Blog Post

How to Prevent Ransomware – A Technical Checklist

John Headley

Filed under

Cybersecurity, Fortinet, KnowBe4, Proofpoint, Ransomware

Unfortunately, there is no single solution to prevent ransomware or stop the spread once it has infiltrated your network; a defense in depth approach must be used. Below is a comprehensive, but not exhaustive, list of technical and administrative controls that can be used in your business' defense against ransomware.

Your Ransomware Technical Checklist

Employee Training

☑ Security Awareness Training

Email Security

☑ Secure Email Gateway
☑ Zero-Day Threat Prevention (Sandboxing)

Endpoint Security

☑ Endpoint Detection & Response (EDR)

Zero Trust Network Access (ZTNA)

☑ Next-Gen Firewall
☑ SSL Deep Packet Inspection
☑ Internal Network Segmentation / Microsegmentation
☑ Network Access Control (NAC)

Security Information & Event Management (SIEM)

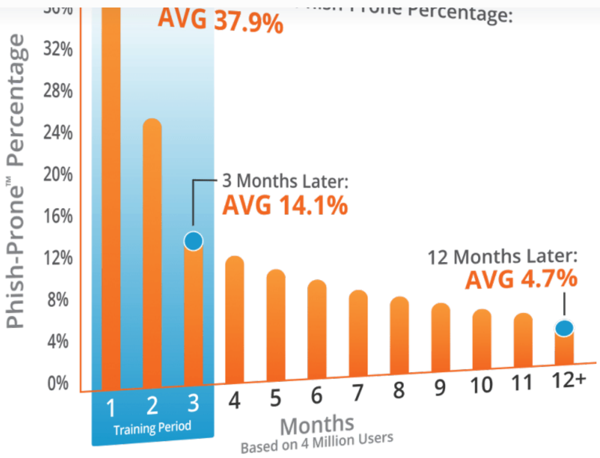
☑ SIEM

Business Continuity

☑ Offsite Backups & Disaster Recovery

Employee Training

report, the most common attack vector for ransomware is email, with infection occurring from a user unknowingly clicking on a malicious link or attachment. Before focusing on email security (our next recommendation on this checklist), security awareness training is imperative to decrease the odds that your workforce falls for common social engineering tactics employed by attackers.



Source: KnowBe4

With simulated phishing attacks on your employees, ransomware simulation, domain spoof testing, and more, good security awareness training programs go far beyond than just presenting a boring slideshow to your employees, and will leave your workforce much more cautious and prepared to defend themselves against these clever attacks.

