



CheckMe

Instant Security Assessment

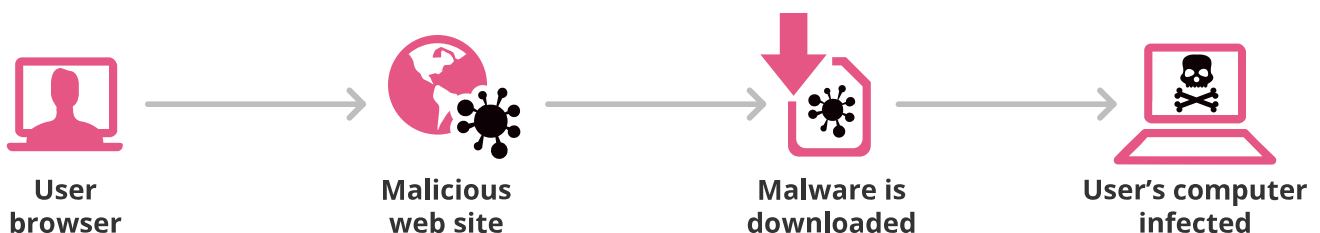
# YOUR FULL REPORT



On an average day, users download malware every 81 seconds. They access malicious websites every 5 minutes. Threat actors release 1 million new forms of malware every day. These all add up to a significant likelihood your network will be breached.

## ARE YOU VULNERABLE TO NEW TYPES OF ATTACKS?

CheckMe simulates many types of attacks that can compromise your computer and the information on your network. This report summarizes your exposure to ransomware, phishing, zero-day malware, c&c communication, data leakage, and other threats.



## EXECUTIVE SUMMARY

NETWORK

 **2 SECURED**

 **5 VULNERABLE**

ENDPOINT

 **4 SECURED**

 **2 VULNERABLE**

CLOUD

 **4 SECURED**

 **4 VULNERABLE**



**MALWARE INFECTION** is used to gather guarded information or disrupt corporate, governance and individual operation.



**COMMAND & CONTROL COMMUNICATION** let attackers take complete control over an infected computer.



**ZERO DAY** attacks use the surprise element to exploit holes in the software that are unknown to the vendor.



**BROWSER EXPLOIT** is an attack that takes advantage of a particular vulnerability in a computing system.



**RANSOMWARE** is a malware that encrypts users' files and require ransom for their decryption.

-



-



**PERSISTENT MALWARE** is a continuous computer hacking processes targets private organizations or states for business or political motives.

-



-



**IDENTITY THEFT** attack captures personal information by fake websites that appears to be legitimate.



-



**ANONYMIZER USAGE** can open back doors into an organization's network.



-



**DATA LEAKAGE** unintentional or theft release of sensitive information outside the organization's network.



-



**CLOUD SEGMENTATION** scans for open ports of accessible machines within the same environment to indicate for access control lacking.

-

-



## ASSESSMENT DETAILS

ASSESSMENT DATE: **MARCH 19, 2018****NETWORK**IP Address: **91.90.132.217**Operating System: **WINDOWS****ENDPOINT****CLOUD**Web Service Type: **AWS**VPC / VNE: **VPC-D69988AE**Region: **US-EAST-1**

The **CheckMe** report identifies security risks on your enterprise environments and presents them. In addition, it contains guidelines on how to address the security issues to make your organization more secure.



## MALWARE INFECTION

Malware refers to software that is intentionally designed to be malicious. Over the past few years malware has morphed into tools that are developed and used by a wide range of professional threat actors, such as organized crime rings or agents sponsored by nation states. Malware is used against government, corporate and individuals to gather guarded information or to disrupt their operation.

The first test simulates the download of an EICAR file over HTTP and HTTPS, and the second test checks exposure to the **IoTroop** botnet that can control smart devices. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Downloading of infected zipped file through HTTP.	✓	✓	✗
Downloading of infected file through HTTPS.	✗	-	✓
Simulating vulnerability exposure on the 850L router.	✓	-	✗

## REMEDIATION

**Network and Cloud:** To address this finding, we recommend using explicit controls to block IOT botnet communications. These controls must be continuously updated without requiring administrators to download new records. Check Point's Next Generation Threat Prevention (NGTP) and Next Generation Threat Extraction (NGTX) include such protections as integral elements of their multi-layer threat prevention functionality.

To achieve maximum protection, configure NGTX solution as follow:

1. Make sure your Anti-Virus blade is configured based on the Check Point's "Recommended\_Profile" or "Optimized Profile".
2. Enable the "Archive scanning" in your Anti-Virus blade (in the Threat Prevention profile).
3. Enable the HTTPS Inspection feature to inspect HTTPS traffic.
4. Enable the IPS blade and ensure that IPS protections are up to date.
5. In case it is not possible to update the IPS protections to the latest release, enable the following IPS protection: D-Link 850L Router Remote Unauthenticated Information Disclosure



## COMMAND & CONTROL COMMUNICATION

A bot is malicious software that allows cybercriminals to remotely control computers and execute illegal activities such as stealing data, spreading spam and distributing malware. The final phase of malware-based attacks is the use of command and control sites for remote administration of the malware.

