4 WAYS TO PROTECT YOUR CHARTER SCHOOL FROM CYBER ATTACKS

MARCO ALCALA

626-449-5549

marco@alcalaconsulting.com

www.alcalaconsulting.com

ALCALA

AGENDA

- About Me
- The Cyber Threat Landscape
- 4 Ways To Protect Your Charter Schools Form Cyber Attacks and Self Assessment

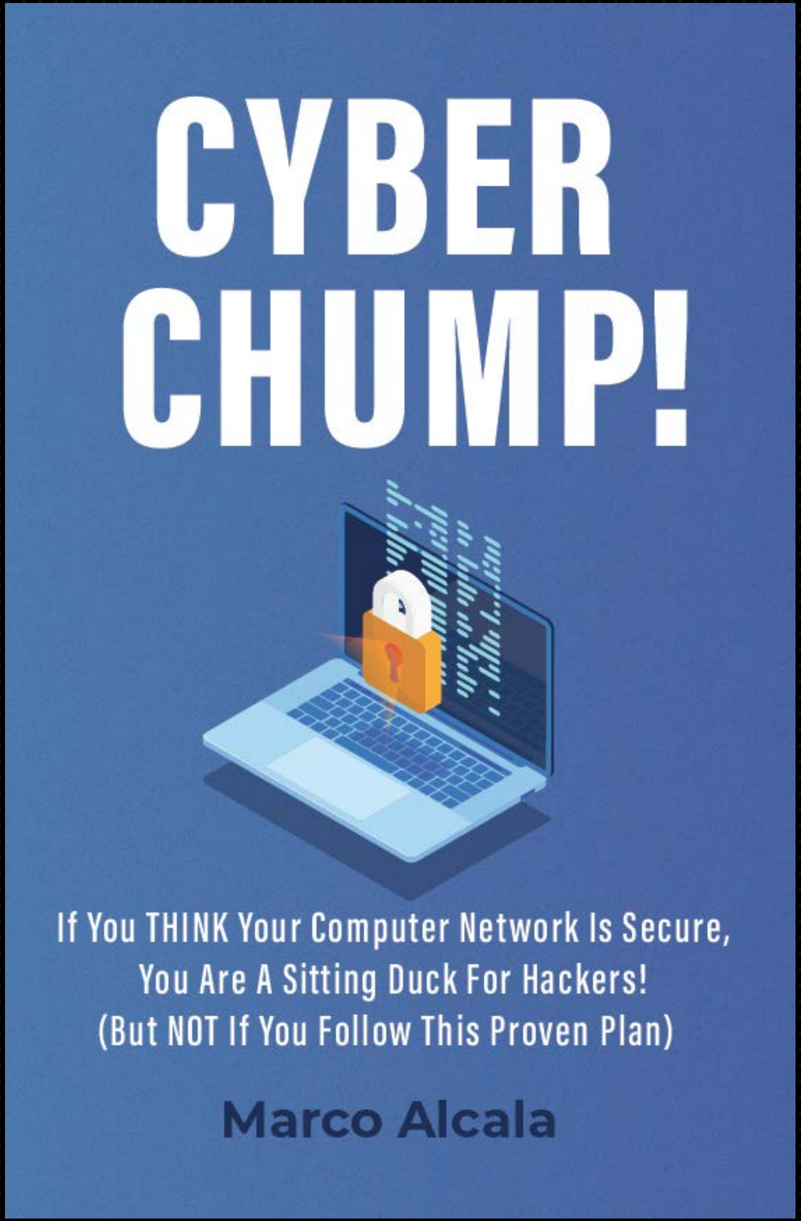
ABOUT ME

MY RELEVANT EXPERIENCE

25 Years Experience

27 Cybersecurity Programs

Published Cybersecurity Book Author

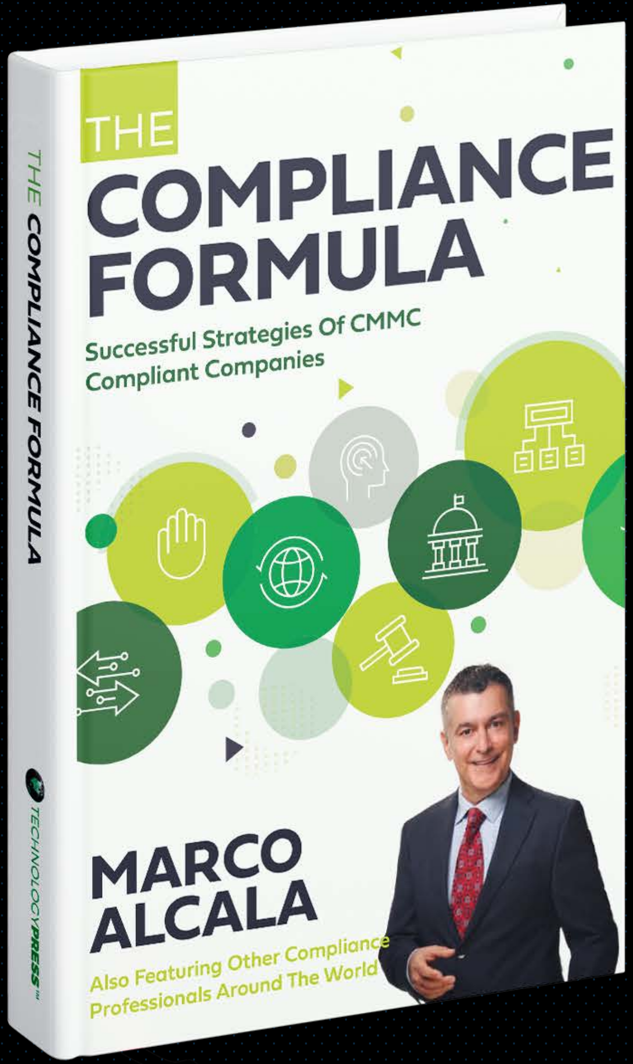


CYBER CHUMP!

If You THINK Your Computer Network Is Secure, You Are A Sitting Duck For Hackers! (But NOT If You Follow This Proven Plan)

Marco Alcala

BOOK RELEASED IN 2022


THE
COMPLIANCE
FORMULA
Successful Strategies Of CMMC
Compliant Companies
MARCO
ALCALA
Also Featuring Other Compliance
Professionals Around The World
THE COMPLIANCE FORMULA
TECHNOLOGYPRESS

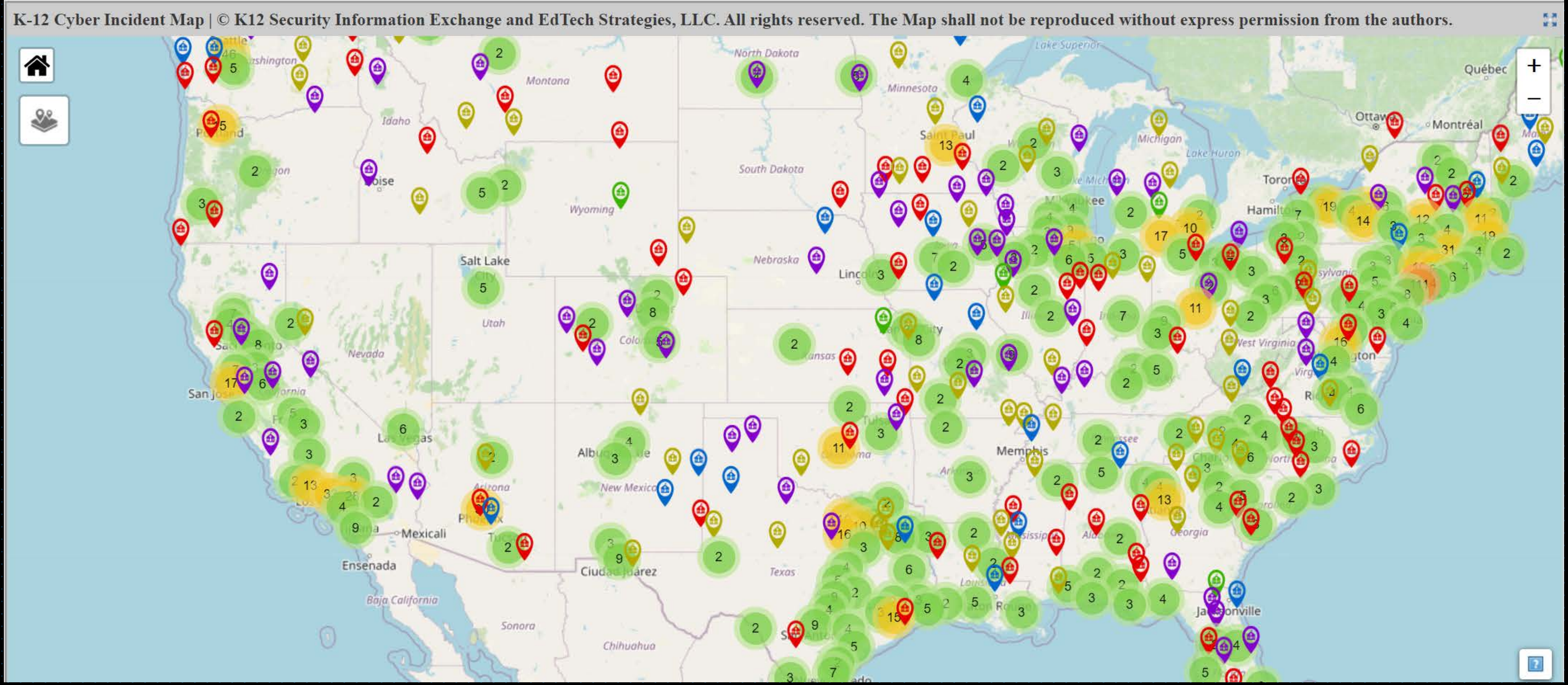
RELEASE DATE:
MARCH 30, 2023

All royalties will be donated
to St. Jude’s Children Hospital

ENOUGH ABOUT ME

THE CYBER THREAT LANDSCAPE

SCHOOL CYBER INCIDENTS



K-12 Cyber Incident Map | © K12 Security Information Exchange and EdTech Strategies, LLC. All rights reserved. The Map shall not be reproduced without express permission from the authors.

Source https://www.k12six.org/

EASY MONEY

$10 PER STUDENT RECORD

$1 PER STAFF/TEACHER RECORD

CYBERCRIME MARKET VALUE

Business Email Compromise (BEC) 1.1 billion in 2022

BEC will grow to 2.8 billion by 2027

Ransomware payments of $457 million in 2022

Sources: https://www.marketsandmarkets.com and https://www.bleepingcomputer.com

ALL EXPENSES PAID RETREATS

HOW MUCH THE BAD GUYS GET PAID

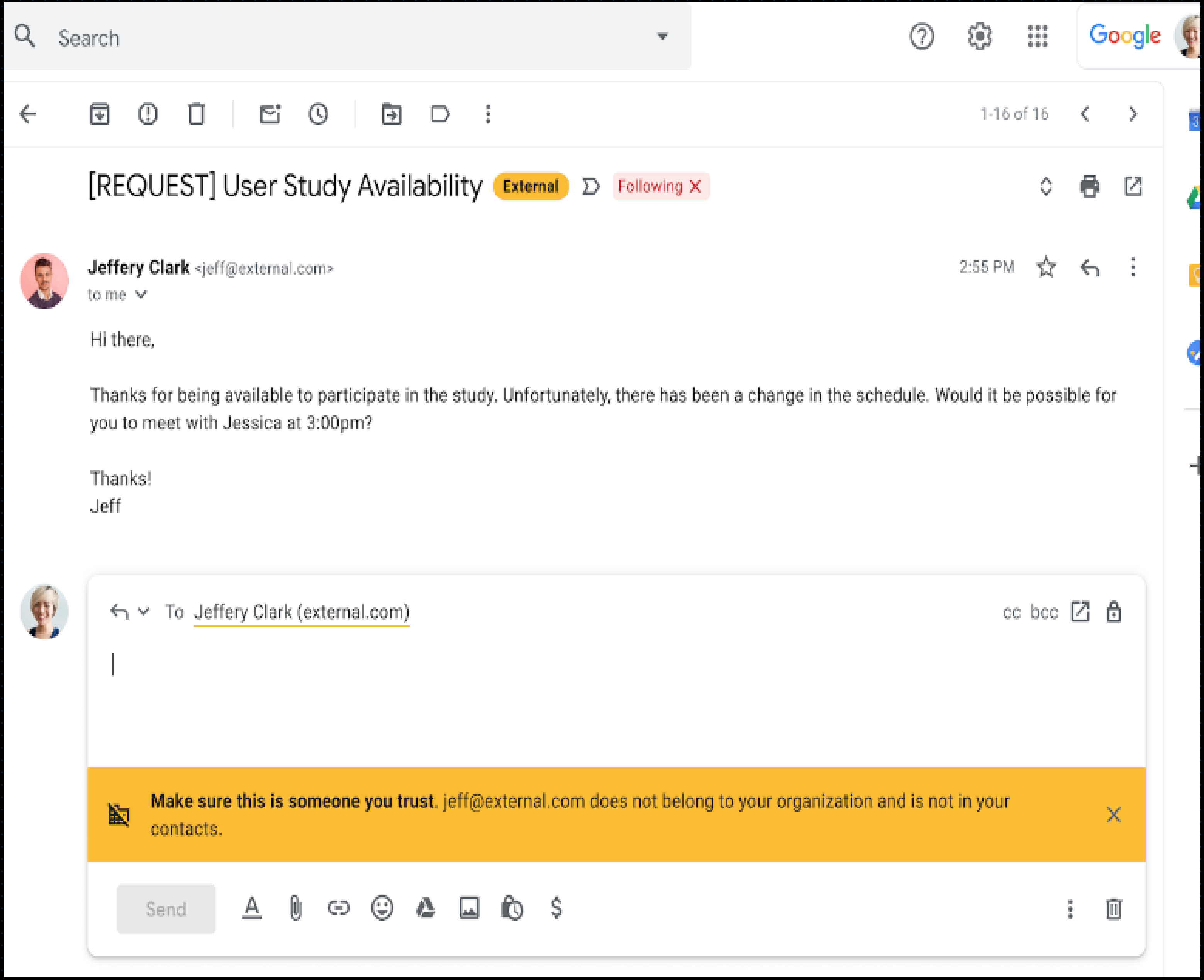
$5,000/MONTH – DURING TRAINING

$60,000/MONTH – AFTER PROBATION

$90,000/MONTH – IF THEY ARE GOOD

THAT WAS THE CYBER THREAT LANDSCAPE

1. EMAIL SECURITY CONTROLS



[REQUEST] User Study Availability

Jeffery Clark <jeff@external.com>

to me

2:55 PM

Hi there,

Thanks for being available to participate in the study. Unfortunately, there has been a change in the schedule. Would it be possible for you to meet with Jessica at 3:00pm?