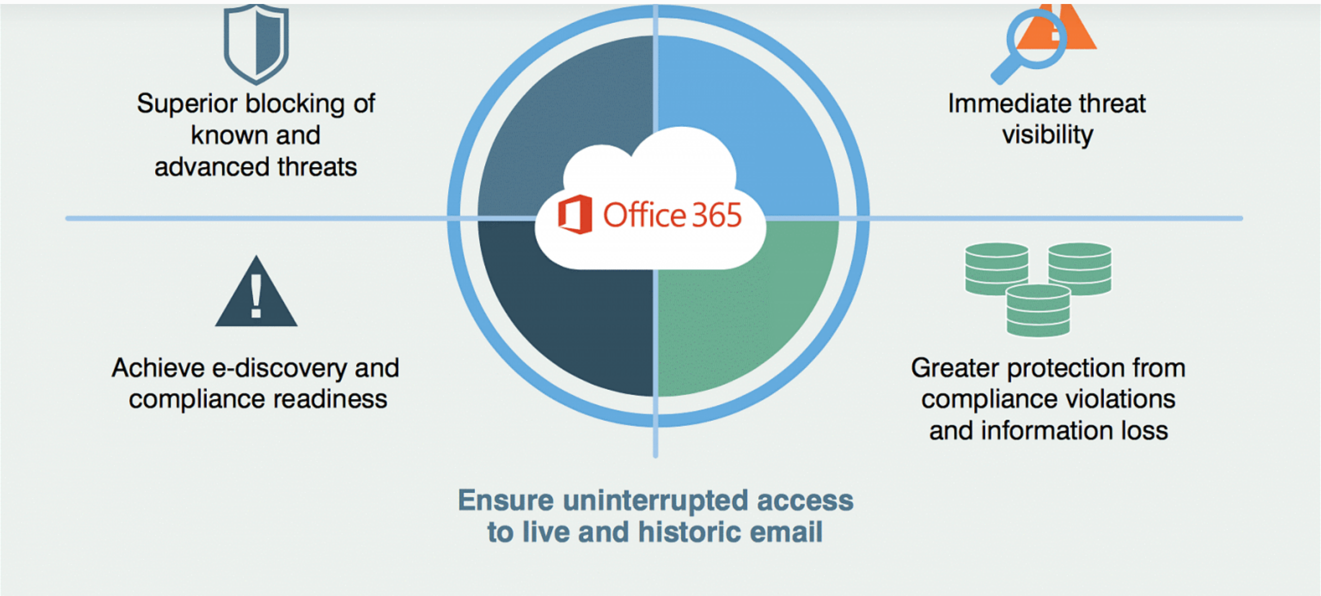
VPLS Recommends: KnowBe4

Email Security

Secure Email Gateway

As we discussed above, email is statistically the most likely threat vector for ransomware and therefore one your organization should not take lightly. Major email providers, such as Office 365, do offer some level of threat prevention built into their platform, but data shows administrators are not confident in the capabilities of this included protection. Secure email gateways offer a more complete list of protection mechanisms to thwart the ever-changing techniques employed by modern day attackers, as well as providing better visibility to any incidents that may occur.

VPLS Recommends: Proofpoint Essentials


Superior blocking of known and advanced threats
Immediate threat visibility
Office 365
Achieve e-discovery and compliance readiness
Greater protection from compliance violations and information loss
Ensure uninterrupted access to live and historic email

Zero-Day Threat Prevention (Sandboxing)

Of the assortment of comprehensive protection features offered by secure email gateways, ensure that your solution includes both attachment and URL sandboxing. Sandboxing is the solution for zero-day ransomware threats that can bypass normal filters. Files and URLs are automatically scanned using a cloud-based or on-prem sandbox environment, allowing full execution and analysis of the attachment or URL to ensure no bad behavior will occur once the attached has been opened or the URL visited.

VPLS Recommends: Proofpoint Essentials (email only) or FortiSandbox(standalone/multi-source)

Endpoint Security

Endpoint Detection & Response (EDR)

We discuss the what and why of EDR in our 5-minute primer on EDR, but the crux is that traditional endpoint protection is not good

enable both protecting the host from getting infected in the first place (pre-infection protection), as well as detecting an infection has occurred and handling the threat if it infiltrates the computer (post-infection protection).

