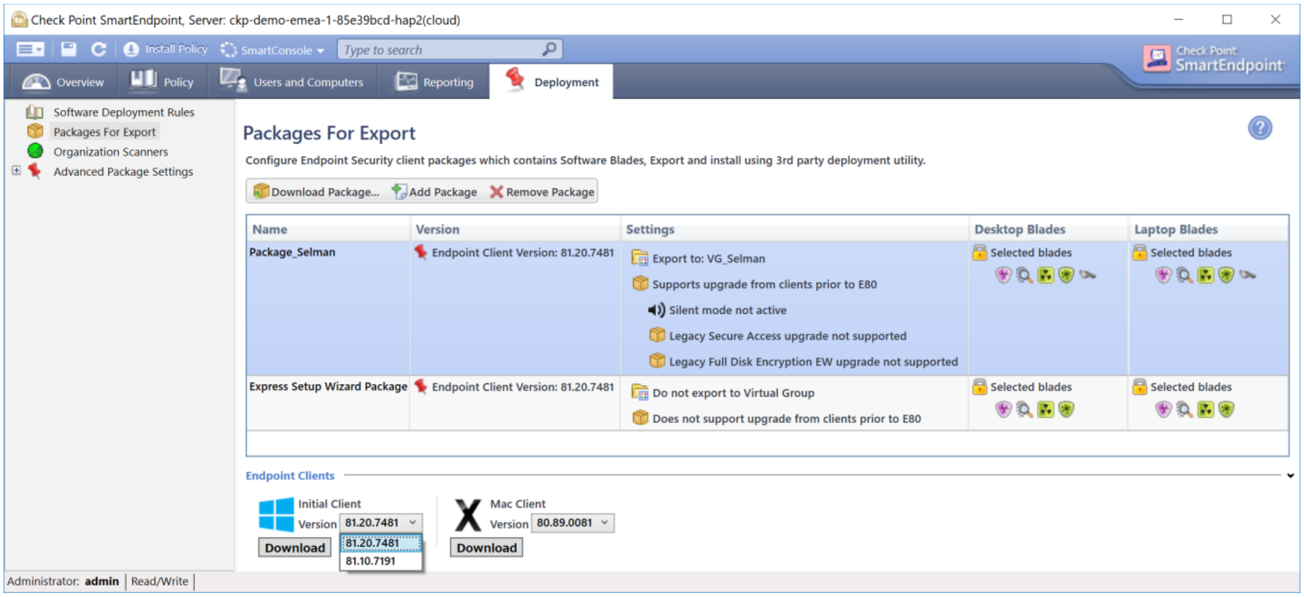
Install on 2 gateways out of 2

☑	Sta...	Name	IP Addr...	Version	Last...	Comments
☑	✓	Corporate-GW	198.51.100.5	R80.20	-	First Office gateway
☑	✓	ThreatEmulationDevice	192.0.111.13	R80.20	-	Threat Emulation

Install Mode

● Install on each selected gateway independently
☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.
○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

7. Deploy Endpoint Security clients



Check Point SmartEndpoint, Server: ckp-demo-emea-1-85e39bcd-hap2(cloud)

Packages For Export

Configure Endpoint Security client packages which contains Software Blades, Export and install using 3rd party deployment utility.

Name	Version	Settings	Desktop Blades	Laptop Blades
Package_Selman	Endpoint Client Version: 81.20.7481	Export to: VG_Selman Supports upgrade from clients prior to E80 Silent mode not active Legacy Secure Access upgrade not supported Legacy Full Disk Encryption EW upgrade not supported	Selected blades	Selected blades
Express Setup Wizard Package	Endpoint Client Version: 81.20.7481	Do not export to Virtual Group Does not support upgrade from clients prior to E80	Selected blades	Selected blades