Thanks!
Jeff

To Jeffery Clark (external.com)

Make sure this is someone you trust. jeff@external.com does not belong to your organization and is not in your contacts.

1.1 - EXTERNAL EMAIL TAGGING

SOLUTIONS FOR EXTERNAL EMAIL TAGGING:

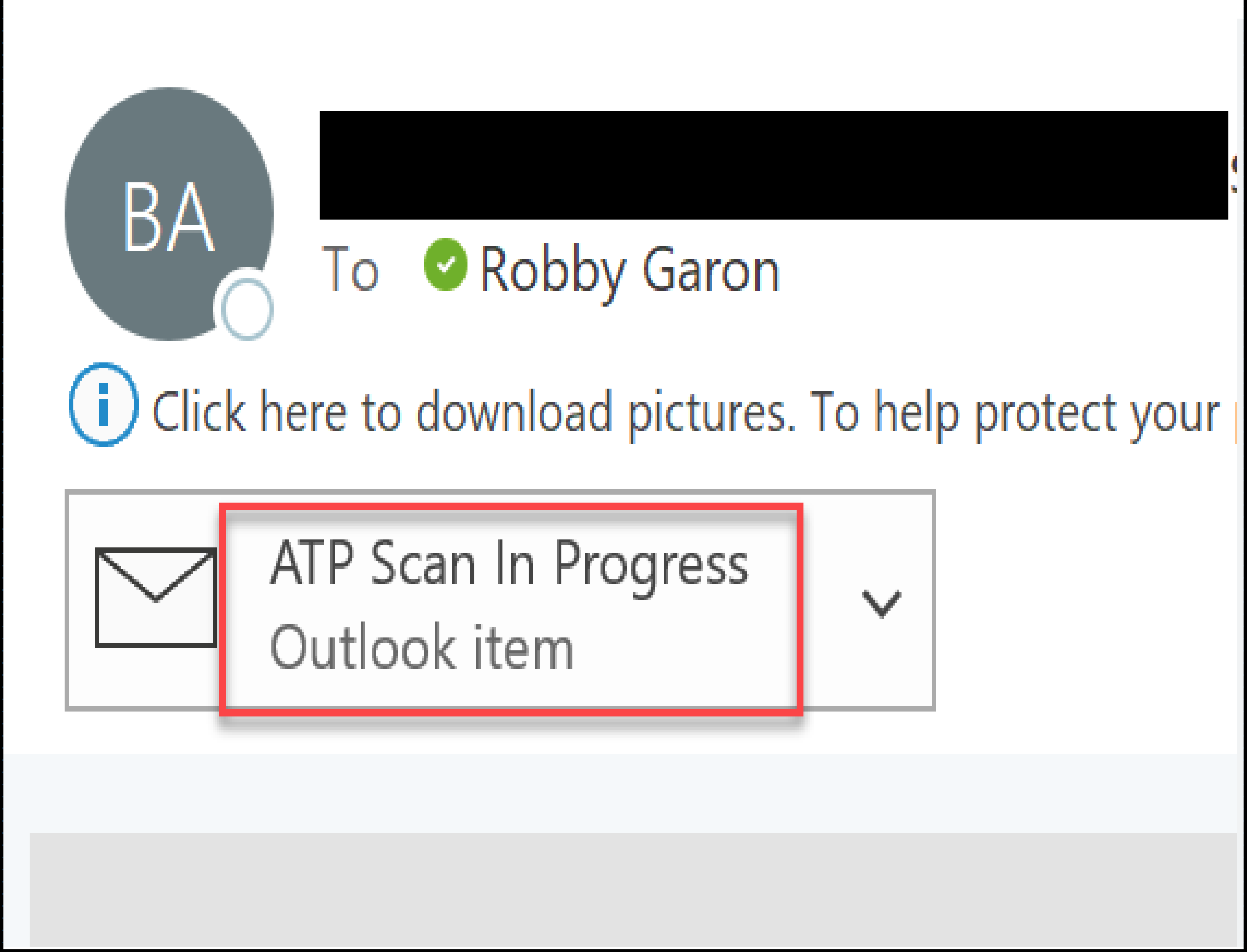
Google Workspace:

- Warn for external recipients

Office 365

- Transport rule to prepend “External” to subject line

1.2 - EMAIL ATTACHMENT SCANNING



[redacted]

To ✓ Robby Garon

Click here to download pictures. To help protect your

ATP Scan In Progress
Outlook item

SOLUTIONS FOR EMAIL ATTACHMENT SCANNING:

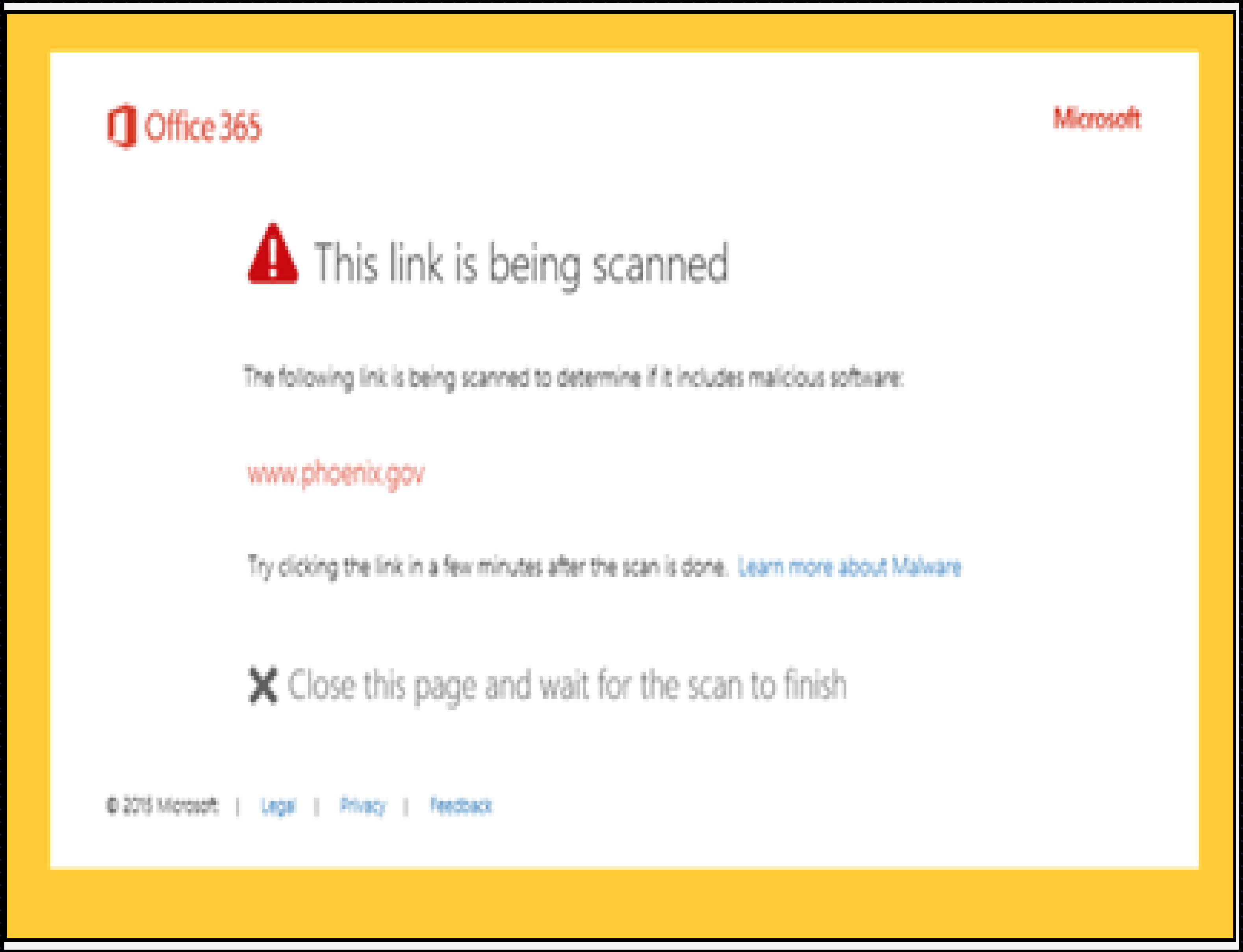
Google Workspace:

Set up rules to detect harmful attachments

Office 365

Set up Safe Attachments Policies In Microsoft Defender For Office 365

1.3 - EMAIL LINKS SCANNING



Office 365

Microsoft

This link is being scanned

The following link is being scanned to determine if it includes malicious software:

www.phoenix.gov

Try clicking the link in a few minutes after the scan is done. Learn more about Malware

✕ Close this page and wait for the scan to finish

© 2015 Microsoft | Legal | Privacy | Feedback

SOLUTIONS FOR EMAIL LINKS SCANNING:

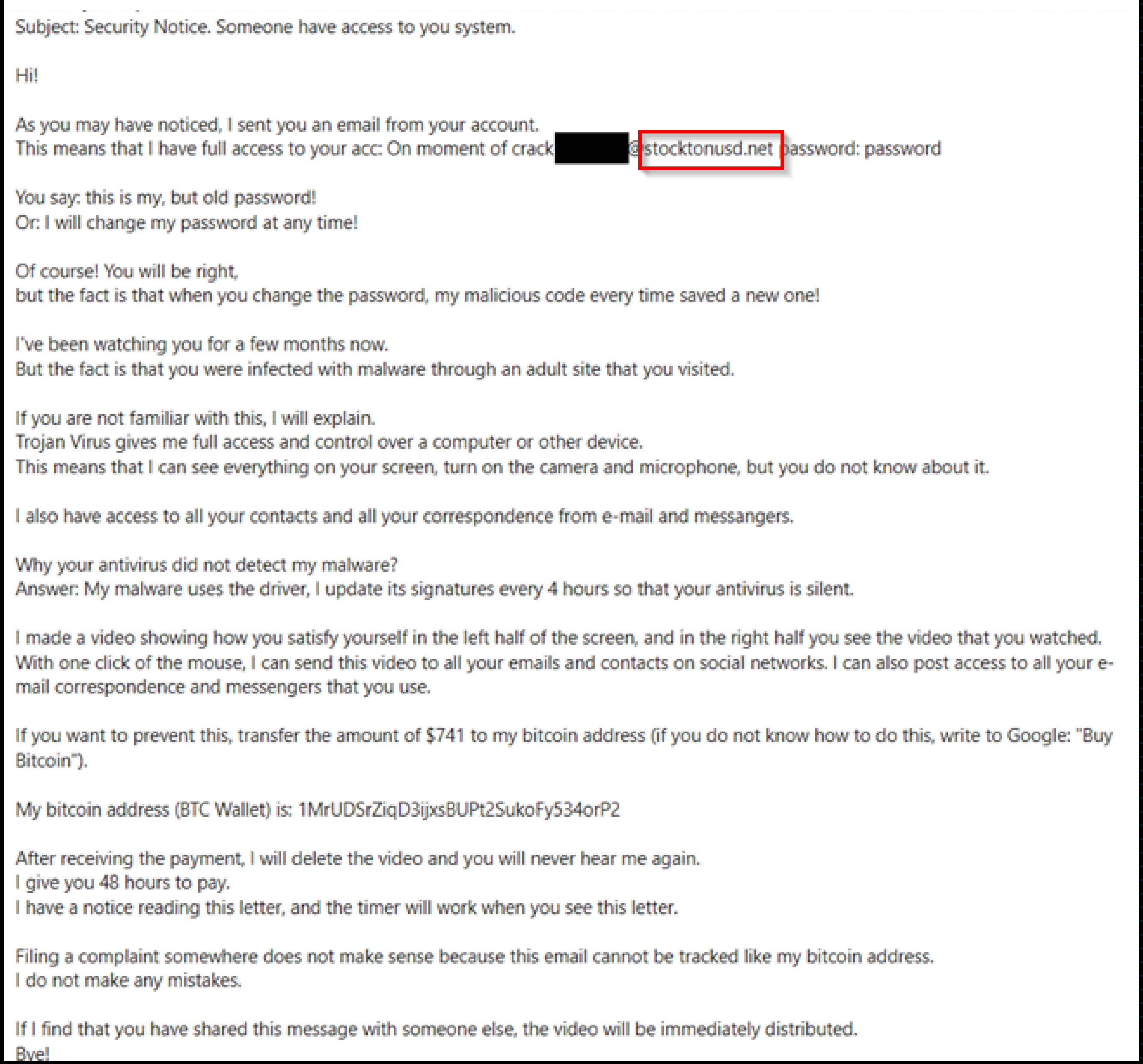
Google Workspace:

Turn on External Images and Links Protection

Office 365

Set up Safe Links Policies In Microsoft Defender For Office 365

1.4 -SPOOFED EMAILS



Subject: Security Notice. Someone have access to you system.

Hi!

As you may have noticed, I sent you an email from your account.
This means that I have full access to your acc: On moment of crack [redacted]@stocktonusd.net password: password

You say: this is my, but old password!
Or: I will change my password at any time!

Of course! You will be right,
but the fact is that when you change the password, my malicious code every time saved a new one!

I've been watching you for a few months now.
But the fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence from e-mail and messangers.

Why your antivirus did not detect my malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched. With one click of the mouse, I can send this video to all your emails and contacts on social networks. I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this, transfer the amount of $741 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 1MrUDSrZiqD3ijxsBUPt2SukoFy534orP2

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.
Bye!