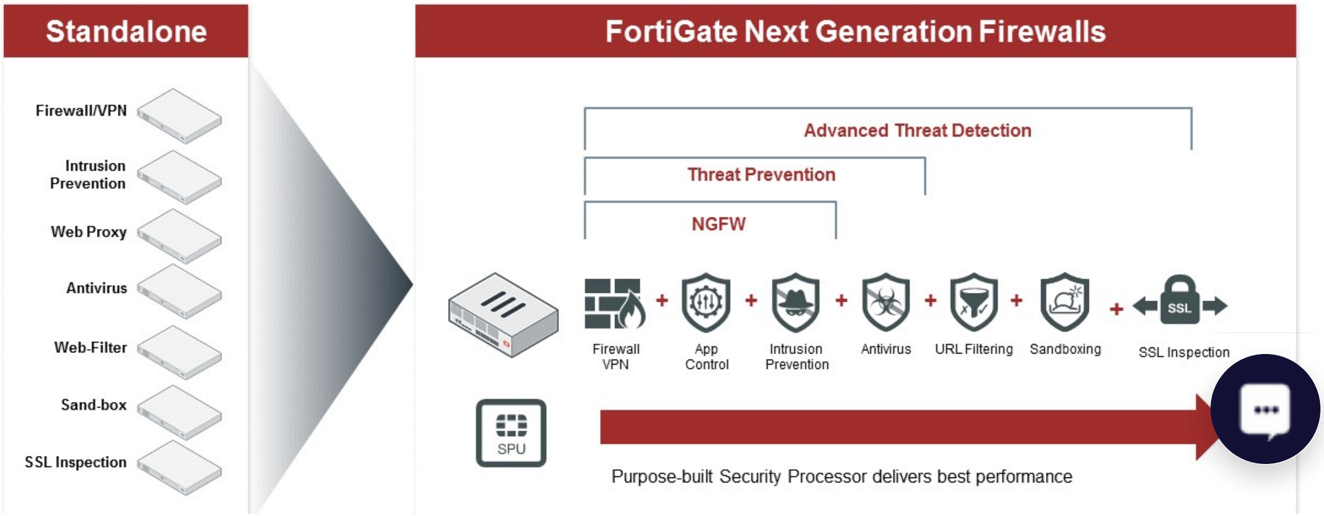
The ability to detect and defuse ransomware, as well as automatic playbooks for responding and remediating the infection are critical to ensure one infected host does not compromise the rest of your corporate assets.

VPLS Recommends: FortiEDR via VPLS's Managed Detection & Response (MDR) Service

Zero Trust Network Access (ZTNA)

Next-Gen Firewall

For protecting both on-prem and remote corporate users and company assets, a next-gen firewall is critical to ensure you have the detailed visibility and granular policy enforcement required to protect a network environment from ransomware. The old days of creating policies using just IP addresses and port numbers alone are gone, as a next-gen firewall has the intelligence to allow layer 7 application filtering and granular network access based on user ID or user group, regardless of their IP address or port numbers.



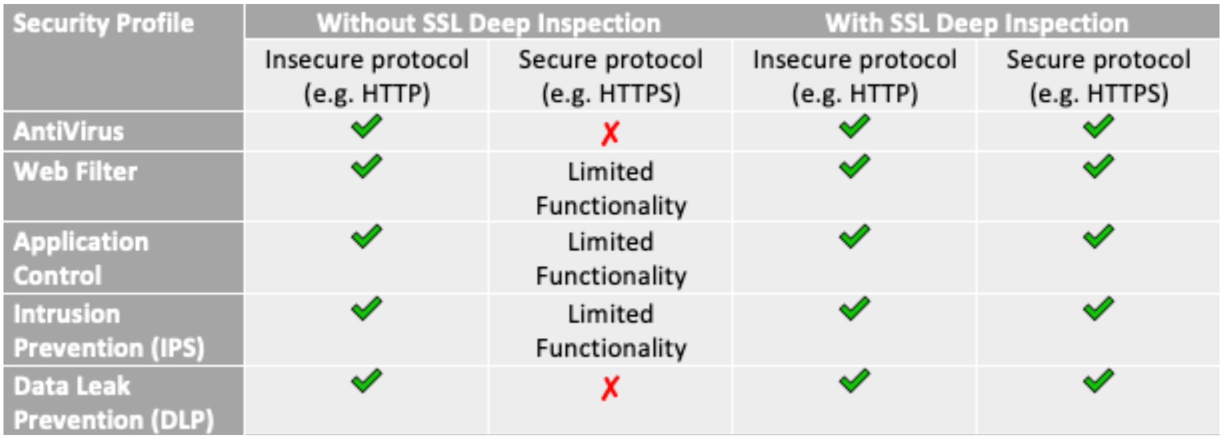
filtering, and SSL inspection, which when configured with ransomware in mind, will ensure that you notice and block even the most elusive indicators of attack (IOA) and indicators of compromise (IOC).

