

X X X X X X

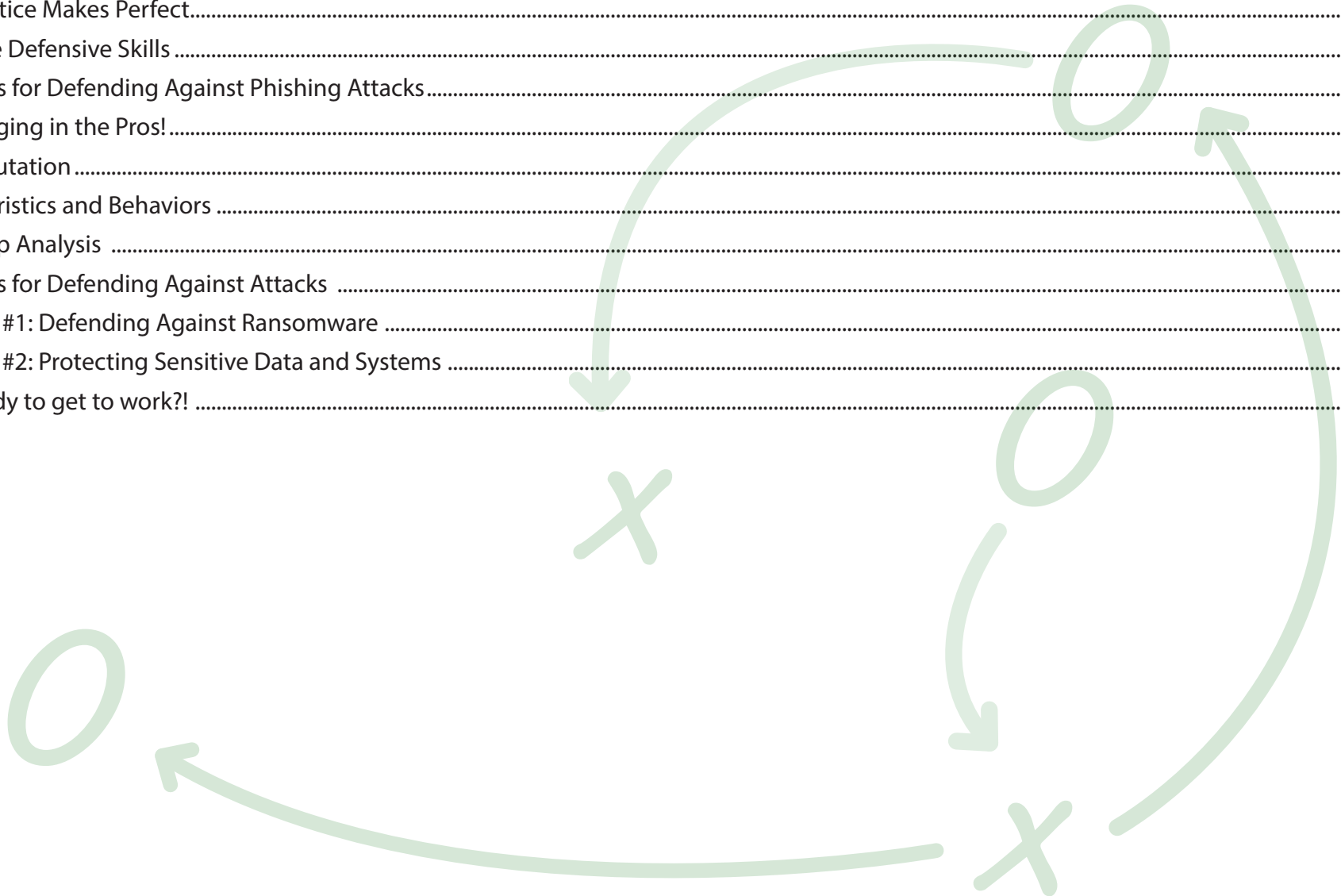
Perfecting Your
Defensive Strategy
Playbook

O O O O O O



Table of Contents

Defensive Skills and Drills	3
Practice Makes Perfect.....	3
Core Defensive Skills	4
Drills for Defending Against Phishing Attacks.....	6
Bringing in the Pros!	7
Reputation	8
Heuristics and Behaviors	10
Deep Analysis	11
Plays for Defending Against Attacks	12
Play #1: Defending Against Ransomware	12
Play #2: Protecting Sensitive Data and Systems	14
Ready to get to work?!	16



DEFENSIVE SKILLS AND DRILLS

Practice Makes Perfect

If you want a winning defense, you need to train your employees and staff to be prepared for any type of attack. Here are some key security elements that you want to cover in your security training planning:



①. Password security



④. Wireless Security



②. Phishing Attacks



⑤. Desktop Security¹



③. Advanced Malware

¹ <https://www.rapid7.com/fundamentals/security-awareness-training/>

Core Defensive Skills²

StaySafeOnline.org offers some important things to remind your employees about to help them keep themselves safe from attack:

①. Keep your machine clean

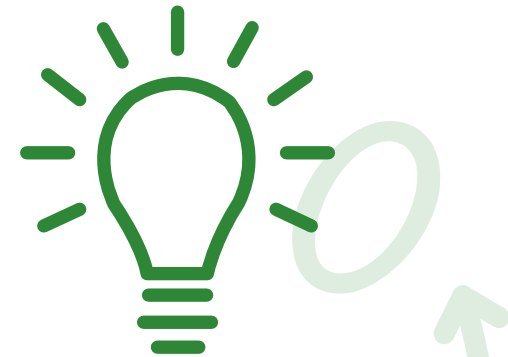
As an IT team, make sure you restrict who can install what on their devices. These types of restrictions are often through permissions preset by the IT administrator.