SOLUTIONS SPOOFED EMAILS:

Sender Policy Framework (SPF)

Configuring SPF

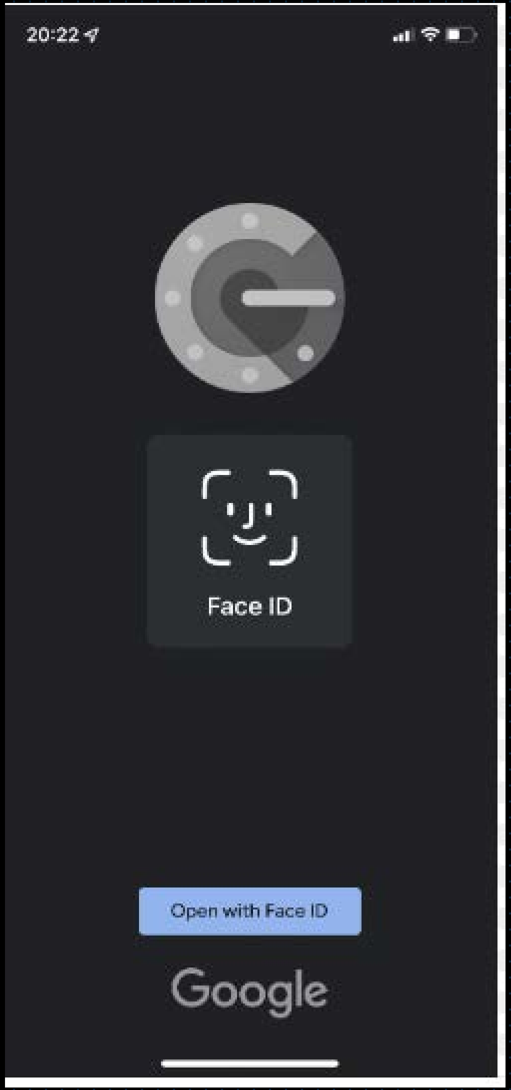
Domain-based Message Authentication Reporting and Conformance (DMARC):

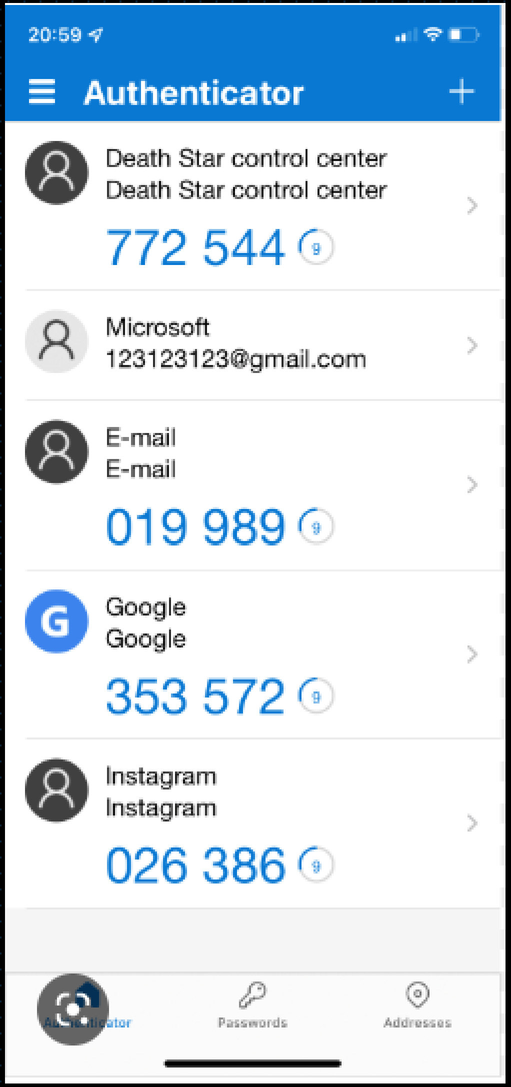
How to configure DMARC

Domain Keys Identified Email (DKIM)

How to configure DKIM

1.5 –EMAIL MULTIFACTOR AUTHENTICATION (MFA)





Death Star control center
Death Star control center
772 544

Microsoft
123123123@gmail.com

E-mail
E-mail
019 989

Google
Google
353 572

Instagram
Instagram
026 386

SOLUTIONS EMAIL MULTIFACTOR AUTHENTICATION:

Google Workspace

- How to configure 2-step Verification

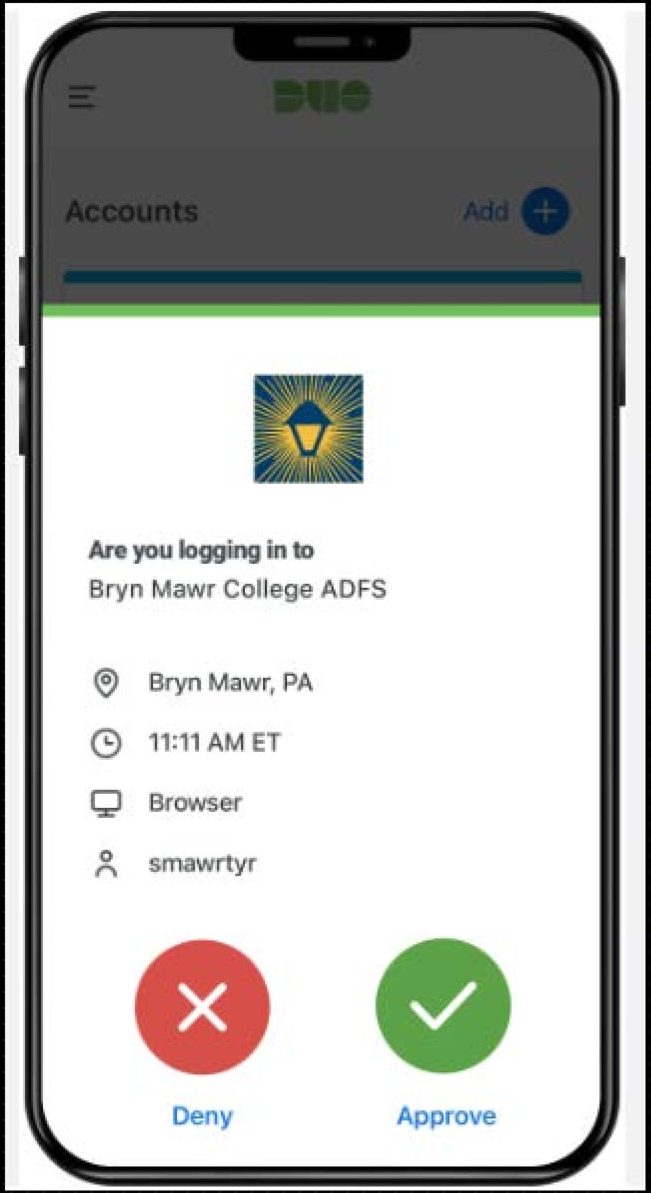
Microsoft 365

- How to configure M365 Multi-factor Authentication

THAT CONCLUDES EMAIL SECURITY CONTROLS

2. INTERNAL SECURITY CONTROLS

2.1 – MULTIFACTOR AUTHENTICATION (MFA) FOR CLOUD APPS, VPN, REMOTE DESKTOPS, AND SYSTEM ADMINISTRATOR ACCOUNTS



Are you logging in to
Bryn Mawr College ADFS

Bryn Mawr, PA
11:11 AM ET
Browser
smawrtyr

MFA FOR CLOUD APPS, VPN, REMOTE DESKTOPS, AND ADMINISTRATOR ACCOUNTS:

MFA Providers

- Duo Security
- JumpCloud
- Okta

2.2 – DATA ENCRYPTION FOR LAPTOPS, DESKTOPS, SERVERS, AND MOBILE DEVICES

DATA ENCRYPTION SOLUTIONS:

APPLE

How to configure Apple FileVault

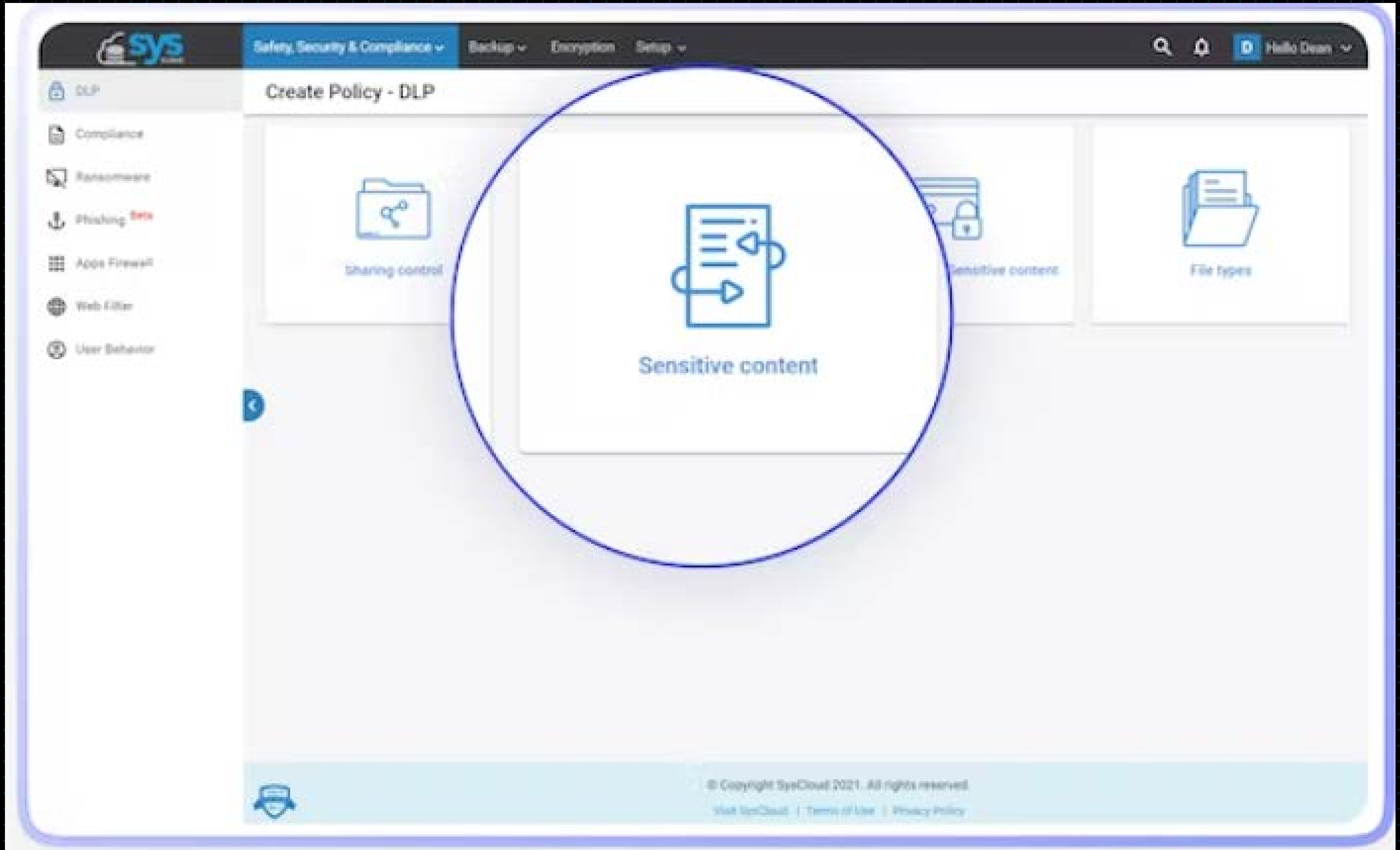
GOOGLE

Requiring Data Encryption For Mobile Devices and Endpoints

MICROSOFT

Configuring data encryption using Microsoft Intune

2.3 – DATA LOSS PREVENTION (DLP)

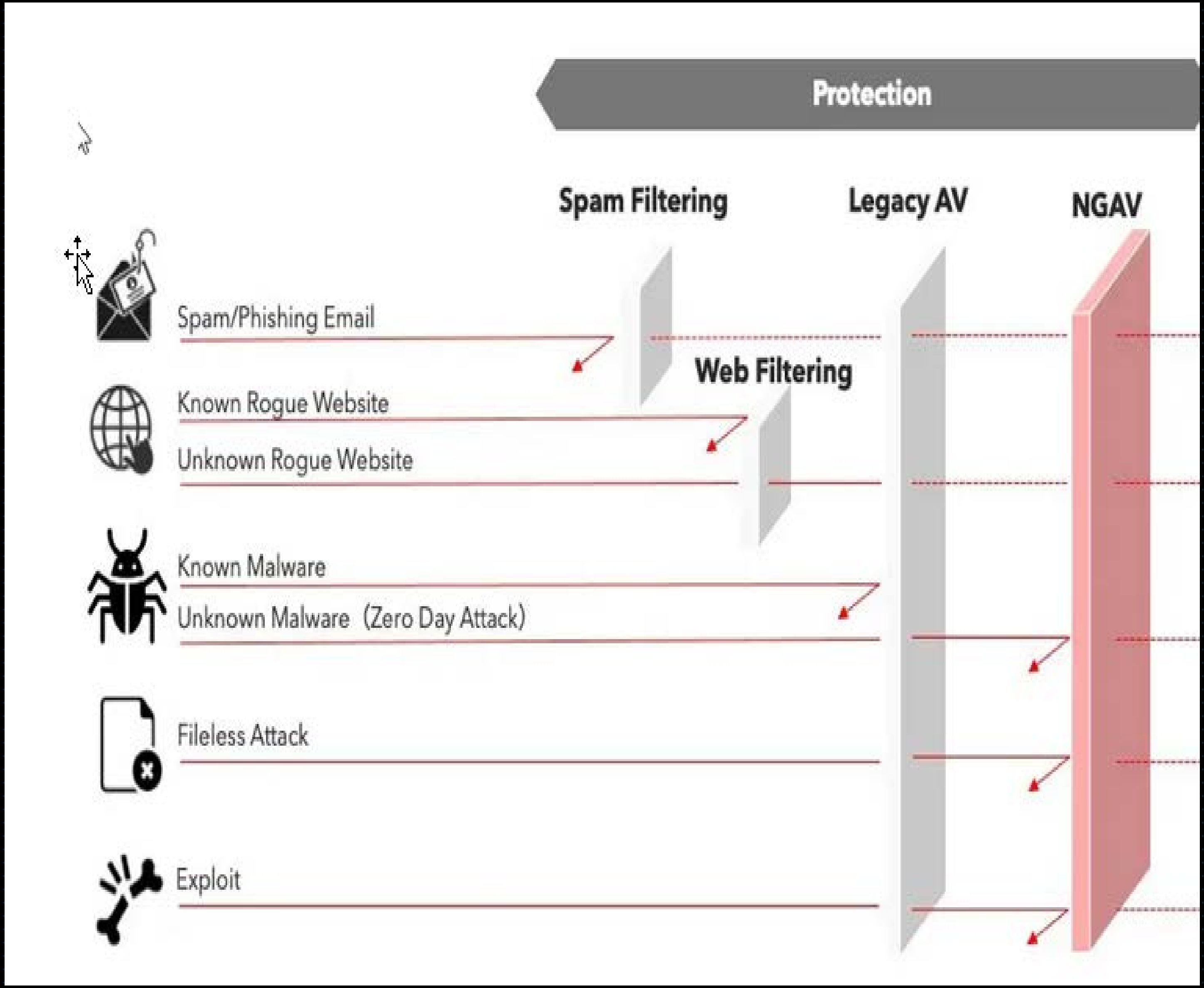


DATA LOSS PREVENTION SOLUTIONS:

DLP Providers For K-12 Schools

Managed Methods

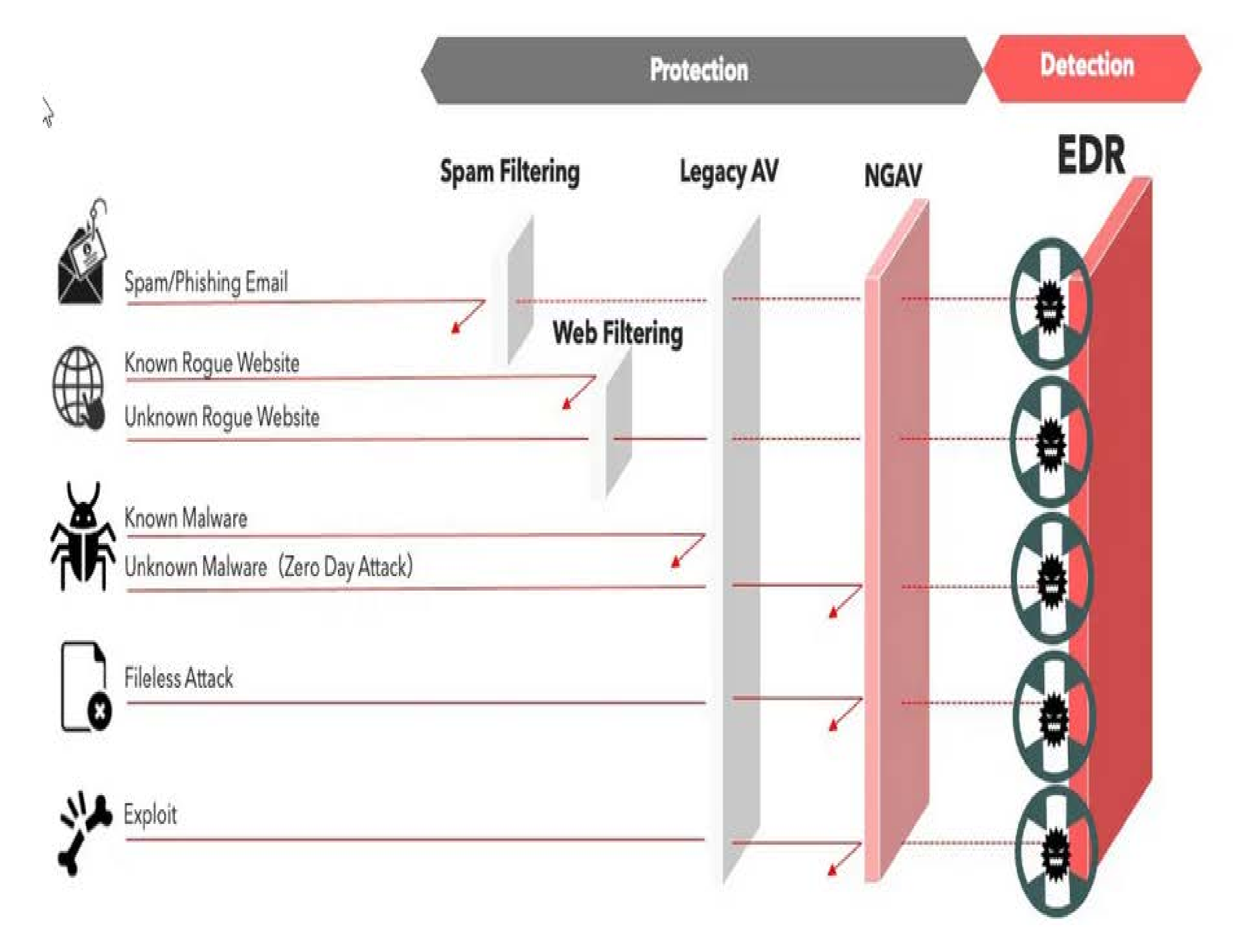
Syscloud



2.4 – NEXT GENERATION ANTIVIRUS (NGAV)

NEXT GENERATION ANTIVIRUS SOLUTIONS:

- CrowdStrike
- Microsoft
- SentinelOne



2.5 – ENDPOINT DETECTION AND RESPONSE (EDR)

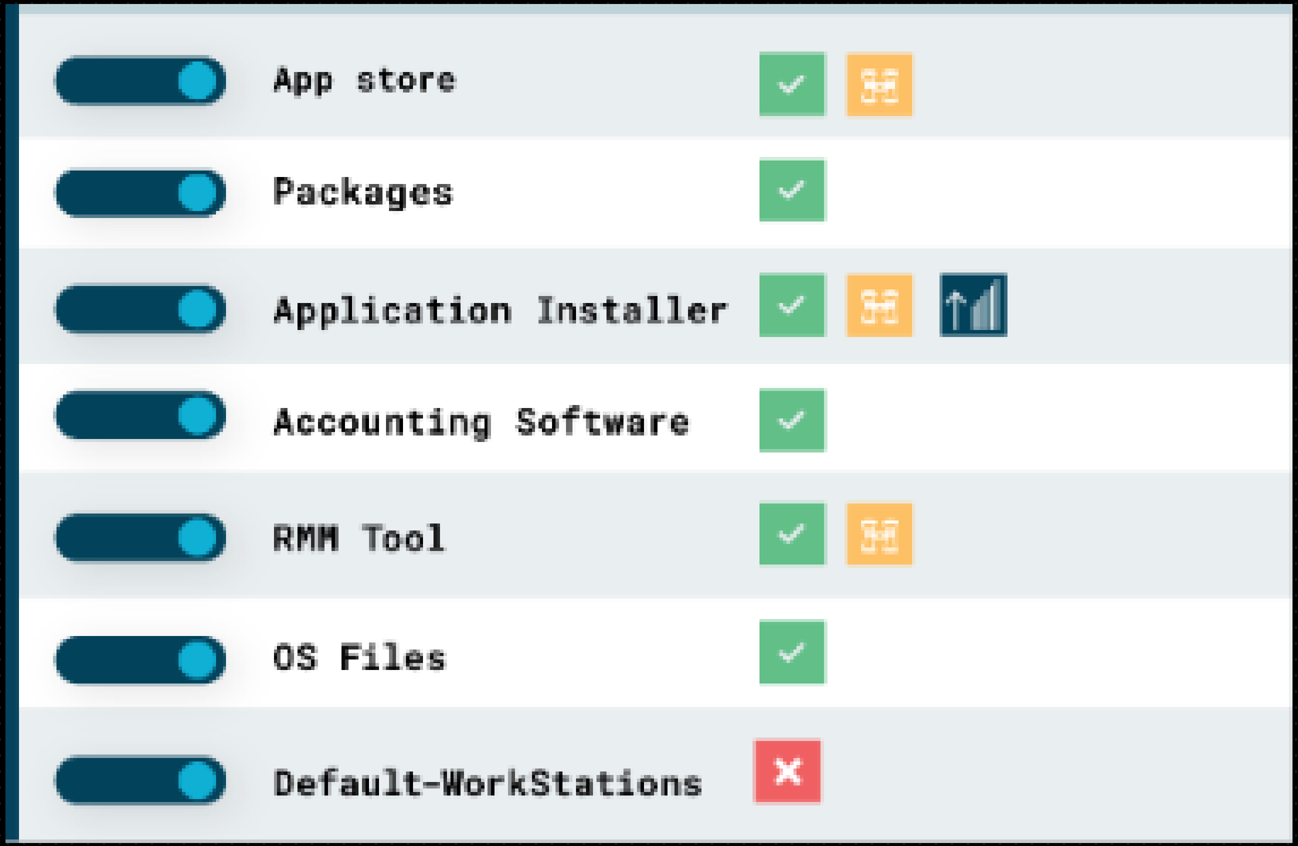
ENDPOINT DETECTION AND RESPONSE SOLUTIONS:

CrowdStrike

Microsoft

SentinelOne

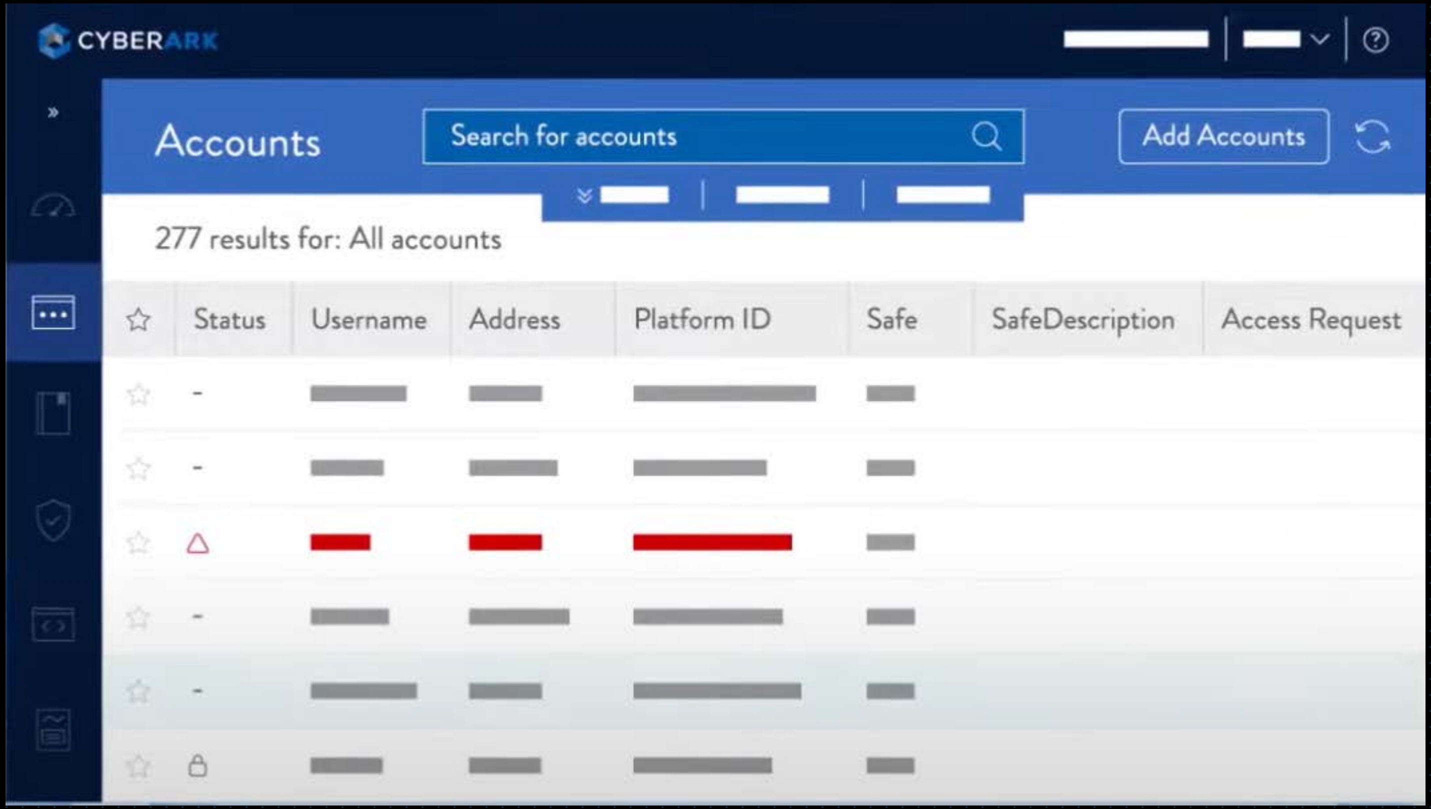
2.6 – APPLICATION ALLOWLISTING



●	App store	✓ ⌘
●	Packages	✓
●	Application Installer	✓ ⌘ 📶
●	Accounting Software	✓
●	RMM Tool	✓ ⌘
●	OS Files	✓
●	Default-WorkStations	✗

APPLICATION ALLOW LISTING SOLUTIONS:

ThreatLocker



277 results for: All accounts

☆	Status	Username	Address	Platform ID	Safe	SafeDescription	Access Request
☆	-	[redacted]	[redacted]	[redacted]	[redacted]		
☆	-	[redacted]	[redacted]	[redacted]	[redacted]		
☆	△	[redacted]	[redacted]	[redacted]	[redacted]		
☆	-	[redacted]	[redacted]	[redacted]	[redacted]		
☆	-	[redacted]	[redacted]	[redacted]	[redacted]		
☆	🔒	[redacted]	[redacted]	[redacted]	[redacted]		

2.7 – PRIVILEGED ACCOUNT MANAGEMENT (PAM)

PRIVILEGED ACCOUNT MANAGEMENT SOLUTIONS:

BeyondTrust

CyberArk

2.8 – HARDENED BASELINE FOR SERVERS, DESKTOPS, LAPTOPS, AND MOBILE DEVICES

CIS Benchmarks

CIS Microsoft Windows Server 2012 (non-
Benchmark

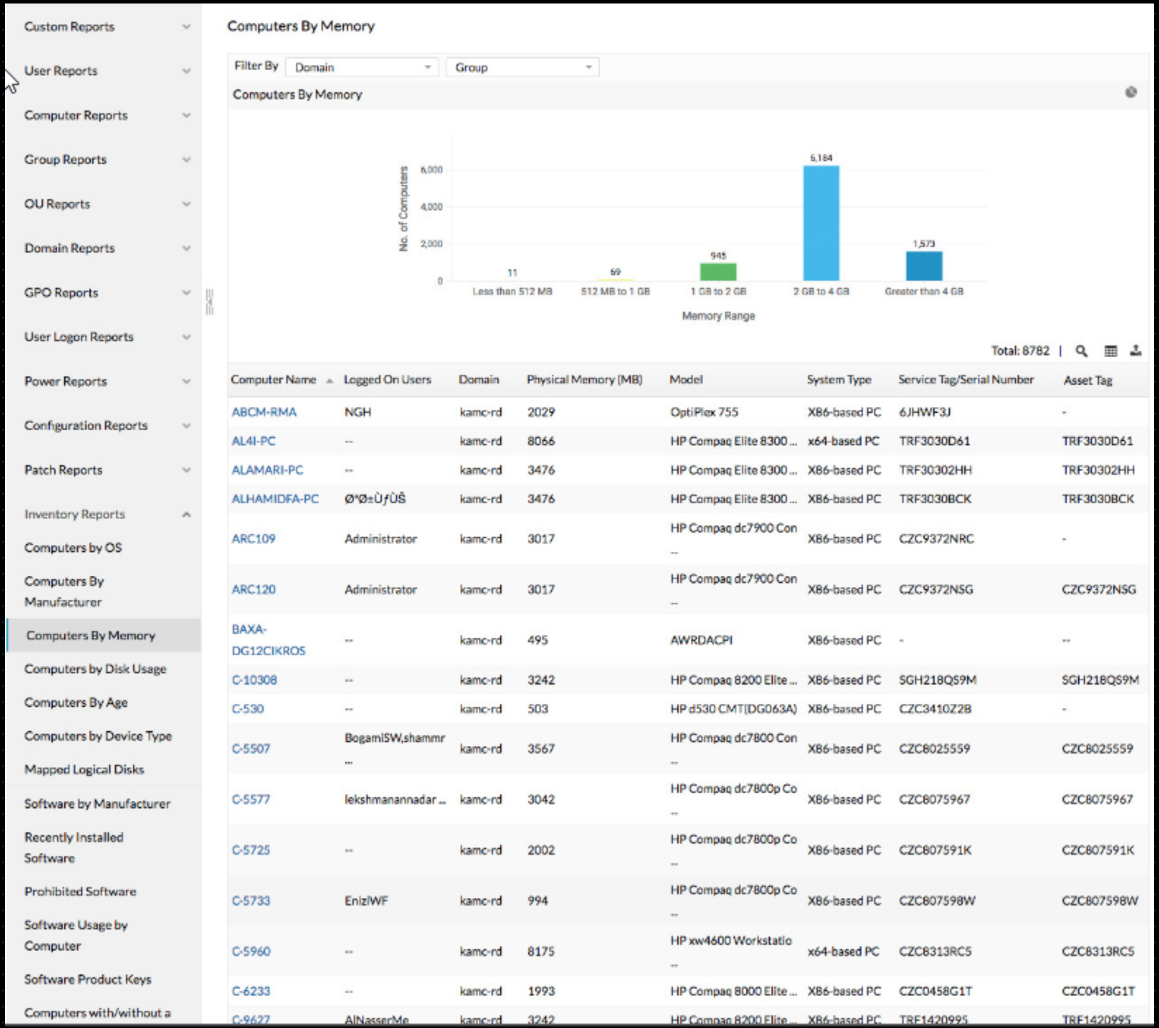
CIS Distribution Independent Linux

v1.1.0 - 12-26-2017

t Enterprise Linux 7 Benchmark

HARDENED BASELINES SOLUTIONS:

[Center for Internet Security]



Computers By Memory

Computers By Memory

Total: 8782

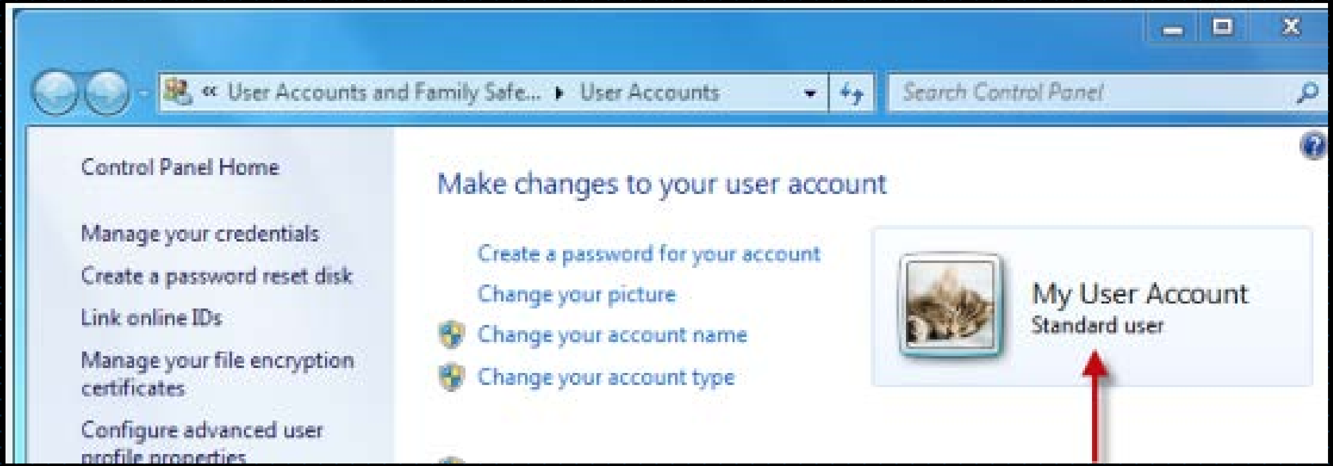
Computer Name	Logged On Users	Domain	Physical Memory (MB)	Model	System Type	Service Tag/Serial Number	Asset Tag
ABCM-RMA	NGH	kamc-rd	2029	OptiPlex 755	X86-based PC	6JHWF3J	-
AL4I-PC	--	kamc-rd	8066	HP Compaq Elite 8300 ...	x64-based PC	TRF3030D61	TRF3030D61
ALAMARI-PC	--	kamc-rd	3476	HP Compaq Elite 8300 ...	X86-based PC	TRF30302HH	TRF30302HH
ALHAMIDFA-PC	Ø'Ø±ÙƒÙŠ	kamc-rd	3476	HP Compaq Elite 8300 ...	X86-based PC	TRF3030BCK	TRF3030BCK
ARC109	Administrator	kamc-rd	3017	HP Compaq dc7900 Con --	X86-based PC	CZC9372NRC	-
ARC120	Administrator	kamc-rd	3017	HP Compaq dc7900 Con --	X86-based PC	CZC9372NSG	CZC9372NSG
BAXA-DG12CIKROS	--	kamc-rd	495	AWRDACPI	X86-based PC	-	--
C-10308	--	kamc-rd	3242	HP Compaq 8200 Elite ...	X86-based PC	SGH218QS9M	SGH218QS9M
C-530	--	kamc-rd	503	HP d530 CMT(DG063A)	X86-based PC	CZC3410Z2B	-
C-5507	BogamiSW,shammr ...	kamc-rd	3567	HP Compaq dc7800 Con --	X86-based PC	CZC8025559	CZC8025559
C-5577	lekshmanannadar ...	kamc-rd	3042	HP Compaq dc7800p Co --	X86-based PC	CZC8075967	CZC8075967
C-5725	--	kamc-rd	2002	HP Compaq dc7800p Co --	X86-based PC	CZC807591K	CZC807591K
C-5733	EnizlWF	kamc-rd	994	HP Compaq dc7800p Co --	X86-based PC	CZC807598W	CZC807598W
C-5960	--	kamc-rd	8175	HP xw4600 Workstatio --	x64-based PC	CZC8313RC5	CZC8313RC5
C-6233	--	kamc-rd	1993	HP Compaq 8000 Elite ...	X86-based PC	CZC0458G1T	CZC0458G1T
C-9627	AlNasserMe	kamc-rd	3242	HP Compaq 8200 Elite ...	X86-based PC	TRF1420995	TRF1420995

2.9 – AUTOMATED HARDWARE AND SOFTWARE INVENTORY

AUTOMATED HARDWARE AND SOFTWARE INVENTORY SOLUTIONS:

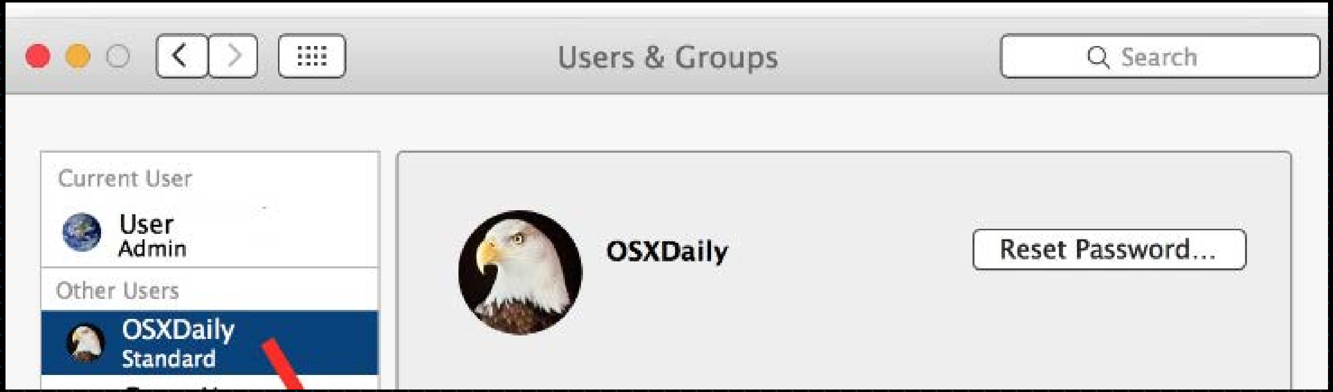
- ManageEngine
- NinjaOne
- Tanium

2.10 – STANDARD USER ACCOUNTS FOR NON-IT USERS


« User Accounts and Family Safe... ▸ User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Create a password reset disk
Link online IDs
Manage your file encryption certificates
Configure advanced user profile properties
Create a password for your account
Change your picture
Change your account name
Change your account type

Make changes to your user account

My User Account
Standard user



Current User
User
Admin

Other Users
OSXDaily
Standard

OSXDaily

SETTING UP COMPUTER USERS AS STANDARD USERS:

Chromebooks

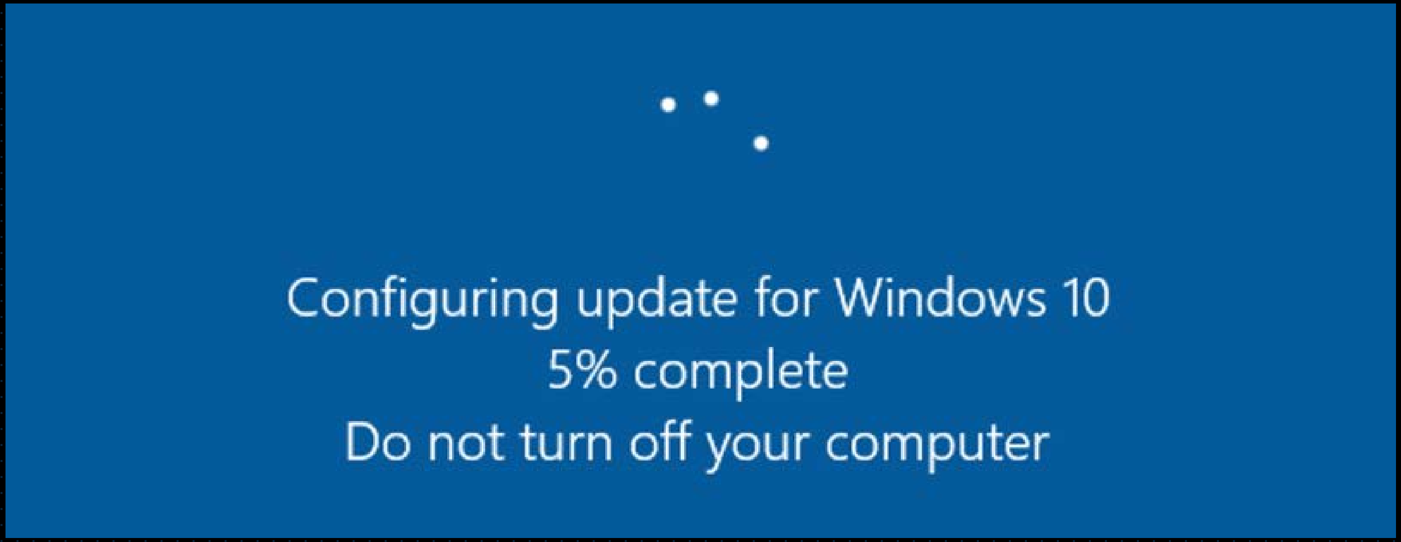
Google Workspace

Macs

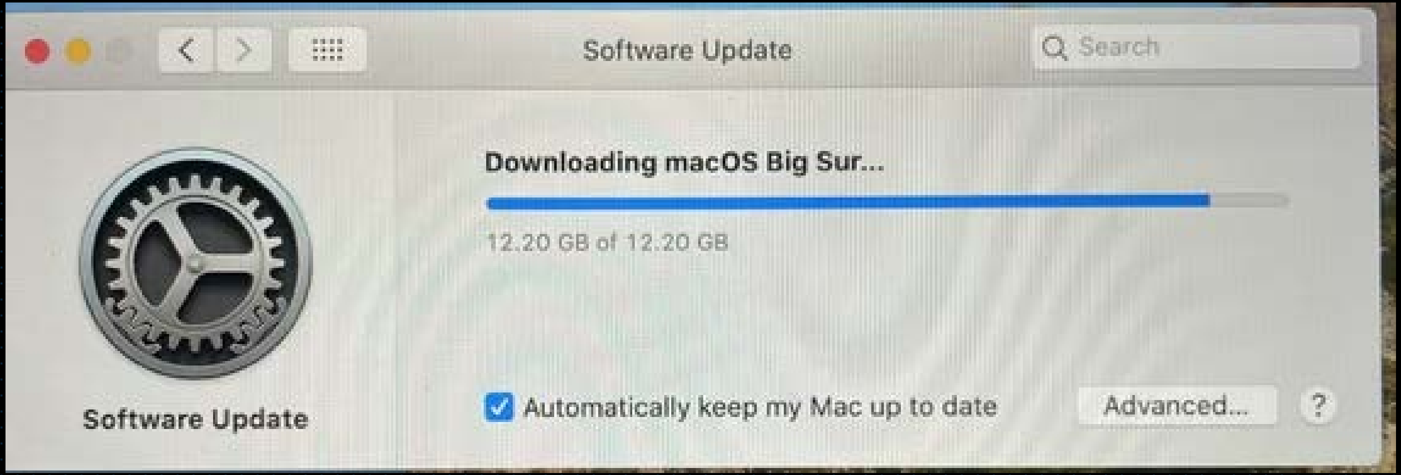
Microsoft 365

Microsoft Windows

2.11 – SECURITY PATCH UPDATES



Configuring update for Windows 10
5% complete
Do not turn off your computer



Downloading macOS Big Sur...

12.20 GB of 12.20 GB

☑ Automatically keep my Mac up to date

SECURITY UPATES SYSTEMS:

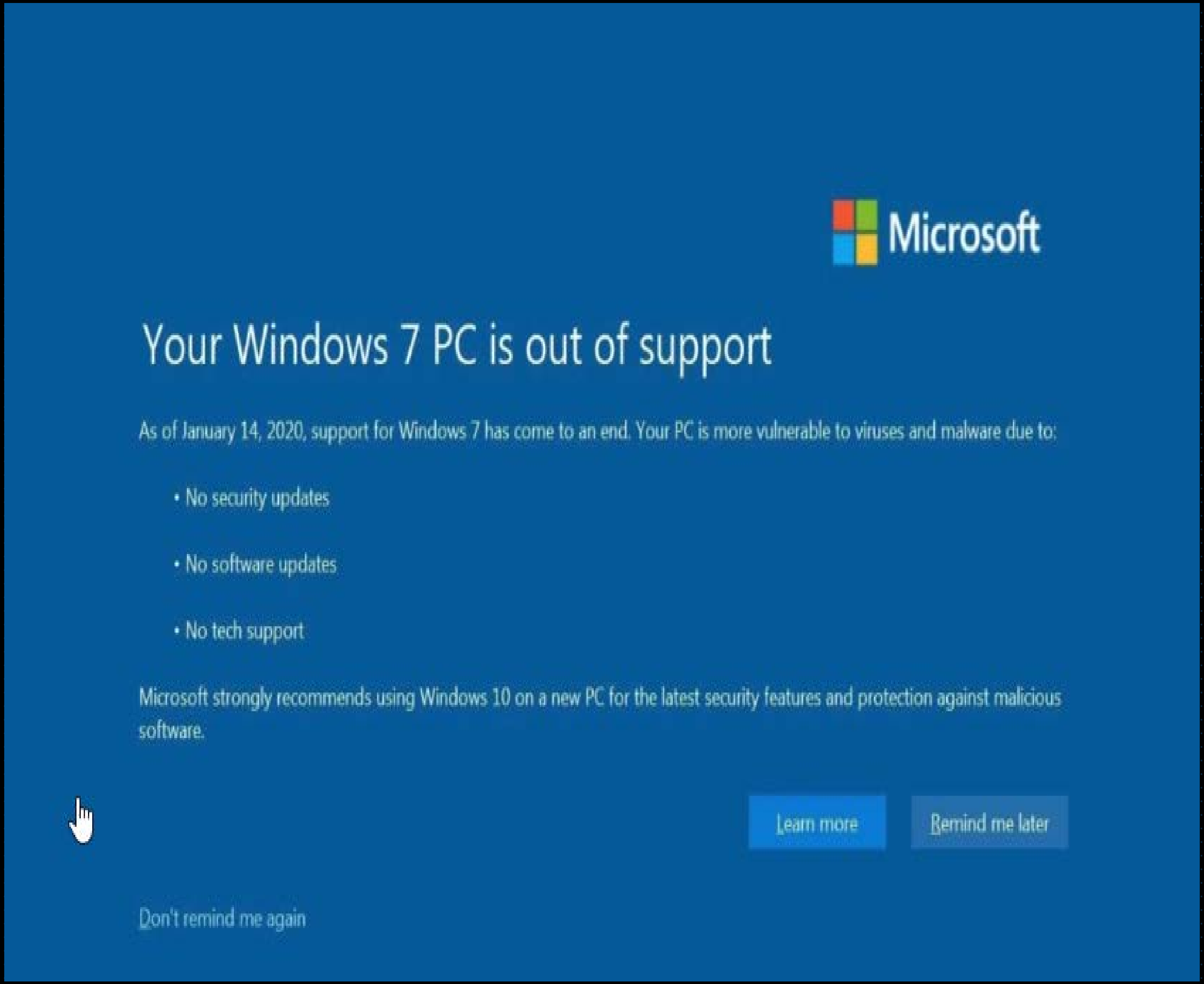
Chromebooks

Google Workspace Mobile Device Management (MDM)

Macs

PCs and mobile devices

2.12 – SEGREGATION OF END OF LIFE OR END OF SUPPORT SOFTWARE



Your Windows 7 PC is out of support

As of January 14, 2020, support for Windows 7 has come to an end. Your PC is more vulnerable to viruses and malware due to:

- No security updates
- No software updates
- No tech support

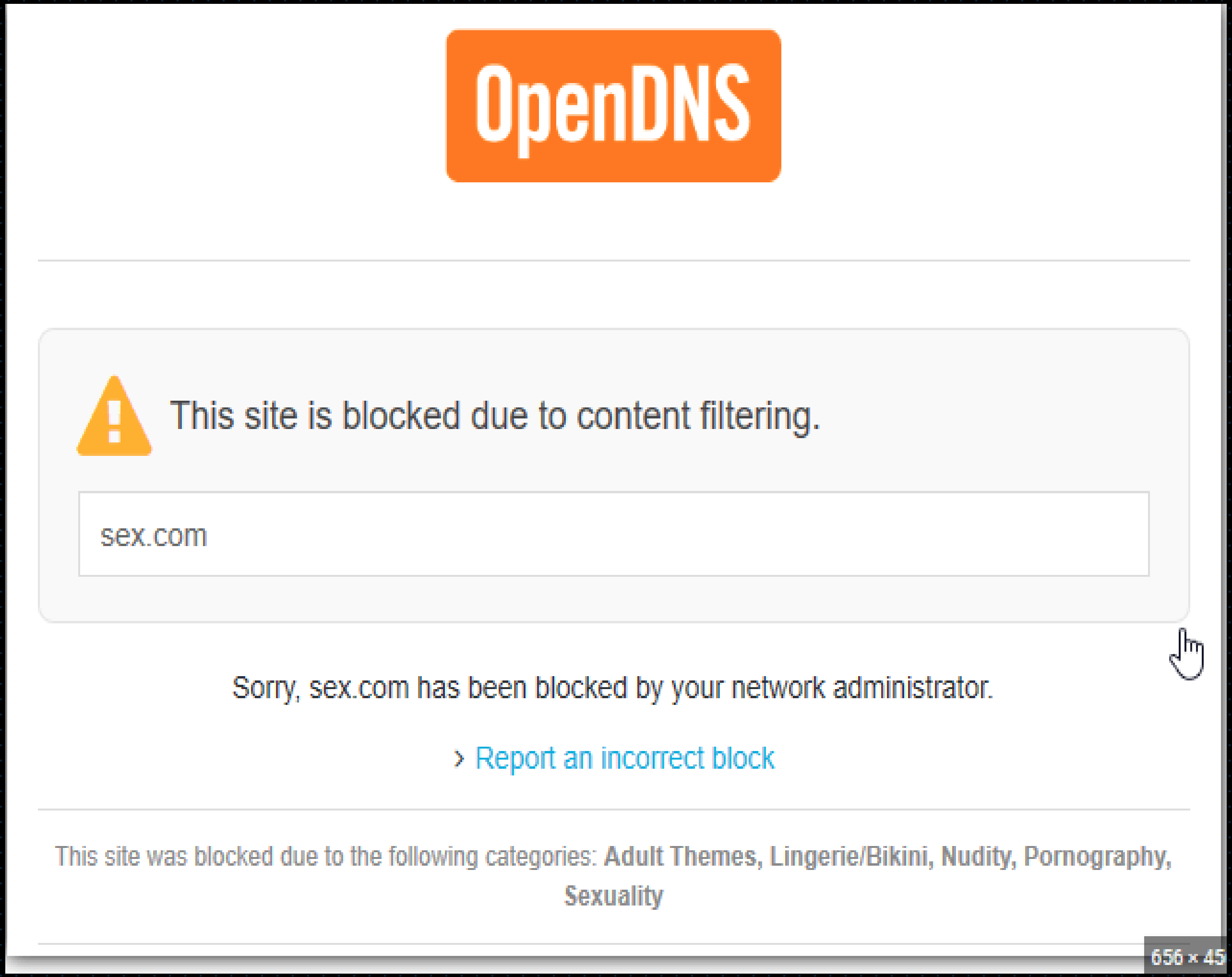
Microsoft strongly recommends using Windows 10 on a new PC for the latest security features and protection against malicious software.

SOLUTIONS FOR SEGREGATING END OF SUPPORT SYSTEMS:

Zero Trust Platforms

- Iboss
- ThreatLocker

2.13 – PROTECTIVE DOMAIN NAME SYSTEM (PDNS)



⚠ This site is blocked due to content filtering.

sex.com

Sorry, sex.com has been blocked by your network administrator.

› Report an incorrect block

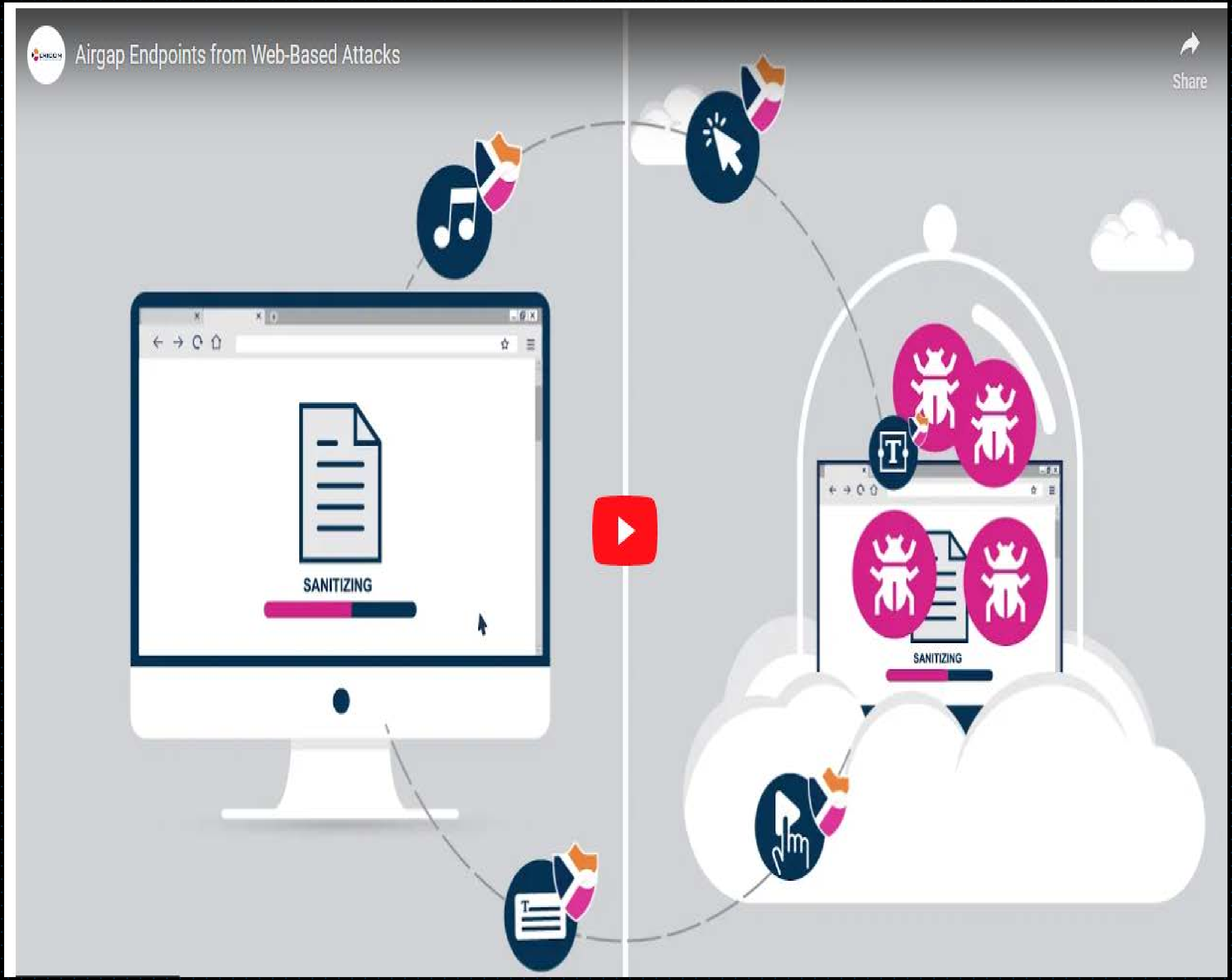
This site was blocked due to the following categories: **Adult Themes, Lingerie/Bikini, Nudity, Pornography, Sexuality**

PROTECTIVE DNS SYSTEMS:

Cisco Umbrella

DNSFilter

TitanHQ Web Security



2.14 – APPLICATION ISOLATION AND CONTAINMENT

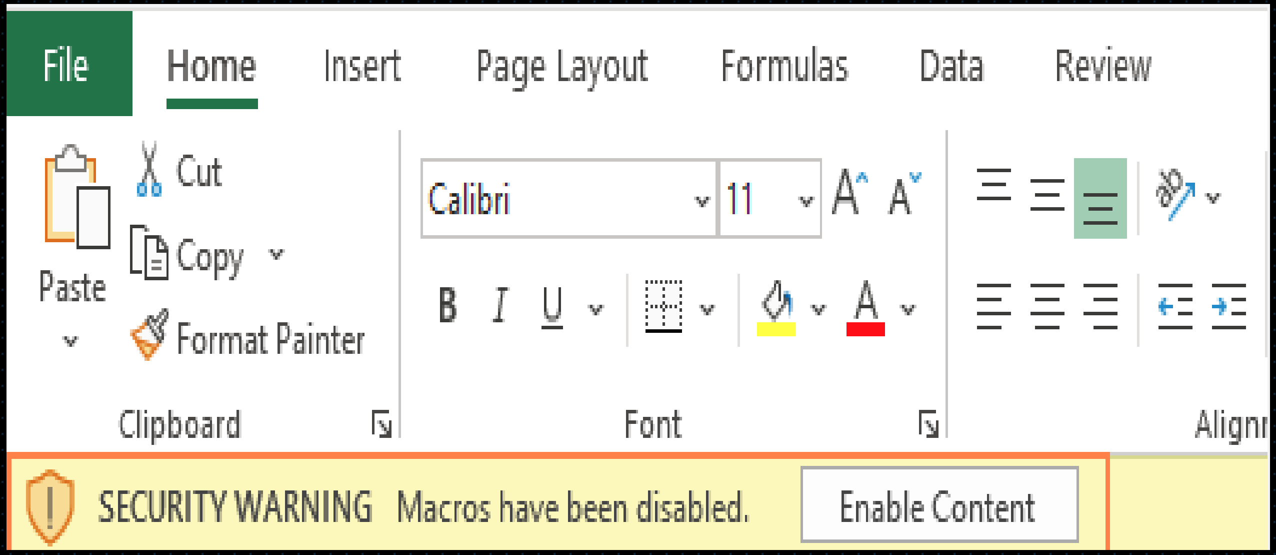
APPLICATION ISOLATION AND CONTAINMENT SOLUTIONS:

Ericom

CylancePROTECT

Menlo Security

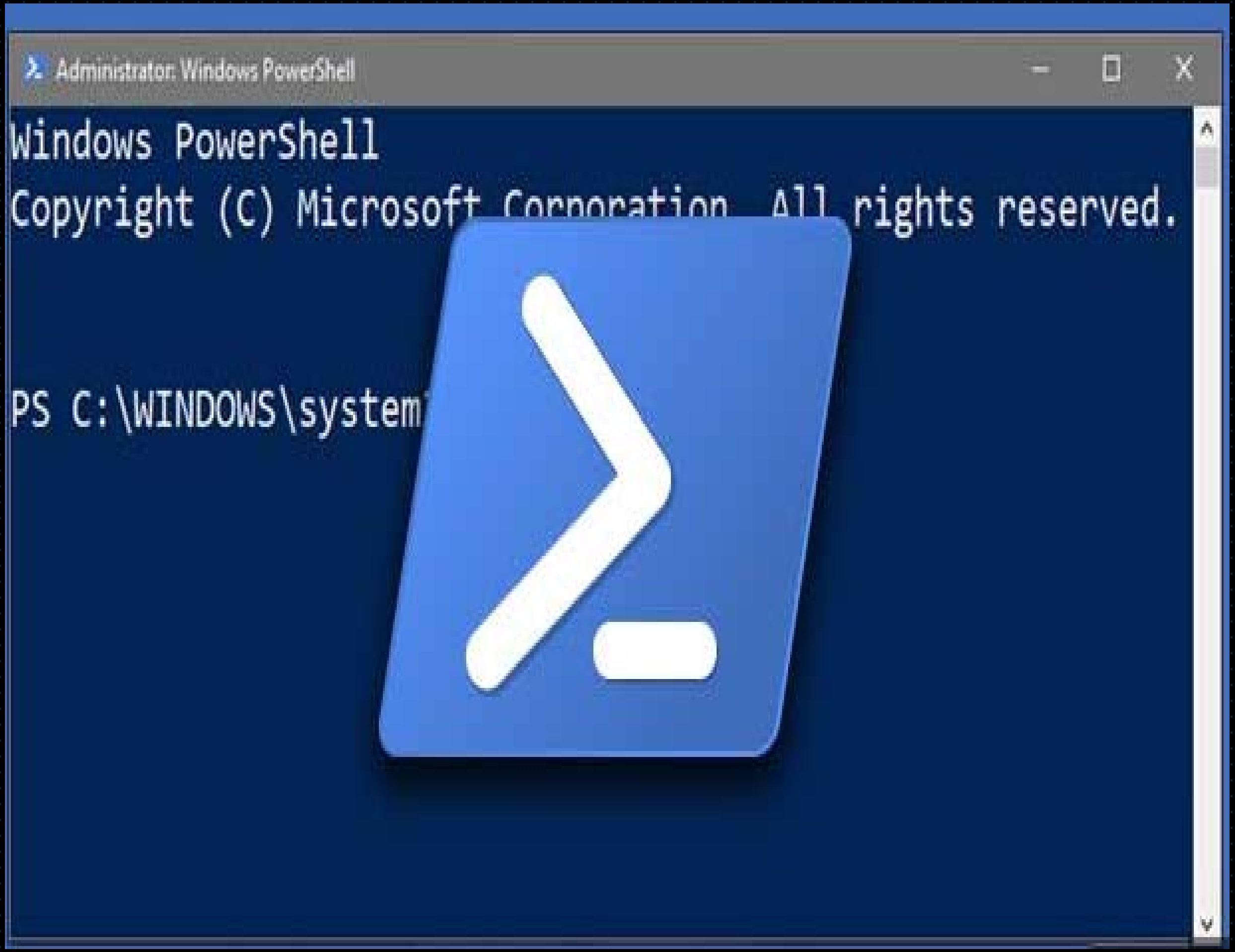
2.15 – DISABLING MICROSOFT OFFICE MACROS



SECURITY WARNING Macros have been disabled.

DISABLING MICROSOFT OFFICE MACROS:

How to disable Microsoft Office macros via group policy



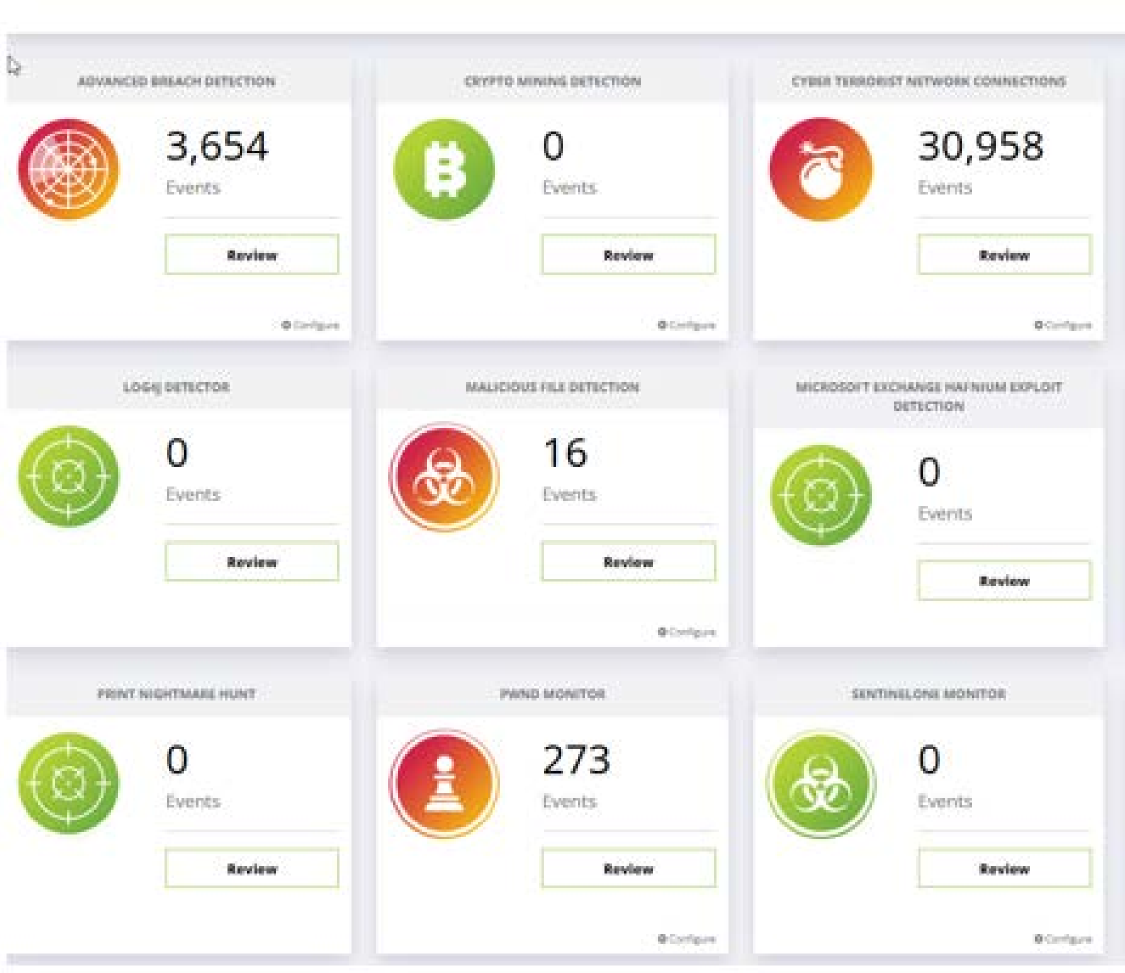
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.


PS C:\WINDOWS\system
```

2.16 – MICROSOFT POWERSHELL BEST PRACTICES

MICROSOFT POWERSHELL ENVIRONMENT RECOMMENDATIONS:

Environment Recommendations

2.17 – SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)



ADVANCED BREACH DETECTION

3,654
Events

CRYPTO MINING DETECTION

0
Events

CYBER TERRORIST NETWORK CONNECTIONS

30,958
Events

LOG4J DETECTOR

0
Events

MALICIOUS FILE DETECTION

16
Events

MICROSOFT EXCHANGE HAFNIUM EXPLOIT DETECTION

0
Events

PRINT NIGHTMARE HUNT

0
Events

PWND MONITOR

273
Events

SENTINELONE MONITOR

0
Events

SIEM PROVIDERS:

Artic Wolf

Binary Defense

Elastic

2.18 – SECURITY OPERATIONS CENTER (SOC)

SOC PROVIDERS:

Multi-State Information Sharing and Analysis Center® (MS-ISAC®)

Artic Wolf

2.19 – THIRD-PARTY PENETRATION TESTING

THIRD-PARTY PENETRATION TEST PROVIDERS:

CrowdStrike

Rapid 7

SecureWorks

WE ARE DONE WITH INTERNAL SECURITY CONTROLS

3. BACKUP AND RECOVERY POLICIES

3

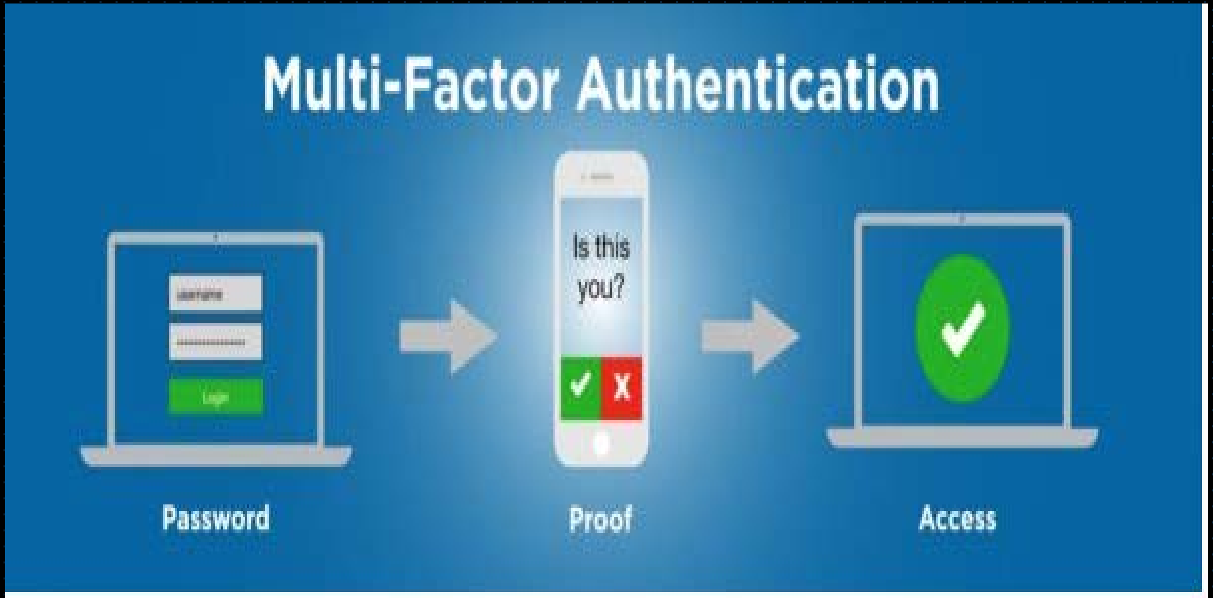
Copies of Data

3.1 – THE 3-2-1 RULE

3 COPIES OF DATA:

1. Live data and on-site backup copy

2. Cloud provider immutable backup copy



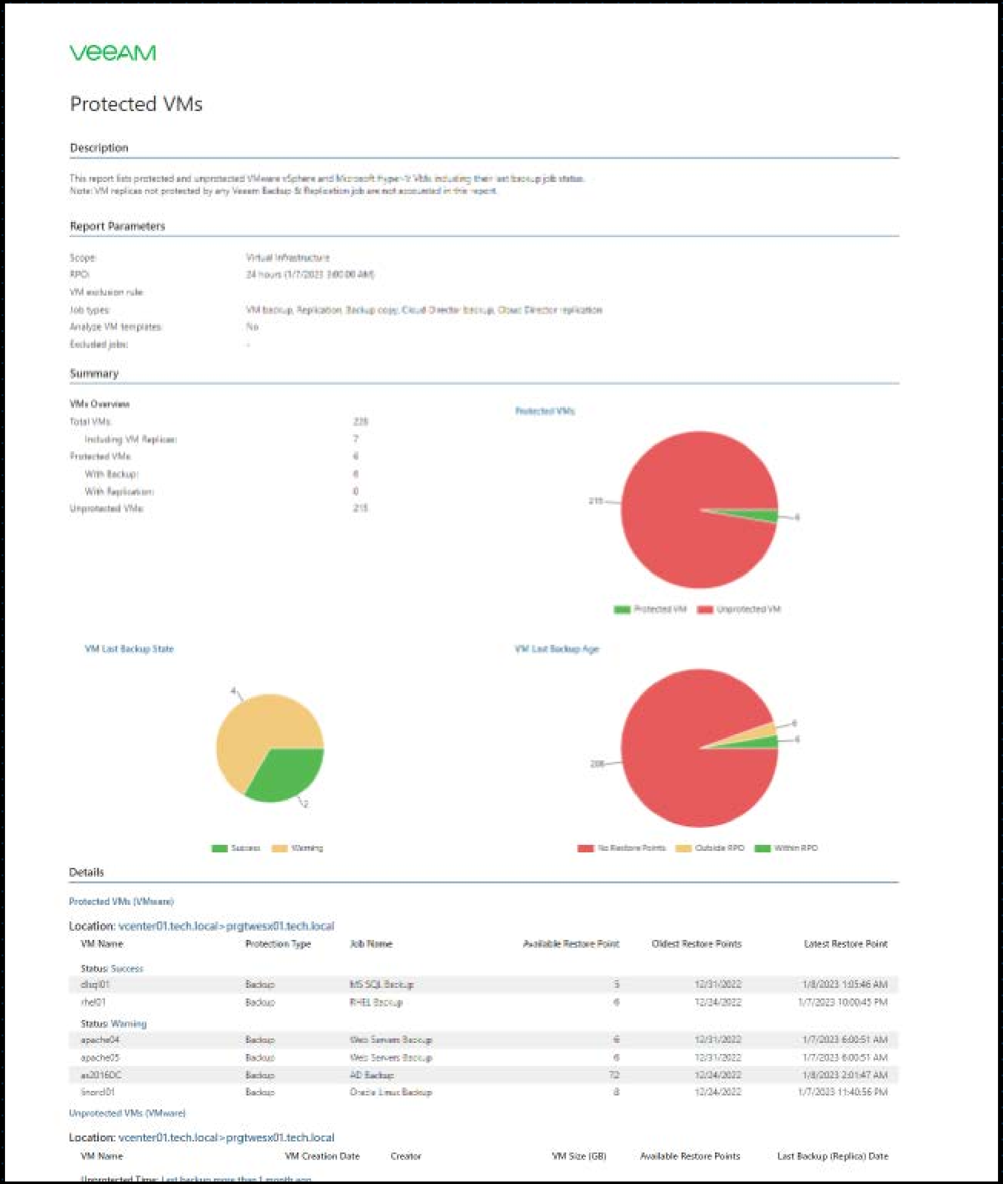
3.2 – MULTIFACTOR AUTHENTICATION (MFA) PROTECTION FOR BACKUPS

MFA FOR BACKUP APPLICATIONS:

MFA Providers

- Duo Security
- JumpCloud
- Okta

3.3 – MONTHLY BACKUP REPORTING AND TESTING



VEEAM

Protected VMs

Description

This report lists protected and unprotected VMware vSphere and Microsoft Hyper-V VMs including their last backup job status.
Note: VM replicas not protected by any Veeam Backup & Replication job are not accounted in the report.

Report Parameters

Scope:	Virtual Infrastructure
RPO:	24 hours (1/7/2023 3:00:00 AM)
VM exclusion rule:	
Job types:	VM backup, Replication, Backup copy, Cloud Director backup, Cloud Director replication
Analyze VM templates:	No
Excluded jobs:	-

Summary

VMs Overview

Total VMs:	220
Including VM Replicas:	7
Protected VMs:	6
With Backup:	6
With Replication:	0
Unprotected VMs:	215

Details

Protected VMs (VMware)

Location: vcenter01.tech.local>prgtwesx01.tech.local

VM Name	Protection Type	Job Name	Available Restore Point	Oldest Restore Points	Latest Restore Point
Status: Success					
dbsql01	Backup	MS SQL Backup	5	12/31/2022	1/8/2023 1:05:46 AM
rhel01	Backup	RHEL Backup	6	12/24/2022	1/7/2023 10:00:45 PM
Status: Warning					
apache04	Backup	Web Servers Backup	6	12/31/2022	1/7/2023 6:00:51 AM
apache05	Backup	Web Servers Backup	6	12/31/2022	1/7/2023 6:00:51 AM
ad2016DC	Backup	AD Backup	72	12/24/2022	1/8/2023 2:01:47 AM
linorcl01	Backup	Oracle Linux Backup	8	12/24/2022	1/7/2023 11:40:56 PM

Unprotected VMs (VMware)

Location: vcenter01.tech.local>prgtwesx01.tech.local

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: Last backup more than 1 month ago					

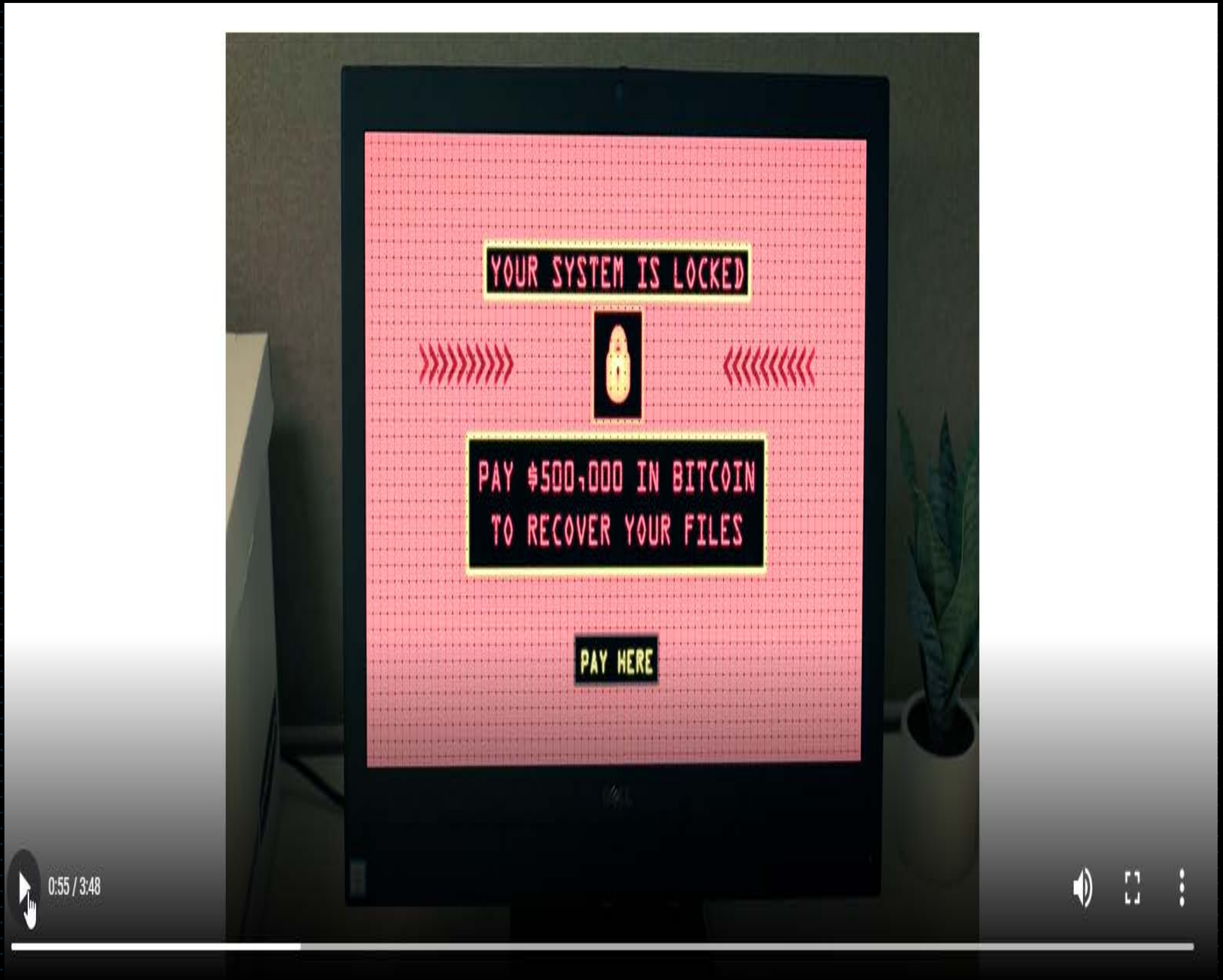
BACKUP PROVIDERS WITH AUTOMATIC TESTING AND REPORTING:

Datto

Veeam

THAT IS IT FOR BACKUP POLICIES

4. PHISHING CONTROLS



4.1 – CYBERSECURITY TRAINING

CYBERSECURITY TRAINING PROVIDERS:

CISA Online Training Toolkit

Consortium for School Network (CoSN)

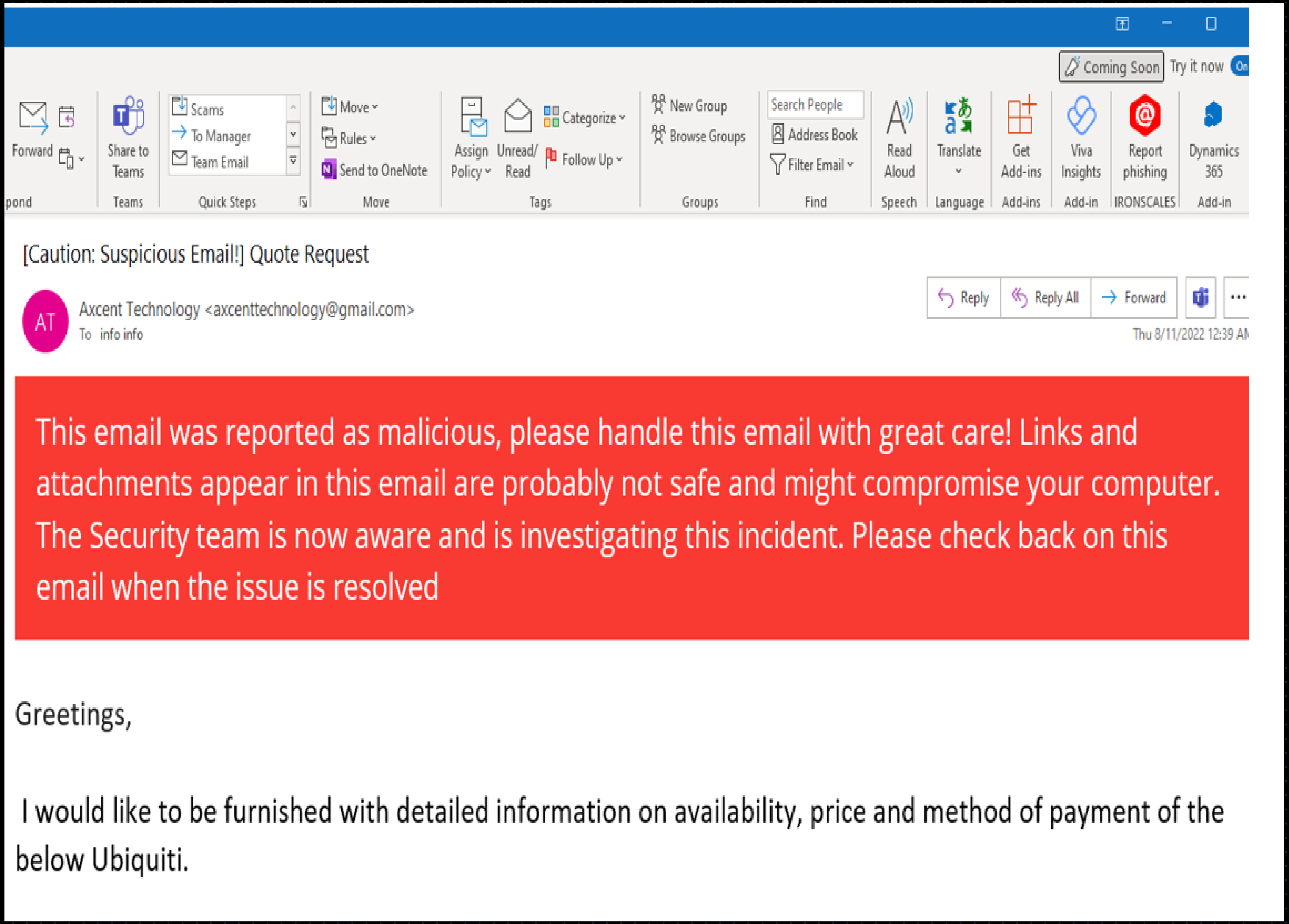
Fortinet

4.2 – WIRE TRANSFER OR ELECTRONIC PAYMENT PROTOCOL

SAMPLE WIRE TRANSFER PROTOCOL:

Establishing a Wire Transfer Protocol to Avoid Fraud

4.3 – ANTI-PHISING PLATFORM



[Caution: Suspicious Email!] Quote Request

Axcent Technology <axcenttechnology@gmail.com>
To info info

Thu 8/11/2022 12:39 AM

This email was reported as malicious, please handle this email with great care! Links and attachments appear in this email are probably not safe and might compromise your computer. The Security team is now aware and is investigating this incident. Please check back on this email when the issue is resolved

Greetings,

I would like to be furnished with detailed information on availability, price and method of payment of the below Ubiquiti.

ANTI-PHISHING PLATFORM PROVIDERS:

Avanan

IronScales

Managed Methods

WE ARE DONE WITH PHISHING CONTROLS

QUESTIONS?

ONE MORE THING