VPLS Recommends: Fortinet FortiGate via VPLS's Managed Firewall Service

SSL Deep Packet Inspection

Commonly overlooked or put at the bottom of a firewall admin's to-do list, SSL deep packet inspection, also known as SSL decryption, allows a next-gen firewall to inspect the payload of encrypted traffic being sent to and from corporate assets. This is important because without SSL deep packet inspection, ransomware hiding in encrypted payloads will not be caught by the next-gen firewall. Additionally, since many next-gen firewall features will not function or will only function partially, like IPS/IDS and network-level antivirus, you may miss out on key indicators of attack (IOA) and indicators of compromise (IOC) that you would otherwise have visibility into.

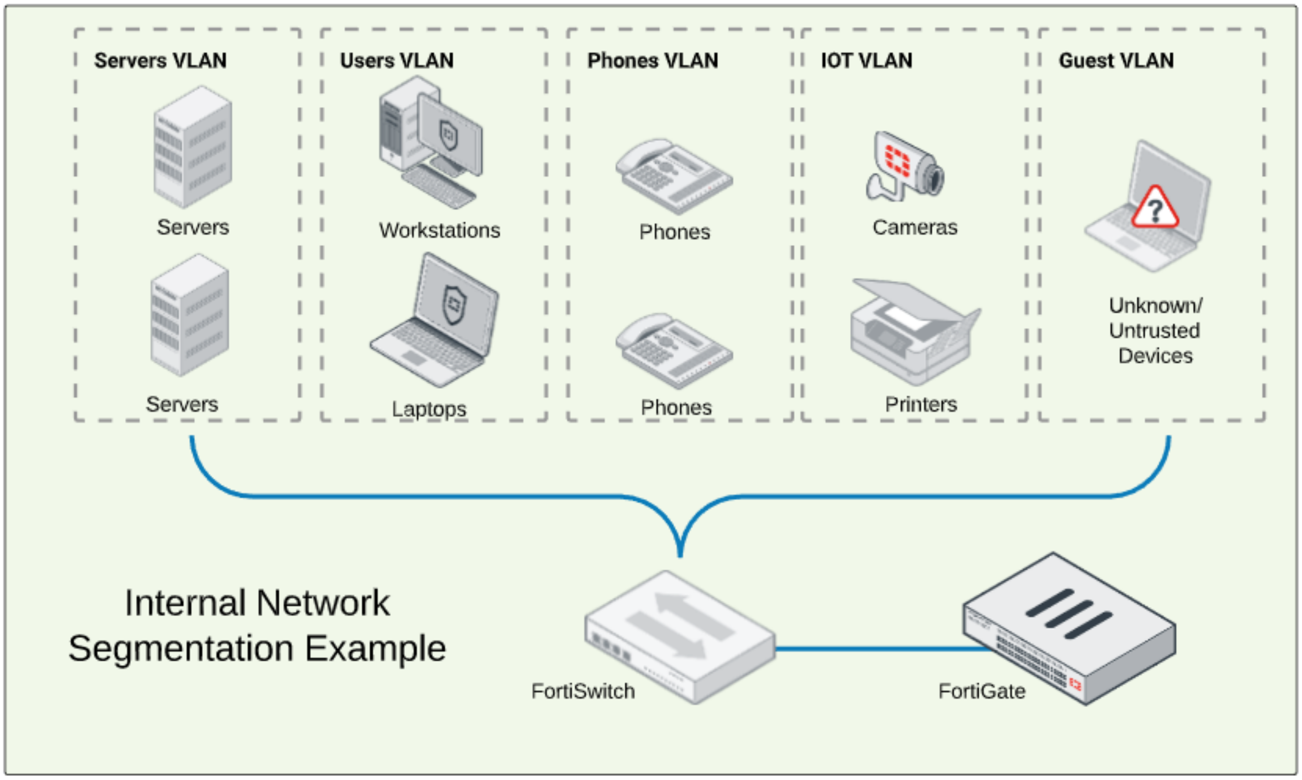
VPLS Recommends: Fortinet FortiGate via VPLS's Managed Firewall Service