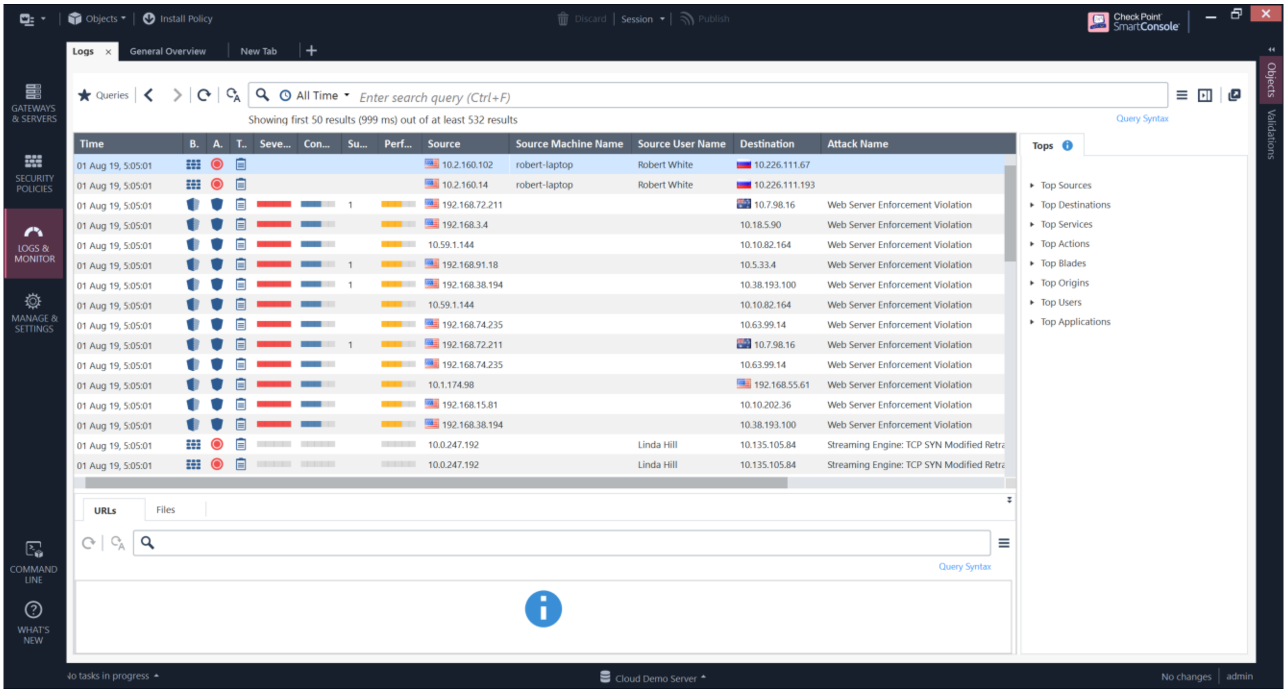
Endpoint Clients

Initial Client
Version 81.20.7481 (81.20.7481, 81.10.7191)
Download

Mac Client
Version 80.89.0081
Download

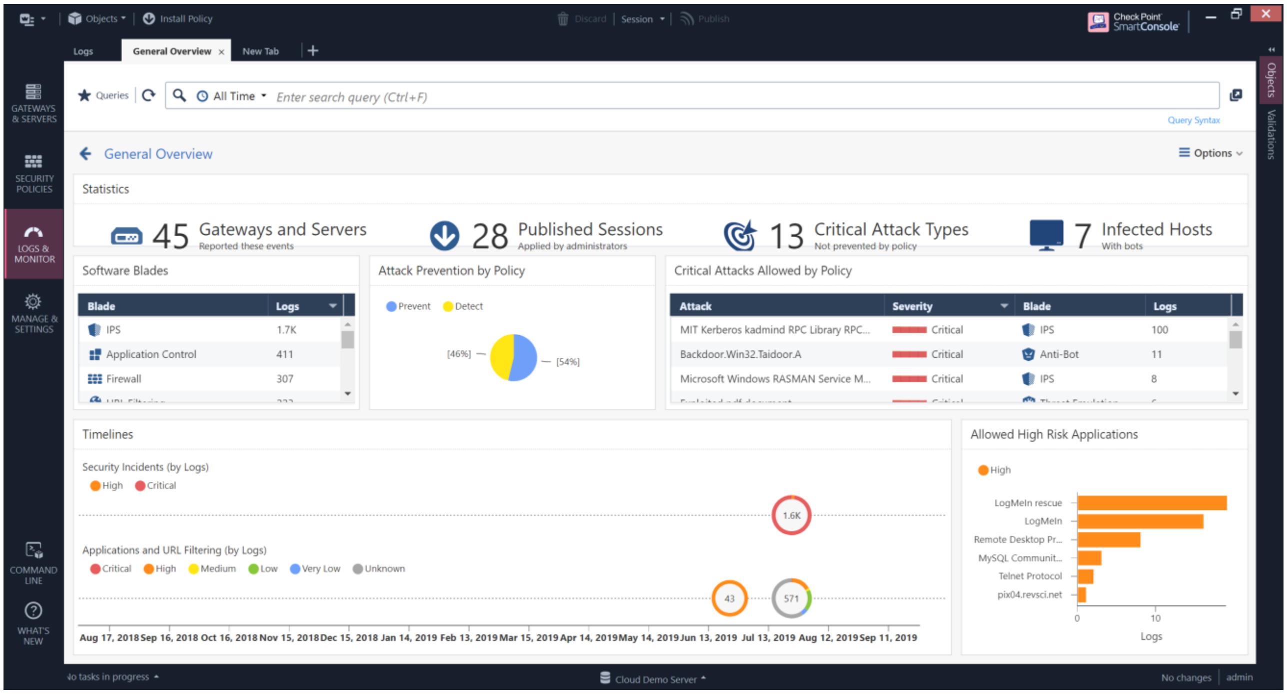
Administrator: admin | Read/Write |

8. Monitor and fine-tune policies



Showing first 50 results (999 ms) out of at least 532 results

Time	B.	A.	T..	Seve...	Con...	Su...	Perf...	Source	Source Machine Name	Source User Name	Destination	Attack Name
01 Aug 19, 5:05:01								10.2.160.102	robert-laptop	Robert White	10.226.111.67	
01 Aug 19, 5:05:01								10.2.160.14	robert-laptop	Robert White	10.226.111.193	
01 Aug 19, 5:05:01						1		192.168.72.211			10.7.98.16	Web Server Enforcement Violation
01 Aug 19, 5:05:01								192.168.3.4			10.18.5.90	Web Server Enforcement Violation
01 Aug 19, 5:05:01								10.59.1.144			10.10.82.164	Web Server Enforcement Violation
01 Aug 19, 5:05:01						1		192.168.91.18			10.5.33.4	Web Server Enforcement Violation
01 Aug 19, 5:05:01						1		192.168.38.194			10.38.193.100	Web Server Enforcement Violation
01 Aug 19, 5:05:01								10.59.1.144			10.10.82.164	Web Server Enforcement Violation
01 Aug 19, 5:05:01								192.168.74.235			10.63.99.14	Web Server Enforcement Violation
01 Aug 19, 5:05:01						1		192.168.72.211			10.7.98.16	Web Server Enforcement Violation
01 Aug 19, 5:05:01								192.168.74.235			10.63.99.14	Web Server Enforcement Violation
01 Aug 19, 5:05:01								10.1.174.98			192.168.55.61	Web Server Enforcement Violation
01 Aug 19, 5:05:01								192.168.15.81			10.10.202.36	Web Server Enforcement Violation
01 Aug 19, 5:05:01								192.168.38.194			10.38.193.100	Web Server Enforcement Violation
01 Aug 19, 5:05:01								10.0.247.192		Linda Hill	10.135.105.84	Streaming Engine: TCP SYN Modified Retra
01 Aug 19, 5:05:01								10.0.247.192		Linda Hill	10.135.105.84	Streaming Engine: TCP SYN Modified Retra



General Overview

Statistics

45 Gateways and Servers
Reported these events

28 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
Application Control	411
Firewall	307

Attack Prevention by Policy

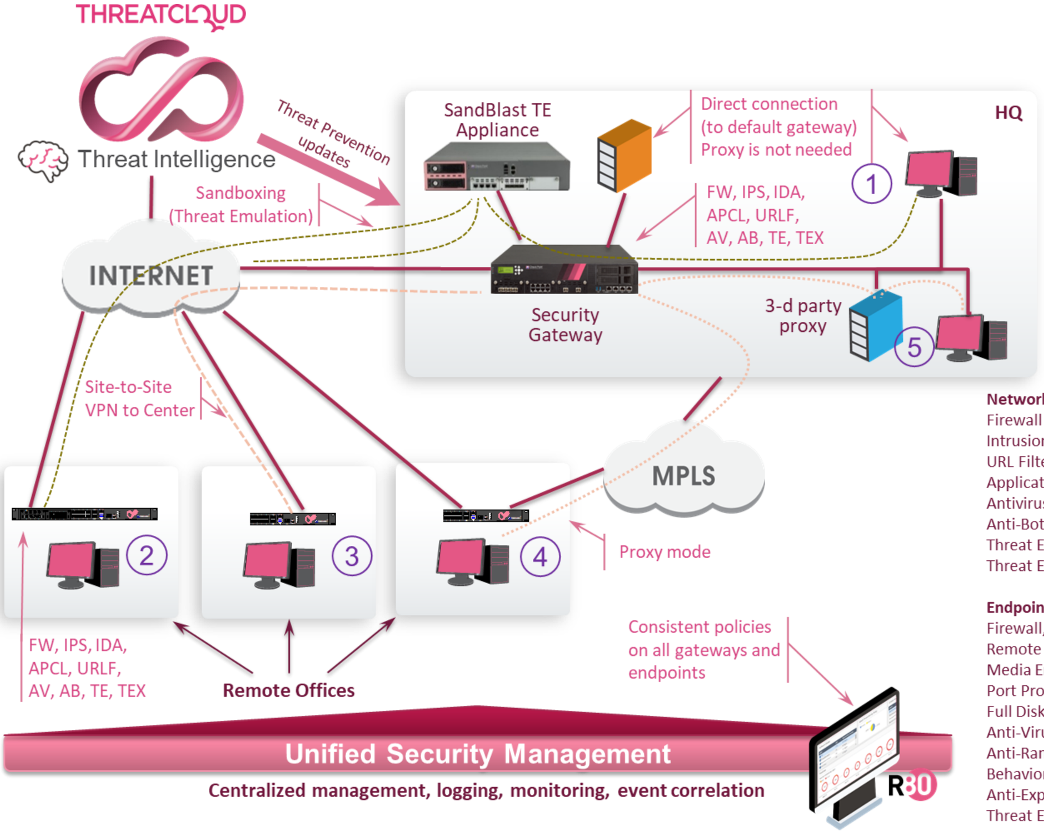
Critical Attacks Allowed by Policy

Attack	Severity	Blade	Logs
MIT Kerberos kadmind RPC Library RPC...	Critical	IPS	100
Backdoor.Win32.Taidoor.A	Critical	Anti-Bot	11
Microsoft Windows RASMAN Service M...	Critical	IPS	8

Timelines

Allowed High Risk Applications

USE CASES


THREATCLOUD
Threat Intelligence
Threat Prevention updates
Sandboxing (Threat Emulation)
INTERNET
SandBlast TE Appliance
Direct connection (to default gateway) Proxy is not needed
HQ
FW, IPS, IDA, APCL, URLF, AV, AB, TE, TEX
1
Security Gateway
3-d party proxy
5
Site-to-Site VPN to Center
MPLS
2
3
4
Proxy mode
FW, IPS, IDA, APCL, URLF, AV, AB, TE, TEX
Remote Offices
Consistent policies on all gateways and endpoints
Unified Security Management
Centralized management, logging, monitoring, event correlation
R80

Network security features:
Firewall (FW)
Intrusion Prevention System (IPS)
URL Filtering (URLF)
Application control (APCL)
Antivirus (AV)
Anti-Bot (AB)
Threat Emulation (TE)
Threat Extraction (TEX)

Endpoint security features:
Firewall, Application Control
Remote Access VPN
Media Encryption
Port Protection
Full Disk Encryption
Anti-Virus, Anti-Bot,
Anti-Ransomware, Forensic,
Behavioral Guard,
Anti-Exploit, Zero-Phishing
Threat Emulation and Extraction

Common Internet access cases

① Direct connection

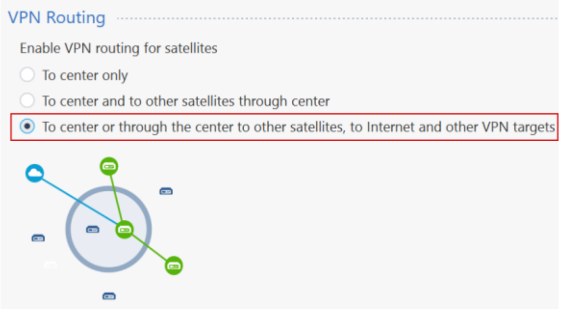
- Default route through the Internet perimeter gateway
- Suitable for endpoints and servers even if their applications do not support proxy
- All security features including Threat Emulation and Threat Extraction

② Additional NGFW/NGTP/NGTX Internet gateway

- Direct connection (as #1)
- All security features
- Security policy is centrally managed (the same or slightly differ from the HQ)
- Sandboxing (TE/TEX) is implemented via Sandblast in HQ

③ Through HQ via VPN

- Remote Office gateway uses the Internet only to establish Site-to-Site VPN to the HQ
- All traffic including the Internet is routed through the VPN to the HQ



VPN Routing

Enable VPN routing for satellites

○ To center only

○ To center and to other satellites through center

● To center or through the center to other satellites, to Internet and other VPN targets

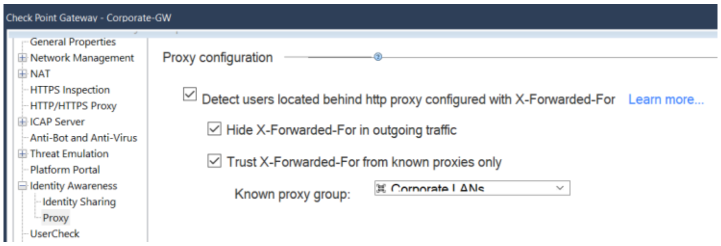
- – Outgoing Web Access policy is enforced by the HQ gateway
- – All security features

④ HQ Security Gateway as a proxy

- – Browsers of Remote Office users are configured to use the HQ security gateway as a proxy
- – The same policies and security features are enforced as for ‘direct connection’ (point 1)

⑤ 3rd party proxy

- – Legacy 3rd party proxy can be used for the transition period
- – Application Control, URL Filtering and Identity Awareness Security Gateways can use X-Forward-For HTTP header, which is added by the proxy server, to see identities of users behind the 3-d party proxy IP address and apply individual policies to users.



Proxy configuration

☑ Detect users located behind http proxy configured with X-Forwarded-For

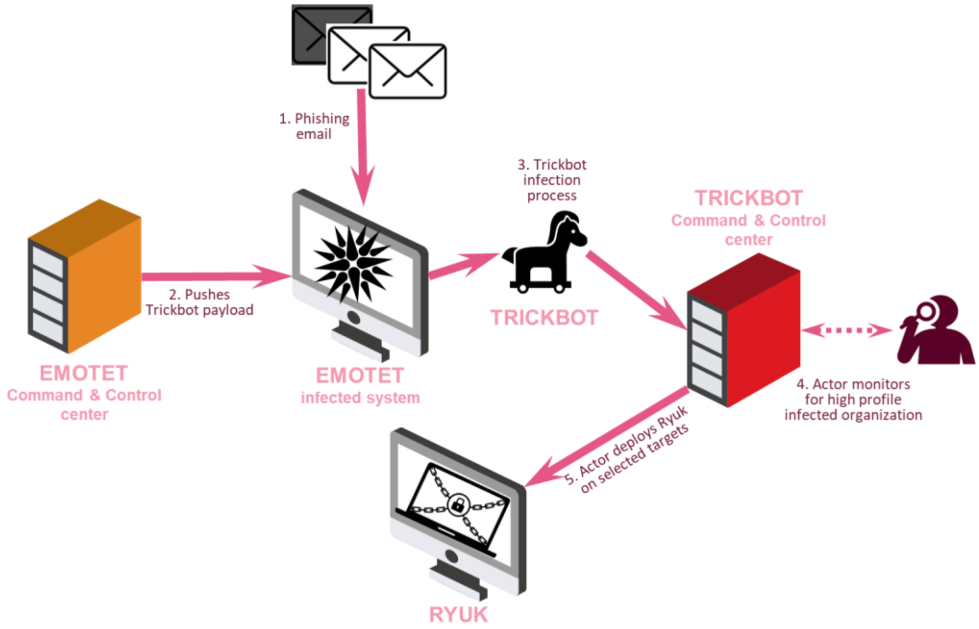
☑ Hide X-Forwarded-For in outgoing traffic

☑ Trust X-Forwarded-For from known proxies only

Known proxy group: Corporate LANs

THREAT SCENARIO

Consider the following triple attack: Emotet + Trikbot + Ryuk.


1. Phishing email
3. Trickbot infection process
TRICKBOT Command & Control center
2. Pushes Trickbot payload
TRICKBOT
EMOTET Command & Control center
EMOTET infected system
4. Actor monitors for high profile infected organization
5. Actor deploys Ryuk on selected targets
RYUK

Emotet initiates TrickBot, which deploys Ryuk

The first stage of the attack starts with a weaponized Microsoft Office document attached to a phishing email. This file contains a malicious, macro-based code. Once the user opens the document, the malicious file will run cmd and execute a PowerShell command. The PowerShell command attempts to download the Emotet payload.

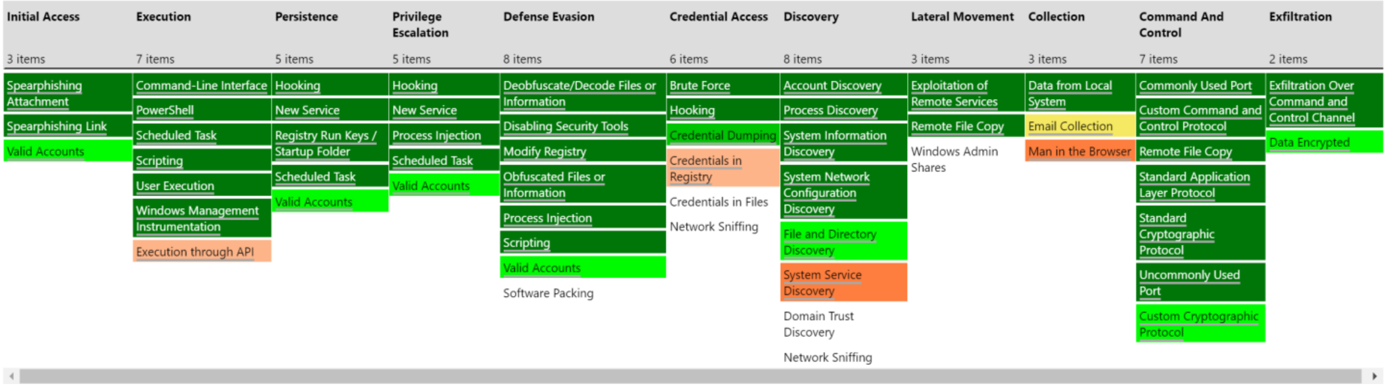
When the Emotet payload executes, it looks to continue its malicious activity by further infecting and gathering information on the affected machine. It initiates the download and execution of the TrickBot Trojan by communicating with and downloading from a pre-configured and remote malicious host.

TrickBot is a modular Trojan. Once the machine is infected with TrickBot, it begins to steal sensitive information. Meanwhile, the attackers check to see if the target machine is part of an industry they are looking to target. If it is, they download the Ryuk ransomware payload and use the admin credentials, stolen using TrickBot, to perform lateral movement, and reach the assets they intend to infect.

The ransomware dropper Ryuk.exe checks the system architecture and drops its main payload accordingly. The dropper also stops multiple services and processes related to antimalware products by using the netstop and taskkill commands. The main Ryuk payload injects itself into multiple processes and achieves persistence using the registry.

To ensure the victim is forced to pay to decrypt the valuable files, Ryuk changes the configuration of and deletes the Virtual Shadow Copy. Ryuk then encrypts files on the disk, changes the extension to .RYK, and drops a ransom note RyukReadMe.txt created with notepad.exe in every processed folder.

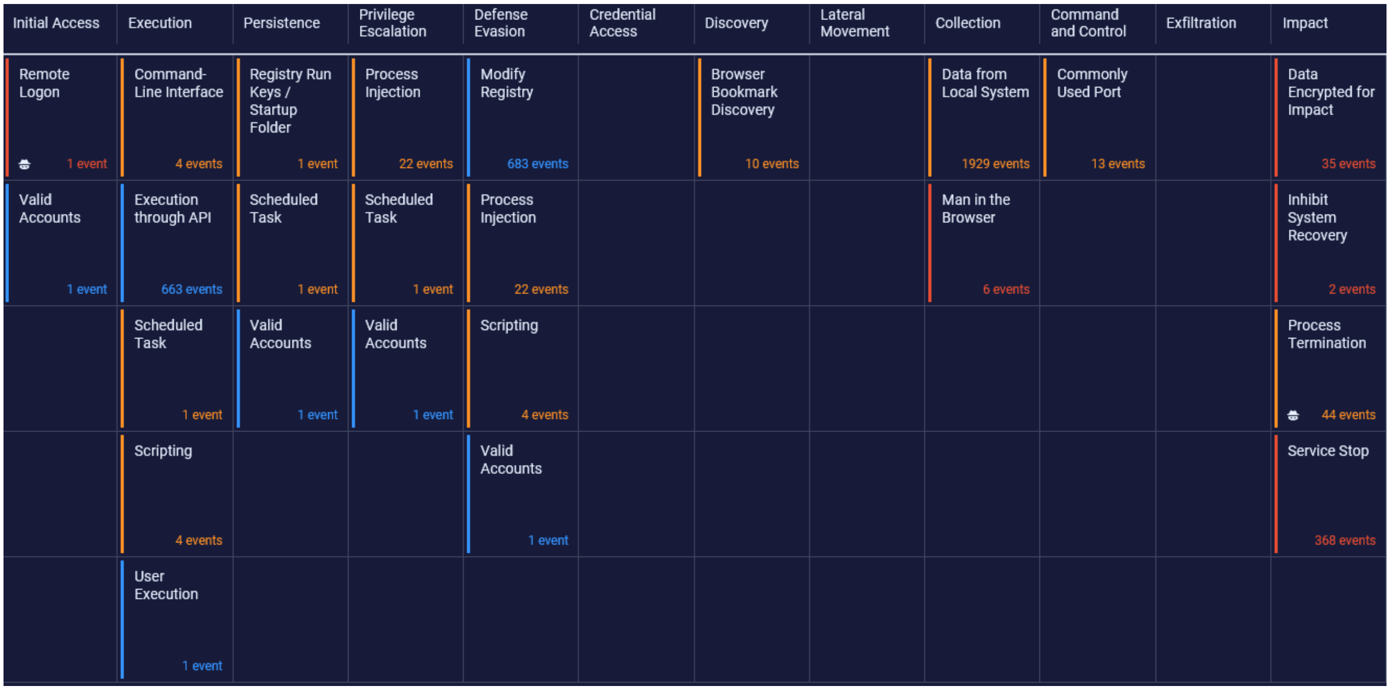
Looking to the MITRE ATT&CK Enterprise matrix, which provide a list of methods and techniques used by hackers, it can be seen that Check Point can detect and prevent such an attack at almost every stage:



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
3 items	7 items	5 items	5 items	8 items	6 items	8 items	3 items	3 items	7 items	2 items
Spearphishing Attachment	Command-Line Interface	Hooking	Hooking	Deobfuscate/Decode Files or Information	Brute Force	Account Discovery	Exploitation of Remote Services	Data from Local System	Commonly Used Port	Exfiltration Over Command and Control Channel
Spearphishing Link	PowerShell	New Service	New Service	Disabling Security Tools	Hooking	Process Discovery	Remote File Copy	Email Collection	Custom Command and Control Protocol	Data Encrypted
Valid Accounts	Scheduled Task	Registry Run Keys / Startup Folder	Process Injection	Modify Registry	Credential Dumping	System Information Discovery	Windows Admin Shares	Man in the Browser	Remote File Copy	
	Scripting	Scheduled Task	Scheduled Task	Obfuscated Files or Information	Credentials in Registry	System Network Configuration Discovery			Standard Application Layer Protocol	
	User Execution	Valid Accounts	Valid Accounts	Process Injection	Credentials in Files	File and Directory Discovery			Standard Cryptographic Protocol	
	Windows Management Instrumentation			Scripting	Network Sniffing	System Service Discovery			Uncommonly Used Port	
	Execution through API			Valid Accounts		Domain Trust Discovery			Custom Cryptographic Protocol	
				Software Packing		Network Sniffing				

MITRE ATT&CK matrix: Technics used by Emotet + Trikbot

Besides stopping the attack, it is also possible to generate a comprehensive report at the endpoint.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon 1 event	Command-Line Interface 4 events	Registry Run Keys / Startup Folder 1 event	Process Injection 22 events	Modify Registry 683 events		Browser Bookmark Discovery 10 events		Data from Local System 1929 events	Commonly Used Port 13 events		Data Encrypted for Impact 35 events
Valid Accounts 1 event	Execution through API 663 events	Scheduled Task 1 event	Scheduled Task 1 event	Process Injection 22 events				Man in the Browser 6 events			Inhibit System Recovery 2 events
	Scheduled Task 1 event	Valid Accounts 1 event	Valid Accounts 1 event	Scripting 4 events							Process Termination 44 events
	Scripting 4 events			Valid Accounts 1 event							Service Stop 368 events
	User Execution 1 event										

Ryuk malicious activity in the MITRE ATT&CK Matrix format.

CONCLUSION

There are many options to secure Internet web access: from very simple solutions to utilizing extremely complicated and expensive technology. The multi-vendor approach requires multiple solutions, such as gateways to protect the Perimeter, proxy/web isolation for outgoing Internet access, multiple endpoint protections and more. Simply deploying a sole protection across these varied environs is challenging, i.e. it is difficult to keep policies consistent when using proxy and for direct connections.

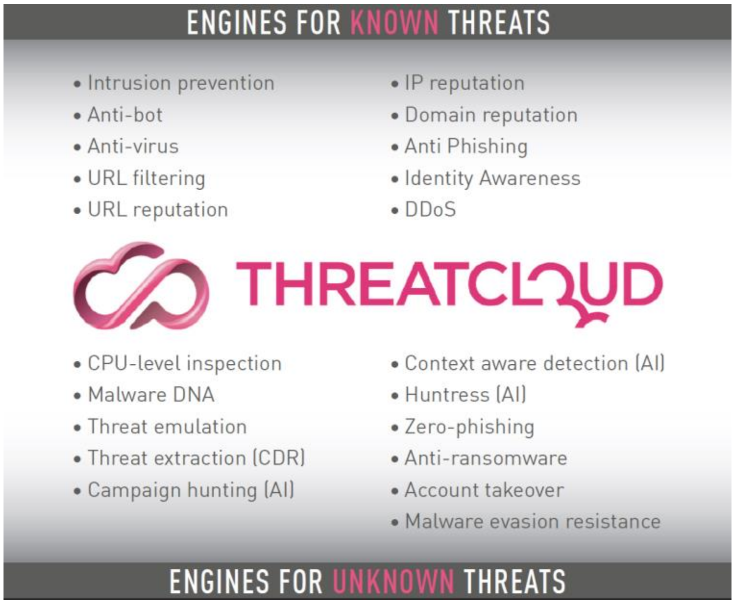
Moreover, multi-vendor solutions typically require more effort to be put into place because the administrator will have to coordinate the integration of disparate (and potentially incompatible) systems. Procurement efforts are also higher as negotiations of multiple contracts will need to take place, and not every contract will be the same length and/or will be renewed at the same time. The management and monitoring of consoles, product upgrades, staff training and more, will require significant time and labor input, as well as a high monetary investment.

	Network	Endpoint	Operations
Multi-vendor	Perimeter firewall Proxy / web isolation	Antivirus + antimalware	3 management servers 3 consoles Inconsistent policies Multiple service contracts
Check Point	Firewall NGTX[2]	Endpoint Security[3]	1 management server Unified consoles and policies Single point of support

Check Point delivers an effective security architecture by uniquely combining three key elements:

- One security platform: leverages unified threat intelligence and open interfaces.
- Preemptive threat prevention: blocks the most sophisticated attacks before they happen.
- Consolidated system of single management, modular policy management and integrated threat visibility.

With 64 different security engines, Check Point protects against known and unknown threats across all networks, endpoints, cloud, mobile, and IoT. In addition, Check Point SandBlast Zero-Day Protection provides advanced protection against zero-day malware with technologies such as threat emulation (sandboxing), threat extraction (safe content delivery), anti-phishing, endpoint forensics, and anti-ransomware.



ENGINES FOR KNOWN THREATS

- Intrusion prevention
- Anti-bot
- Anti-virus
- URL filtering
- URL reputation
- IP reputation
- Domain reputation
- Anti Phishing
- Identity Awareness
- DDoS

THREATCLOUD

- CPU-level inspection
- Malware DNA
- Threat emulation
- Threat extraction (CDR)
- Campaign hunting (AI)
- Context aware detection (AI)
- Huntress (AI)
- Zero-phishing
- Anti-ransomware
- Account takeover
- Malware evasion resistance

ENGINES FOR UNKNOWN THREATS

See if your business is vulnerable to newly deployed attacks: Instant Security Assessment

[2] Includes multi-layered protection from known threats AND zero-day attacks using SandBlast Threat Emulation, SandBlast Threat Extraction, Antivirus, Anti-bot, IPS, App Control, URL Filtering and Identity Awareness

[3] Endpoint Threat Emulation and Extraction, Zero-Phishing, Anti-Ransomware, Endpoint Anti-Bot, Anti-Exploit, Behavioral Guard, Endpoint Anti-Virus, Forensic collection and automated reports; Endpoint Firewall, Application Control, Port Protection, Endpoint Compliance, Remote Access VPN; Full Disk Encryption (FDE), Media Encryption (ME)

Or request a free Security Check Up.