②. Follow good password practices

Use passphrases capitalization, symbols, numbers, even lists of random words - just make sure your password for work and personal accounts are different!

③. Think about multi-factor authentication

Passwords will only get you so far in protecting your organization. Solutions like multi-factor authentication can provide additional layers of defense in gaining access.



TIP:

Use a passphrase with a combination of numbers, symbols, upper- and lowercase letters instead of just one word. These are often easier to remember and harder to crack!

² <https://staysafeonline.org/business-safe-online/train-your-employees>

④. When in doubt, don't!

Be very cautious when opening links found in emails, tweets, posts, online ads or messages. You should also be wary of opening any attachment from a sender you don't recognize.

⑤. Lock it up when you walk away

Always make sure that your computer is locked when you leave your desk to ensure that no one gains access that shouldn't.

⑥. Back-up your work

You should have automatic back-ups in place, but it never hurts to encourage your employees to perform regular back-ups on their own!

⑦. Say something!

Report any strange activity or behavior on your device to IT as soon as possible! The faster the team is alerted, the better chance there is to mitigate the damage.



TIP:

Copy the hyperlink into a new browser instead of clicking a link. This should make it easier to see if the link is taking you where it says it is.

Drills for Defending Against Phishing Attacks³

As discussed, phishing attacks are one of the most common attack methods used by hackers today. In fact in 2016, 91% of cyber attacks started with a phishing email! Here are few tips your employees can use for spotting this malicious type of email!⁴



①.

What is the emotion of the email?

Hackers will often leverage a recipient's emotions to get them to engage with the email. Whether they're playing up curiosity, fear, urgency or even greed, emails with this tone often have a nefarious intent.

②.

Check standard email elements for discrepancies

Review things like the sender domain and email signature for any strange or out-of-place information.

③.

Are there grammatical errors?

A high volume of grammatical errors should be a red flag that this could be a phishing email, especially when combined with the two other tips above.

³ <https://phishme.com/wp-content/uploads/2016/10/PM-How-to-spot-a-phish-Infographic.zip>

⁴ <https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704/>

Bringing in the Pros!

Training is incredibly important as a first step in making sure that your organization is ready to defend against advanced attacks. There are plenty of companies that you can work with to create customer programs designed specifically for your organization.

Don't want to break the bank? Companies like KnowBe4⁵ and PhishMe⁶ offer a variety of free resources to help in educating and training your employees, including:

*Awareness posters
Free phishing tests
Weak password tests
Ransomware simulator
Free training modules*



KnowBe4 also offers a free Phish Alert Button, that provides safe and easy way for employees to forward suspicious emails to your IT or security teams.

Do your users know what to do when they receive a **suspicious** email?

Should they call the help desk, or forward it? Should they forward to IT including all headers? Delete and not report it, forfeiting a possible early warning?

Security threats take time just as they do to respond to them. A single click can prevent future exposure. All with just one click!

Phish Alert Benefits

- ✓ Reinforces your organization's security culture
- ✓ Users can report suspicious emails with just one click
- ✓ Incident Response gets early phishing alerts from users, creating a network of "sensors"
- ✓ Email is deleted from the user's inbox to prevent future exposure

I want my **Free Phish Alert**

First Name* Last Name*

Email*

Company Name*

State*
- Please Select -

Country*
- Please Select -

Number of Employees*

Sign Up!

5 <https://www.knowbe4.com>
6 <https://phishme.com/>

SETTING UP YOUR DEFENSIVE FORMATION

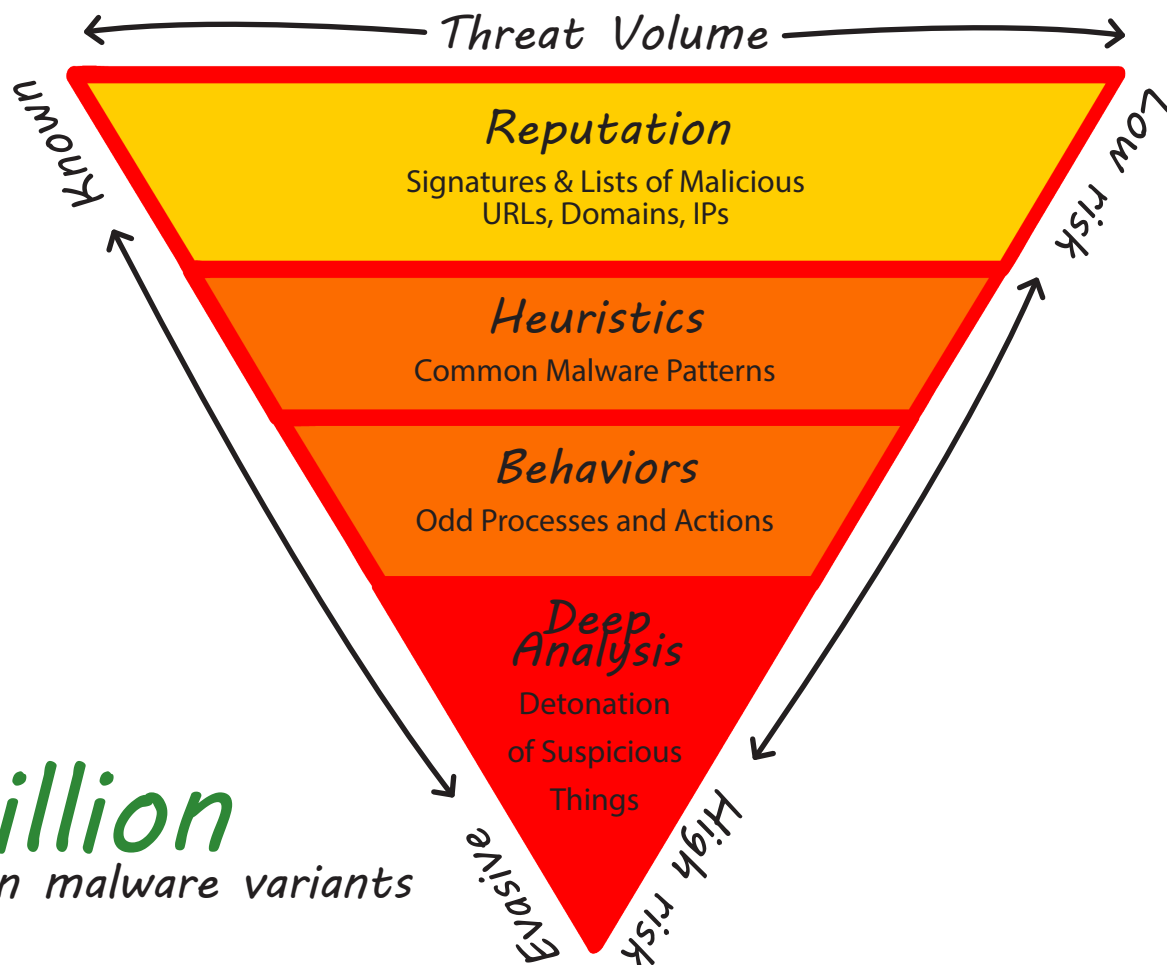
Reputation

Defending against known threats, while straight-forward, is also incredibly important. Hackers know that organizations and individuals are often remiss in patching their systems, leaving themselves vulnerable to these attacks. According to AV-Test, there are currently more than 700 million known malware variants.⁷ Do you have the defenses in place to protect against all of them?

There are more than

700

million
known malware variants



⁷ <https://www.av-test.org/en/statistics/malware/>

You need to have the solutions in place to protect the network and endpoint from these types of attacks, including signature defenses, as well as lists of malicious URLs, domains and IP addresses. These defenses come in all shapes, sizes and price points, but here are a few “must-haves”:

⑦.

Endpoint AV

This is probably the most common signature defense for the endpoint. These lists of signatures can be leveraged to stop known attacks before user interaction. Most of these solutions are updated regularly to ensure they contain the most recent patches.



②.

Intrusion Prevention Service (IPS)

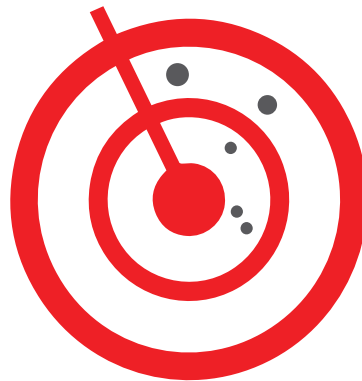
Examines network traffic at the lowest level to identify known threats by matching traffic patterns to signature databases.



③.

Web Reputation

Reviews the destination of outbound connections and identifies its threat level based on intelligence feeds. Traffic to URLs with a bad reputation are immediately blocked.



④.

URL Filtering

Queries URL categories and sub-categories to either allow or block access to the URL based on policy settings, including user, group and schedule.



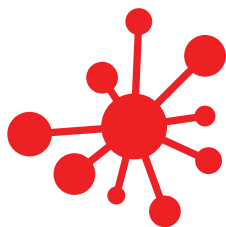
Heuristics and Behaviors

New malware variants are created by hackers every hour. In fact, AV-Test reports that more than 390,000 new malware variants are registered each day! While this seems like a daunting task to defend against, there are a few different solutions that can help in the fight against threats that haven't had a signature created for them yet.

While malware variants are all different in some way, the threat itself will follow a very common, and therefore detectable, pattern of events while waging the attack. Heuristic and behavior detection methods will analyze the malware to detect these processes and actions to determine if the malware is malicious. Threats that are actively creating registry keys, altering the Host file, creating a process or even unpacking code would be deemed malicious and remediated.

Here are some detection methods that leverage heuristics and/or behaviors:

①.



Gateway AV

Leverages both signature-based and heuristic scanning of files to identify known malware and riskware. Once a matching signature is detected the connection is blocked or the file is stripped.

②.



Spam Prevention

Detects common malicious patterns in mail headers that would indicate spam.

③.



Endpoint Heuristics and Behavior Detection

Monitors endpoints for files containing malicious code and exhibiting behaviors commonly found in malware.

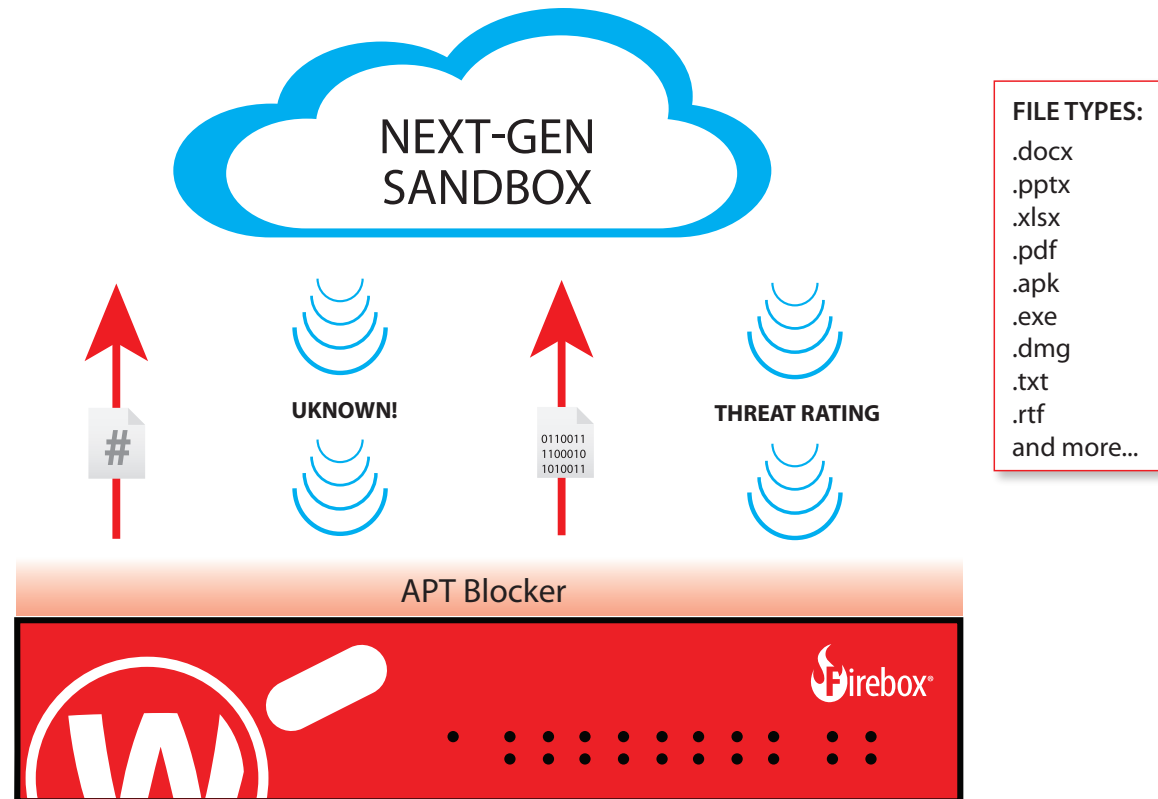
Deep Analysis

Evasive, advanced threats require professional level detection methods. These threats are often designed to specifically avoid traditional detection methods leveraging signatures, heuristics and behaviors. So how can you detect these attacks?

Deep analysis methods enable you to safely detonate suspicious elements discovered on your network and endpoint in a cloud sandboxing environment. Once the file has been detonated, you can easily determine if the event is benign or malicious, and remediate it accordingly.

Network Sandboxing

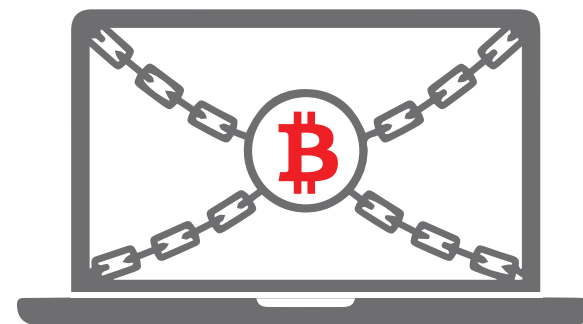
Behavioral analysis determines if a file is malicious, identifying and submitting suspicious files to a cloud-based sandbox where the code is emulated, executed, and analyzed to determine its threat potential. If the suspected file is found to be malicious, the threat is quickly remediated before any damage is done.



PLAYS FOR DEFENDING AGAINST ATTACKS

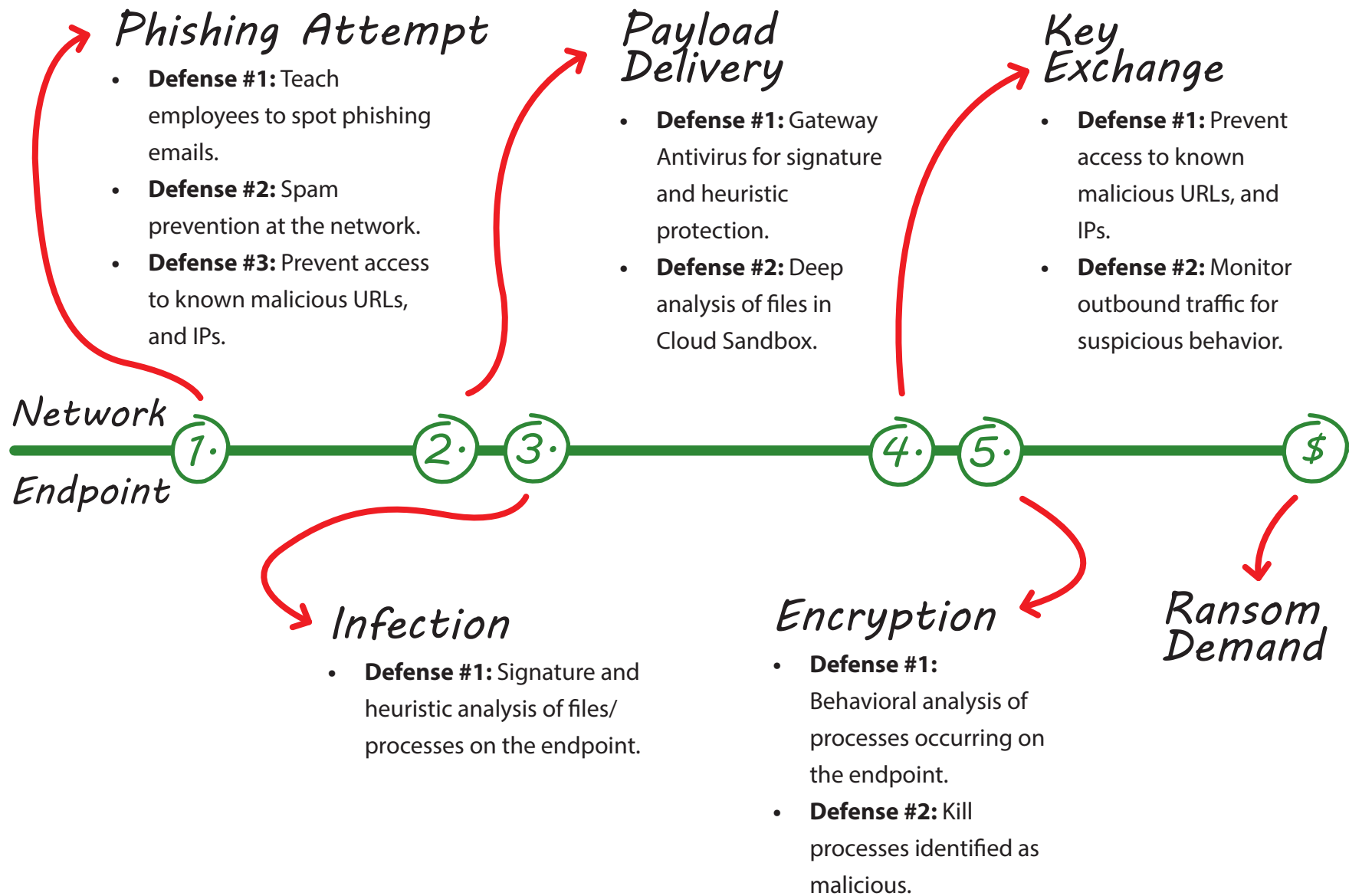
Play #1: Defending Against Ransomware

Ransomware is a type of advanced malware attack that takes hold of a device, either locking the user out entirely or encrypting files so they cannot be used. Recent crypto-ransomware strains have followed a typical path of infection beginning when a user becomes a victim of a phishing campaign by clicking a link or downloading a file found in a malicious email. This begins a process in which the malware is delivered to the endpoint via a dropper, and attempts to communicate with a command and control server external to the target network. If successful, the command and control server will provide an encryption key, the file encryption process will begin, and the victim will receive a ransom note demanding payment for a return of the data.



As you can see in Figure 1, Ransomware attacks are complex, multi-stage affairs. Each of the five phases of the attack can present an opportunity to detect, and potentially prevent a successful attack if proper security and policies are in place.

Figure 1.



Play #2: Protecting Sensitive Data and Systems

One of the most significant and well-publicized breaches of the last decade was that of mega-retailer Target in 2013. Hackers infiltrated Target's network, installed malware directly onto Point of Sale systems, and proceeded to steal 40 million credit card numbers before the breach was detected.

The attack began when VPN credentials were stolen from a third-party vendor. Attackers used these credentials to enter Target's corporate network and pivot to other sensitive points they could exploit. After first copying a database of over 70 million customer records including names, addresses, emails, and phone numbers, the attackers delivered malware to compromise the POS systems capturing credit cards.

Figure 2 shows the various points on the network and endpoints where detection and ultimately prevention could occur in an attack similar to that of Target in 2013.

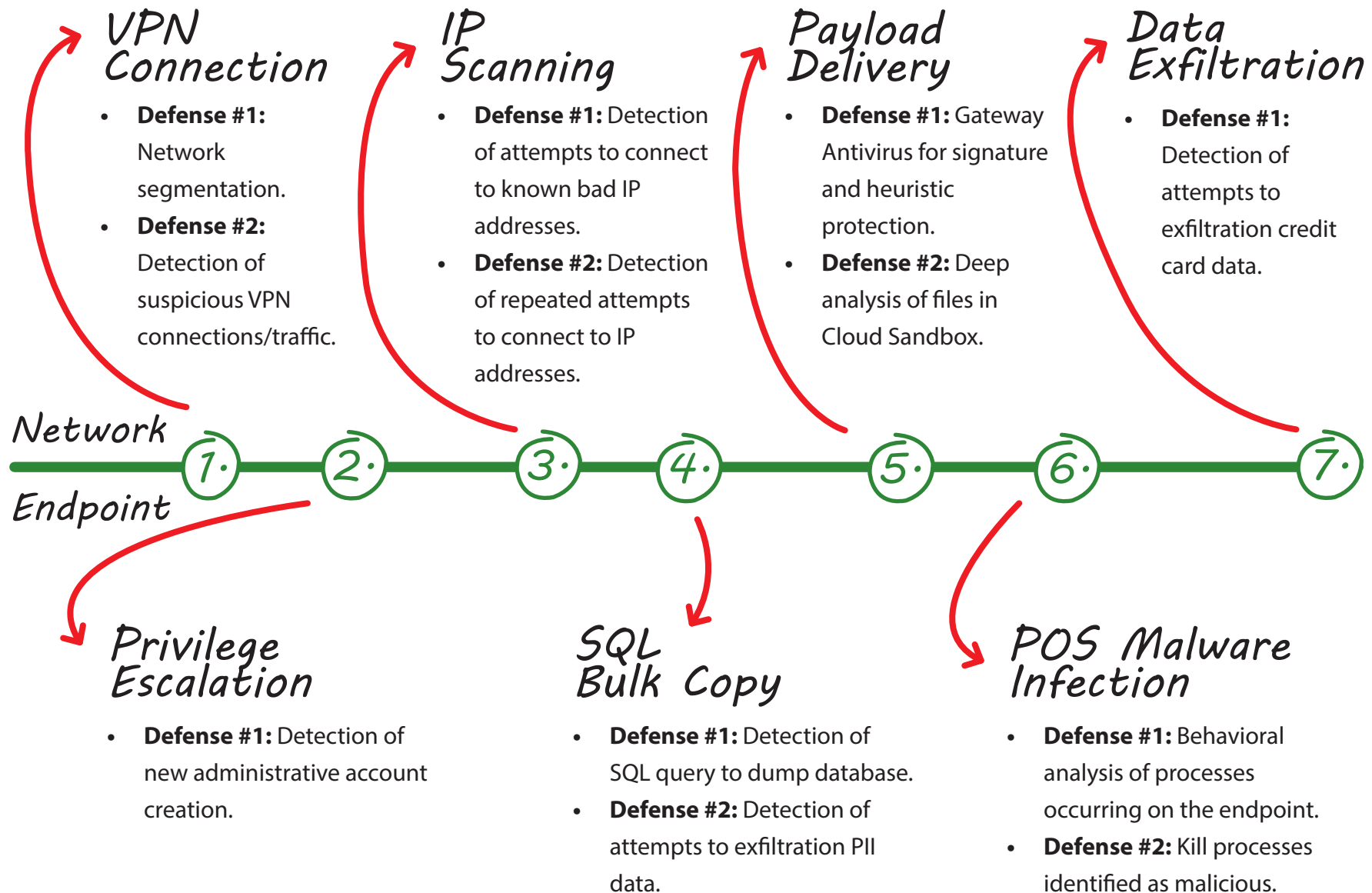


70

million

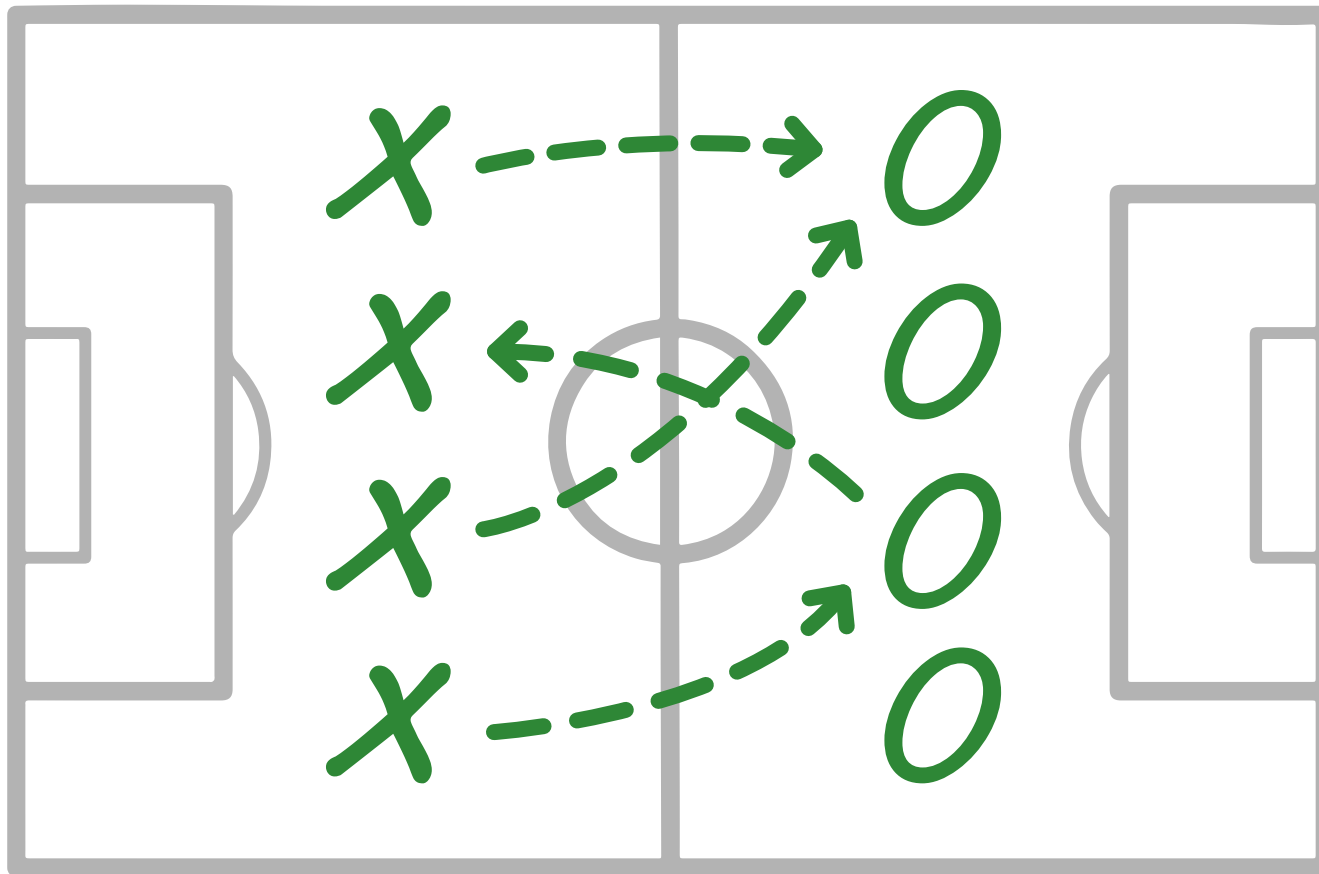
*customer records, including
names, addresses, emails,
and phone numbers were
copied in the 2013 Target
breach*

Figure 2.



Ready to get to work?!

We just covered A LOT of information on what you need to protect your organization against advanced malware attacks. To make it all a little easier, here's a checklist that should help in assessing your current defensive strategy. We would encourage you to re-evaluate your strategy every six months, so we've left space for a 6-month and 12-month check-in.



Now

Notes

☐ Back-ups

- Complete education training
- Ensure that automatic backups are in place

☐ Passwords

- Educate employees on the importance of strong passwords
- Set a standard policy on password length and refreshes
- Implement multi-factor authentication to ensure security even with weak passwords

☐ Phishing Email Education

- Educate employees on what a phishing email looks like
- Test employees with benign phishing emails

☐ Wireless

- Evaluate wireless security solution
- Educate employees on the risks of public Wi-Fi

☐ Defenses Against Known Threats

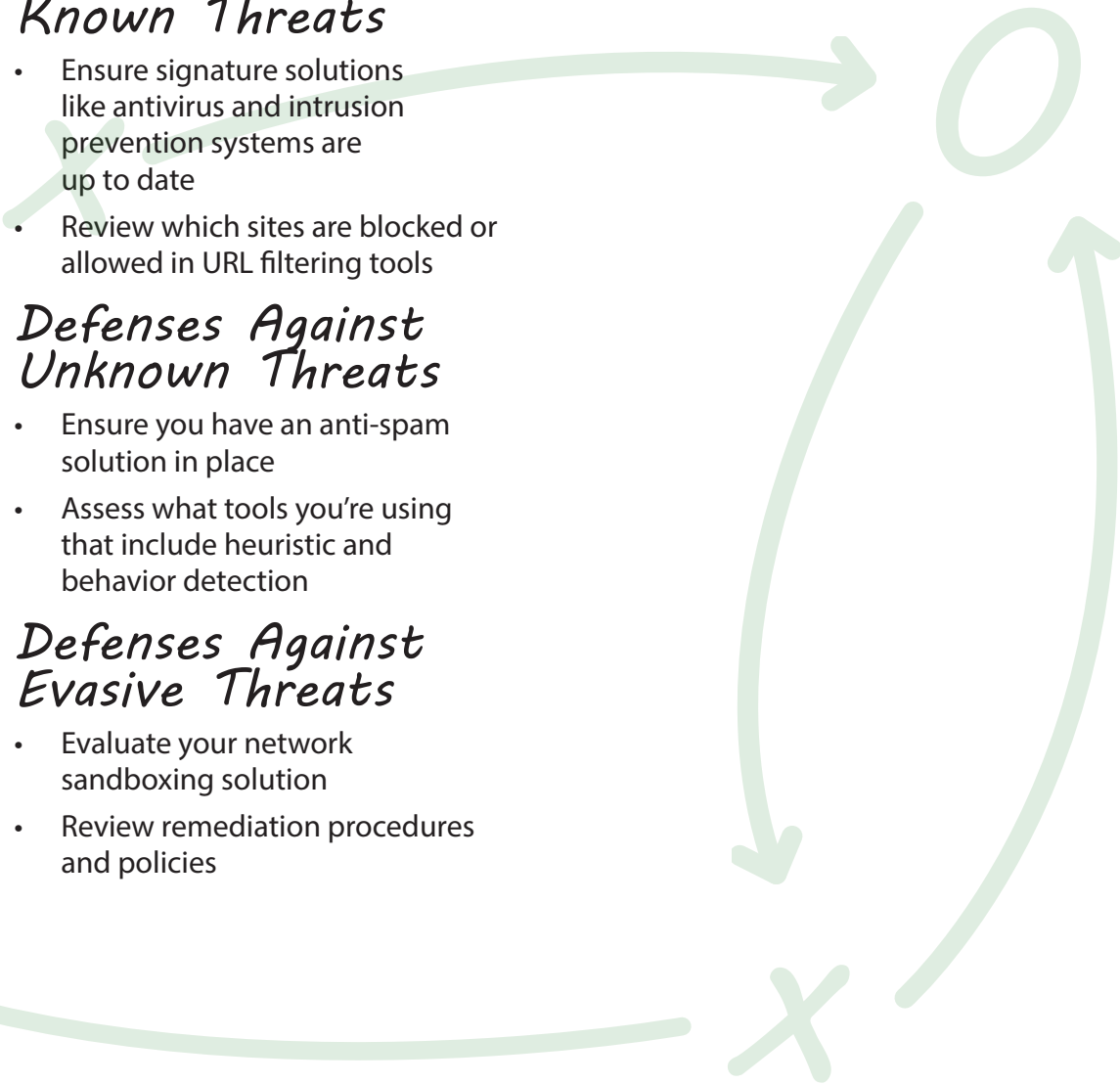
- Ensure signature solutions like antivirus and intrusion prevention systems are up to date
- Review which sites are blocked or allowed in URL filtering tools

☐ Defenses Against Unknown Threats

- Ensure you have an anti-spam solution in place
- Assess what tools you're using that include heuristic and behavior detection

☐ Defenses Against Evasive Threats

- Evaluate your network sandboxing solution
- Review remediation procedures and policies



6-month check-up

Notes

☐ Back-ups

- Complete education training
- Ensure that automatic backups are in place

☐ Passwords

- Educate employees on the importance of strong passwords
- Set a standard policy on password length and refreshes
- Implement multi-factor authentication to ensure security even with weak passwords

☐ Phishing Email Education

- Educate employees on what a phishing email looks like
- Test employees with benign phishing emails

☐ Wireless

- Evaluate wireless security solution
- Educate employees on the risks of public Wi-Fi

☐ Defenses Against Known Threats

- Ensure signature solutions like antivirus and intrusion prevention systems are up to date
- Review which sites are blocked or allowed in URL filtering tools

☐ Defenses Against Unknown Threats

- Ensure you have an anti-spam solution in place
- Assess what tools you're using that include heuristic and behavior detection

☐ Defenses Against Evasive Threats

- Evaluate your network sandboxing solution
- Review remediation procedures and policies

12-month check-up

Notes

☐ Back-ups

- Complete education training
- Ensure that automatic backups are in place

☐ Passwords

- Educate employees on the importance of strong passwords
- Set a standard policy on password length and refreshes
- Implement multi-factor authentication to ensure security even with weak passwords

☐ Phishing Email Education

- Educate employees on what a phishing email looks like
- Test employees with benign phishing emails

☐ Wireless

- Evaluate wireless security solution
- Educate employees on the risks of public Wi-Fi

☐ Defenses Against Known Threats

- Ensure signature solutions like antivirus and intrusion prevention systems are up to date
- Review which sites are blocked or allowed in URL filtering tools

☐ Defenses Against Unknown Threats

- Ensure you have an anti-spam solution in place
- Assess what tools you're using that include heuristic and behavior detection

☐ Defenses Against Evasive Threats

- Evaluate your network sandboxing solution
- Review remediation procedures and policies



WatchGuard Security Services

WatchGuard offers the most comprehensive portfolio of security services in the industry, from traditional intrusion prevention, gateway antivirus, application control, spam prevention, and URL filtering, to more advanced services for protecting against evolving malware, ransomware, and data breaches. Each security service is delivered as an integrated solution within an easy-to-manage and cost-effective Firebox appliance.

Basic Security Services



Intrusion Prevention

Intrusion Prevention Service uses continually updated signatures to scan traffic on all major protocols, providing real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.

[Learn More >](#)



Network Discovery

A subscription-based service for Firebox appliances that generates a visual map of all nodes on your network, making it easy to see where you may be at risk. It helps ensure only authorized devices are connected while detecting all open ports and protocols. [Learn More >](#)



Application Control

Allow, block, or restrict access to applications based on a user's department, job function, and time of day. It's never been easier to decide who, what, when, where, why and how applications are used on your network. [Learn More >](#)



Spam Prevention

Real-time, continuous, and highly reliable protection from spam and phishing attempts. WatchGuard spamBlocker is so fast and effective, it can review up to 4 billion messages per day, while providing effective protection regardless of the language, format, or content of the message. [Learn More >](#)



Reputation-Based Threat Prevention

A powerful, Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead. [Learn More >](#)



Gateway AntiVirus (GAV)

Leverage our continuously updated signatures to identify and block known spyware, viruses, trojans, worms, rogware and blended threats – including new variants of known viruses. At the same time, heuristic analysis tracks down suspicious data constructions and actions to make sure unknown viruses don't slip by.



URL Filtering

In addition to automatically blocking known malicious sites, WatchGuard WebBlocker delivers granular content and URL filtering tools to block inappropriate content, conserve network bandwidth, and increase employee productivity. [Learn More >](#)

Advanced Security Services



APT Blocker

APT Blocker uses an award-winning next-generation sandbox to detect and stop the most sophisticated attacks including ransomware, zero day threats, and other advanced malware designed to evade traditional network security defenses. [Learn More >](#)



WatchGuard Cloud Visibility and on-premises Dimension

WatchGuard Cloud Visibility provides full visibility into your network so that you can make timely, informed, and effective decisions about your network security anywhere, anytime. The platform displays 100+ dashboards and reports that allow you to quickly see high-level trends and anomalies then drill down into detailed information on each.

An on-premises visibility solution is available for those who do not want to move to the Cloud: WatchGuard Dimension. Dimension provides the big data visibility and reporting tools that uniquely identify and distill key network security threats, issues and trends, accelerating the ability to set meaningful security policies across the network. threats instantly, from one central console. [Learn More >](#)



Data Loss Prevention (DLP)

Prevent data breaches and enforce compliance by scanning text and files to detect sensitive information attempting to exit your network, whether it is transferred via email, web, or FTP. [Learn More >](#)



DNSWatch™

Reduce malware infections by detecting and blocking malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices. [Learn More >](#)



Access Portal

Access Portal provides a central location for access to Cloud-hosted applications, and secure, clientless access to internal resources with RDP and SSH. [Learn More >](#)



Threat Detection and Response

Security data collected from the Firebox and WatchGuard Host Sensor is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attacks. [Learn More >](#)



IntelligentAV

IntelligentAV is a signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery. Leveraging deep statistical analysis, it can classify current and future malware in mere seconds. [Learn More >](#)

One Appliance, One Package, Total Security

Simplicity is our mission at WatchGuard and that mission extends beyond how the product is built to how it is packaged. While all of our services are offered à la carte, we have worked to develop two packages that simplify the decision-making process. The Total and Basic Security Suite packages are available on our Firebox T and M Series appliances, as well as our Firebox Cloud and FireboxV virtual models.

- The **Basic Security Suite** includes all the traditional network security services typical to a UTM appliance: Intrusion Prevention Service, Gateway AntiVirus, URL filtering, application control, spam blocking and reputation lookup. It also includes our centralized management and network visibility capabilities, as well as, our standard 24x7 support.
- The **Total Security Suite** includes all services offered with the Basic Security Suite plus artificial intelligence enhanced advanced malware protection, DNS level protection, next-generation cloud sandboxing, data loss protection, enhanced network visibility capabilities, cloud-hosted threat correlation and scoring, and the ability to take action against threats right from Dimension, our network visibility platform. It also includes upgraded Gold level 24x7 support.

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
WatchGuard Cloud Visibility Data Retention	30 Days	1 Day
Support	Gold (24x7)	Standard (24x7)

**Available on latest generation M Series appliances*



PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

Cyber security is more relevant than ever before. The number of worldwide cyber attacks are at an all-time high with no signs of slowing down, as small to midsize businesses continue to fall victim with serious impact to their business operations and continuity. WatchGuard is here to provide the layered protection you need against the most advanced types of malware, and deliver it in a way that is simple to maintain. You face the same threats as enterprise organizations, shouldn't you have the same level of security?

Global Headquarters United States

Tel: +1.800.734.9905
Email: sales@watchguard.com

European Headquarters The Netherlands

Tel: +31(0)70.711.20.85
Email: sales-benelux@watchguard.com

APAC & SEA Headquarters Singapore

Tel: +65.3163.3992
Email: inquiry.sea@watchguard.com

© 2019 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67041_110719