Security Profile	Without SSL Deep Inspection		With SSL Deep Inspection	
	Insecure protocol (e.g. HTTP)	Secure protocol (e.g. HTTPS)	Insecure protocol (e.g. HTTP)	Secure protocol (e.g. HTTPS)
AntiVirus	✓	✗	✓	✓
Web Filter	✓	Limited Functionality	✓	✓
Application Control	✓	Limited Functionality	✓	✓
Intrusion Prevention (IPS)	✓	Limited Functionality	✓	✓
Data Leak Prevention (DLP)	✓	✗	✓	✓

Internal Network Segmentation/Microsegmentation

All next-gen firewall deployments are not created equal. "Flat networks" of yesteryear allow unrestricted lateral movement of ransomware once a computer your internal-to-internal traffic, not just for traffic leaving the network edge.



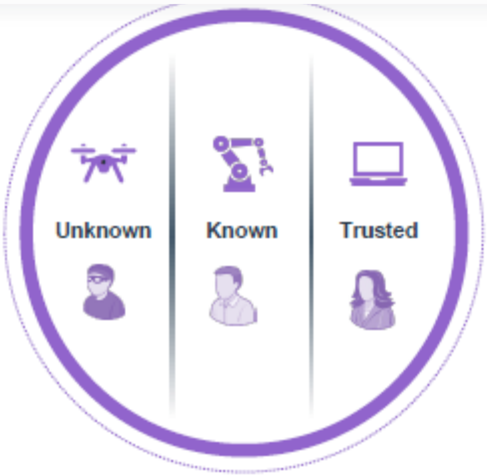
Microsegmentation takes this internal network segmentation one step further and allows you fine-grained control to police the traffic between devices that are a part of two internal segments or even the same internal segment. This can be achieved by creating policies based on user identity and/or deploying an endpoint-level application firewall on the hosts themselves.

VPLS Recommends: Fortinet FortiGate via VPLS's Managed Firewall Service + FortiSwitch via VPLS's Managed Network Service

Network Access Control (NAC)

Whether your users are on-prem or remote, one computer infected with ransomware is all it takes to begin a chain reaction that will quickly bring your business to a halt. In conjunction with your next-gen firewall and the internal network segmentation deployment topology, NAC should be in place to facilitate dynamic network access control, which ensures only trusted corporate devic automatically get placed in an appropriate internal network segment and hav

After the NAC solution dynamically allows access based on device trust, endpoint compliance should also be continually evaluated. If the host does not meet compliance requirements, such as if the host becomes infected, does not have antivirus running or it is out of date for too long, or the host does not have the latest OS patches installed, the host should be moved to a restricted quarantine or remediation VLAN until the missing criteria is met.



Remote users aren't excluded here—NAC and endpoint compliance can and should be enforced for users before allowing them to connect to the corporate VPN.

VPLS Recommends: Fortinet FortiNAC

Security Information & Event Management (SIEM)

SIEM

A defense in depth approach to cybersecurity provides thorough protection against ransomware, but it also provides a thorough amount of something else—logs! Not only will many logs be generated from these various systems we have talked about, but your team must devise an efficient method to parse through the logs, pull out key information, and alert IT personnel about security events that are occurring to ensure your business has a firm grasp of the activity occurring in the network environment.

URLS
http://
MALWARE SAMPLES
FILE HASHES
#
DOMAINS
IP ADDRESSES
192.16
OPEN THREAT EXCHANGE
ALIENVAULT THREAT INTELLIGENCE
PUBLIC CLOUD
AWS
Azure

Enter the SIEM. A SIEM solves the complex problem of aggregating logs from multiple sources and performing event correlation. The logs and real-time diagnostic data from all of your endpoints and network equipment allow the SIEM to intelligently zero in on suspicious or malicious activity and send appropriate alerts to your staff in real-time. SIEMs typically also include vulnerability scanning capabilities, cloud monitoring, host-based IDS, and an assortment of other complementary components too, providing your security team with even more powerful analytics and response capabilities at their fingertips.