This test generates requests to known command and control servers. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Simulating command and control communication to external server.			








### REMEDIATION

**Network:** To address this finding, we recommend using explicit controls to block C&C communications. These controls must be continuously updated without requiring administrators to download new records. Check Point's Next Generation Threat Prevention ([NGTP](#)) and Next Generation Threat Extraction ([NGTX](#)) include such protections as integral elements of their multi-layer threat prevention functionality.

 ZERO DAY

Cyber threats are continuing to evolve. Hackers are finding new ways to hide malware inside emailed documents, on websites as "drive by" exploits or in downloadable content. Many attacks begin by exploiting known vulnerabilities and modifying malware to have unrecognizable signatures to evade traditional security measures. By creating these new, unknown variants, hackers aim to avoid detection by signature-based security solutions, to breach the network and steal critical information.

These test attempts to download files in different formats that are often used in Zero Day attacks. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Downloading an Infected PDF file with random suffix (hide the real format of the file).			
Downloading of an archive with infected PDF file.		-	
Downloading of PDF file.		-	

## REMEDIATION

**Network:** Blocking malware downloads requires multiple layers of malware control. Check Point's Next Generation Threat Extraction (NGTX) offering provides signature based anti-malware as well as advanced threat prevention tools. It includes an array of technologies that scan, emulate and extract malicious content from downloaded files.

To achieve maximum protection make sure that your **Threat Emulation** blade and/or **Threat Extraction** blades are enabled.

**Endpoint:** As part of the Check Point SandBlast Zero-Day Protection solution, **Threat Emulation** prevents infections from new malware and targeted attacks. This innovative zero-day threat sandboxing capability within the SandBlast solution delivers the best possible catch rate for threats, and is virtually immune to attackers' evasion techniques.

Enable Threat Emulation on your Check Point **Endpoint Security** to improve your security risk against exploits.





## BROWSER EXPLOIT

Exploit is usually the first step in an attack that takes advantage of a particular vulnerability in a computing system. The Exploit technique works in a way that the end user can be exploited just by browsing to a legitimate website without downloading anything.

In case that CheckMe assess your network and/or cloud environment this test include the use of cross-site scripting (XSS). The cross-site scripting can be used to inject malicious content from an infected site onto the user's machine via their browser. This attack is often used in websites where user input is gathered without validation or encoding. The test simulates a connection attempt to a site that is known to contain malicious content that can be injected into a browser.

In case that CheckMe assess your Endpoint, the test simulates a shellcode execution in the browser and check if it's exploited.

For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Simulating access to a website that can be infected with java script code.	✓	-	✗
Simulating a shellcode execution in the Internet Explorer.	-	✗	-

## REMEDIATION

**Cloud:** Blocking exposure to sites that are vulnerable to Cross-Site Scripting attack requires Intrusion Prevention System. Check Point's Next Generation Threat Prevention (NGTP) and Next Generation Threat Extraction (NGTX) packages include intrusion prevention solution (IPS) that block both server and client-side exploits built on vulnerabilities that allow cross-site scripting to succeed. IPS also uses technologies that receive feeds from dynamic intelligence sources that automatically block connections to sites that contain cross-site scripting code.

The IPS is part of the NGTX and NGTP and it blocks cross-site scripting attack with its recommended / optimized profile. In case that IPS protections are not updated, enable **cross-site scripting attempt** in your IPS policy to protect your computer from this threat.

**Endpoint:** **Anti-Exploit** provides protection against browser and Office exploit based attacks. By detecting the exploit attempt, Anti-Exploit prevents downloading or execution of a malicious payload. On detection Anti-Exploit will shut down the process being exploited and then will generate a forensics report.

Enable Anti Exploit on your Check Point **Endpoint Security** to improve your security risk against exploits.



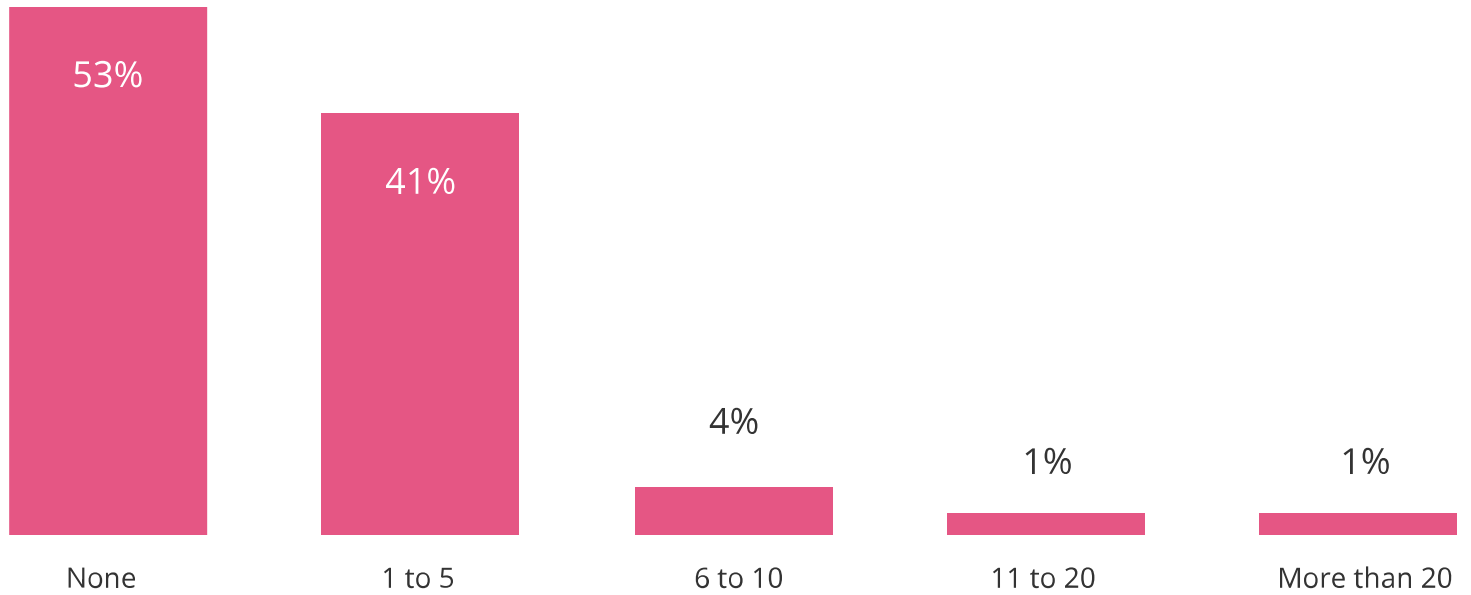
## RANSOMWARE

Ransomware is a form of malware that has grown in frequency and severity. This malware encrypts files, making them unusable. Ransomware forces users to purchase keys to decrypt the files.

To bypass traditional anti-malware solutions, attackers will often package their exploits within standard document formats as well as more complex vehicles such as compressed archives, or through encrypted file distribution channels. This test attempts to create files in the user's downloads directory and encrypts them using AES (Advanced Encryption Standard) and generated key with usage of MD5 of current user SID, And open CMD process. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Simulating files encryption on the endpoint.	-	✓	-

## Nearly 50 percent of organizations have been hit with ransomware during 2016



Source: [Osterman Researches, Inc](#)



## PERSISTENT MALWARE

A Persistent malware is an advanced or evasive malware, consisting of multiple elements and stages that are executed consecutively.

Those malwares are planned and built to survive conventional Anti-Virus remediation attempts by disguising some of its elements as legitimate ones.

This test detects the malicious element of a persistent malware and checks if the full attack chain of the malware, including the seemingly legitimate elements of it, were terminated and remediated. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Simulating persistence extraction of infected file.	-	✓	-

## IDENTITY THEFT

Threat actors primarily use phishing sites to gather sensitive information. They use this information either to directly impact the individual connecting to the site, such as bank customers, or to conduct follow-up attacks, for example gathering administrator credentials.

This test generates connections to phishing and malicious sites. A successful communication attempt is an indication that you could fall prey to a phishing attack and your personal information could be stolen. For more information click [here](#).

### 85%

Of organizations have suffered phishing attacks

### 45%

Of the attacks drive by web links

### 9 out of 10

Phishing emails carried ransomware

### 12,000

New Phishing websites are added every day

Sources: [Osterman Researches, Inc](#)  
[Check Point Software Technologies](#)

NETWORK      ENDPOINT      CLOUD

Simulating connection to phishing sites.



-



## REMEDIATION

**Network and Cloud:** Blocking phishing attacks requires [URL Filtering](#) protection, which is an integral component of Check Point's Next Generation Threat Prevention ([NGTP](#)) and Next Generation Threat Extraction ([NGTX](#)) solutions, can be used to block connections to known phishing sites.

Ensure that phishing and high risk categories are configured in prevent mode within the [URL Filtering](#) policy to protect your computer from this threat.



## ANONYMIZER USAGE

The use of anonymizers has many security implications. It shows that users are hiding their online activity. Anonymizers also indicate potential coordinated campaign activity. Attackers often coordinate their efforts through encrypted communications channels. Further, instructions for the use and purchase of attack tools are often only available on marketplaces within the Dark Web. These sites can only be accessed with anonymizers.

This test generates connections to anonymizers. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Simulating access to an anonymizing site that allows users to hide their online activity.	✓	-	✓





## DATA LEAKAGE

Data leakage happens when users transfer classified or sensitive information outside the corporate network purposely or by mistake. In contrast, exfiltration is the deliberate extraction of sensitive data by external parties. Both are dangerous and can lead to the loss of customer and company sensitive information such as financial data and credit card data. These risks are often the final phase of a security breach. Data leakage and exfiltration can also violate regulations and industry guidelines such as PCI DSS.

This test attempts to upload payment card data to public websites. For more information click [here](#).

# 45

Times a day sensitive information is sent outside an average organization

# 88%

Of organizations experienced data loss

# 400%

Growth of data records over the past three years

Source: [Check Point Software Technologies](#)

	NETWORK	ENDPOINT	CLOUD
Posting credit card numbers to external sites over http.		-	
Posting credit card numbers to external sites over https.		-	

## REMEDIATION

**Network:** Data loss prevention tool is required element of a comprehensive security program. The Check Point's **DLP** designed to preemptively protect sensitive information from unintentional loss. DLP Software combines technology and processes to revolutionize DLP, helping businesses to preemptively protect sensitive information from unintentional loss, educating users on proper data-handling policies and empowering them to remediate incidents in real time

Ensure that PCI - Credit Card Numbers data type is configured in prevent mode within the DLP policy to protect your network from this threat. In addition, make sure that HTTP Inspection is enabled for DLP to avoid loss of data over HTTPS.



## CLOUD SEGMENTATION

Cloud environments are based on the concept of whitelist access control, approving and logging only allowed access while blocking all other communication. In a secured environment the combination of well-defined native cloud security groups and a dedicated L4-L7 security solution enables the enforcement of proper segmentation and access control between workloads.

Assets deployed in a public cloud environment must be configured and handled explicitly in the distributed security groups and an application aware security solution to prevent unauthorized access attempts. Internet facing machines are especially susceptible to unauthorized access as they are deployed to serve incoming connections from external networks.

The Cloud CheckMe virtual machine is deployed in a designated cloud subnet and tenant. Without receiving an association to a specific authorized logical group, it initiates a simple scan for open ports of accessible machines within the same environment. A successful scan of non-Internet-facing machines would indicate that access controls in the environment are lacking. For more information click [here](#).

	NETWORK	ENDPOINT	CLOUD
Scanning for open ports of accessible machines within the same environment.	-	-	

The Cloud CheckMe virtual machine indicates that there are 6 machines with open ports to other machines within the same environment. This section presents up to two machines. To view all machines with open ports please move to Appendix A.

- Machine x.x.2.6 has 1 open ports: tcp/22
- Machine x.x.2.7 has 2 open port: tcp/22, tcp/111

## REMEDIATION

**Cloud:** According to both Check Point and cloud vendors best practices, Internet facing services must be published securely. All other types of services should be segmented according to software-defined protection principles. Machines that are not associated with security groups that define specific access to other workloads must not be allowed permissive access.

Server machines should only be listening to ports mandatory to the service they provide, all other ports must be closed.

**Check Point CloudGuard** protects assets in the cloud from the most sophisticated threats with dynamic scalability, intelligent provisioning and consistent control across physical and virtual networks, ensuring you can embrace the cloud with confidence.

## CONCLUSIONS

CheckMe checked your exposure to **10** common threats based on series of tests that were simulated on your environments. The assessment found that you are exposed to **7** threats.

Mitigating attacks like these requires a security strategy that coordinates multiple protections in a preventative approach. Preventative methodology is the foundation of the Check Point solution set. Our solutions (**NGTP**, **NGTX**, **SandBlast**, **Endpoint** and **CloudGuard**) integrate multiple levels of protections into unified security platforms. In addition, our unified management architecture empowers administrators to build policies and analyze events across all solutions efficiently and effectively.

This CheckMe report is a single snapshot of your security profile. Check Point offers consulting services that can provide you with a full view of your current security profile. We can help you understand how you are positioned today and use this understanding to build a path with that will let you to improve your posture going forward.

**For more information on Check Point technologies and services please contact your local partner and account team or find us online at**

<https://www.checkpoint.com/about-us/contact-us/>

**CONTACT US**

## APPENDICES

## APPENDIX A - CLOUD SEGMENTATION RESULTS

The Cloud CheckMe virtual machine is deployed in a designated cloud subnet and tenant. CheckMe initiates a scan for open ports of accessible machines within the same environment.

The table below contains a list of machines detected with open ports within the designated environment:

MACHINE	OPEN PORTS
x.x.2.1	
x.x.2.6	tcp/22
x.x.2.7	tcp/22, tcp/111
x.x.2.8	
x.x.2.9	
x.x.2.15	