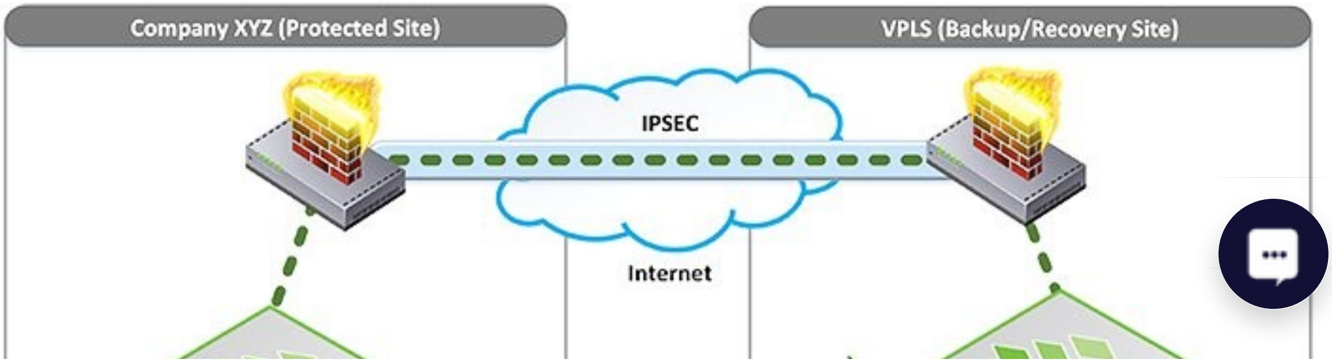
VPLS Recommends: AlienVault via VPLS's Managed SOC Service

Business Continuity

Offsite Backups & Disaster Recovery

When it comes to ransomware, a prepared business should always plan for the worst-case scenario—infection, data being held at ransom, and business grinding to a halt. In this unfortunately common doomsday scenario, having offsite backups protected from infection, as well as a dependable disaster recovery plan, can exponentially decrease financial loss and ensure your business gets back up and running within minutes.

VPLS Recommends: VPLS's Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS)



My checklist is complete; now what?

The checklist above contains truly business-saving technical controls that can be used to enhance your business' security posture and increase its defenses against ransomware. However, as mentioned at the beginning of this post, this list is not exhaustive, and many things were left out from this checklist for the sake of brevity—mobile device management (MDM), cloud access security broker (CASB), browser isolation, and user entity and behavior analytics (UEBA), just to name a few.

The fight against ransomware never stops, and whether you want to discuss the items mentioned in this checklist, or are ready to explore what's next, **VPLS is here to help.**

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

If you enjoyed this article, you'll probably like:

BLOG POST
5 Reasons SOC-as-a-Service
Will Give You Peace of Mind
If you're not sure if outsourcing your SOC is worth it, here are some SOC-as-a-Service features that provide peace of mind
READ NOW

5 Reasons SOC-as-a-Service Features Help You

March 29, 2022

Read More »

What is SOC-as-a-Service?
SOC-as-a-Service (SOCaaS) functions as an extension of a company's IT department and helps take the guesswork out of cybersecurity.
READ NOW

What Is SOC-as-a-Service?

March 28, 2022

Read More »

BLOG POST
VDI vs. VPN
What's Best for Remote Employees?
Many companies struggle with deciding which of these two common remote work is better for their workforce.
READ NOW

VDI vs. VPN: What’s Best for Remote Employees?

Read More »

HOW TO REACH US

24/7/365 Customer Service
+1 (888) 365-2656
support@vpls.com

Sales Inquiries
+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector