Ransomware Resilience:
5 Steps to Cloud Security Success

April 2022

Microsoft Partner

Microsoft

Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

Eric Krusi

Sr. Solutions Engineer

AvePoint

Seattle, Washington

Profile Summary

- Joined AvePoint in 2017
- Specializes in data protection for M365 and Salesforce
- 15 years in the Microsoft information management and collaboration space

John Hodges

SVP, Product Strategy

AvePoint

Hilo, Hawai'i

Profile Summary

- Joined AvePoint in 2008
- 15 Years Data Protection experience
- Lead transition from hardware-based backups to cloud-to-cloud services
- Focus areas include Azure, Salesforce, Dynamics, Office 365, Google

We Are AvePoint

Leader in Microsoft 365 data management solutions

AvePoint® is headquartered in Jersey City, NJ, with approximately 1,800 employees across 29 offices, 88 countries, and seven continents.

25% Fortune 500

9M Cloud Users

88 Countries

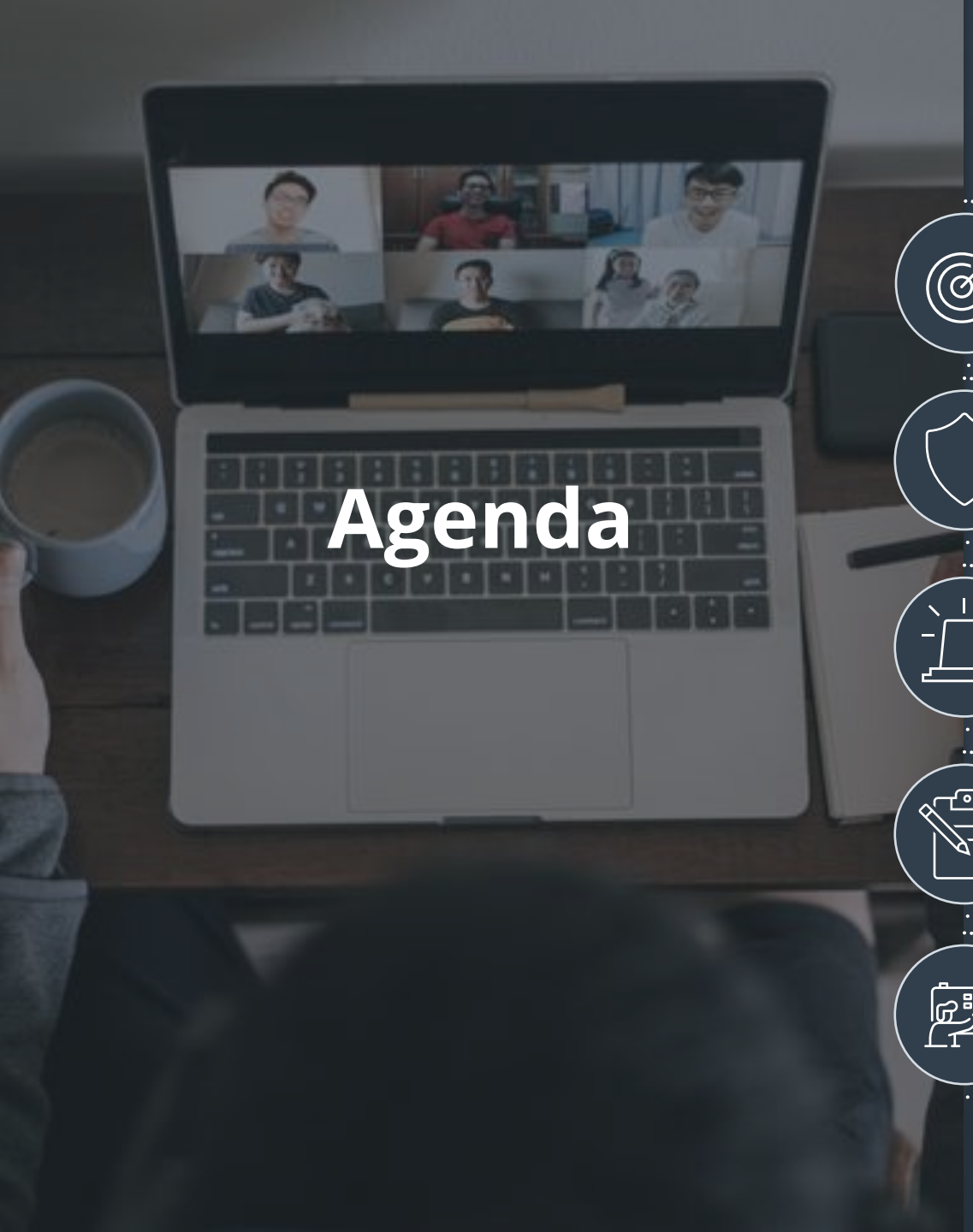
7 Continents

Microsoft Partner

Microsoft

5x Partner of the Year Award Winner

AVPT Nasdaq Listed



Agenda

- Understanding Types of Attacks
- Best Practices for Prevention
- Early Detection Tips
- Response Checklist
- Recovery Solutions

The Challenge

“Ransomware attacks have become one of the top security threats for organizations, especially as increased digital collaboration opens up more vulnerabilities,” said Dr. Tianyi Jiang (TJ), CEO and Co-Founder, AvePoint. “**In 2021 alone, ransomware attacks hit companies every 11 seconds, and the average cost to recover is in the millions of dollars**. With the launch of Ransomware Detection, AvePoint continues to deliver on our promise of securing digital collaboration for enterprises across the globe.”

https://www.cloudwards.net/ransomware-statistics/

The Challenge

Increased digital collaboration opens up more vulnerabilities

37% of all businesses hit with ransomware

75% attacks were on companies making less than **$50 million in revenue**

Every **11 seconds** a company is hit with ransomware attacks

57% of businesses hit recovered their data using cloud backup

Source: cloudwards.net

1

Review types of attacks and low-hanging targets

“Ransomware attacks have become one of the top security threats for organizations, especially as increased digital collaboration opens up more vulnerabilities” ~ Dr. Tianyi Jiang

Understanding Ransomware

The primary goal is to separate you from your data.

#1: Ransomware must remove access to as many files as possible to increase chance of pay-out.

Anomaly Detection: Slow play outs where file names are changed or copied over. Needs machine-learning algorithms to study standard patterns to identify suspicious behavior (new files, changes, deletions)
Example: Copy > Encrypt > Delete results in unusually high change rates

#2: The most common way to lock someone out of their file is to encrypt it.

Encryption Detection: Locking files through encryption files will automatically increase the “entropy” (randomness) of a file. Requires a baseline of heuristics for each file.
Example: An attempt to encrypt many files generates a suspicious event

2 Review best practices and available solutions for ransomware prevention

"Proper security should enable collaboration, not restrict it." ~ Dr. Tianyi Jiang

Best Practices for Ransomware Protection

Baselines

- Secure Score
- Attack surface reduction rules
- Email settings

Detection & Response

- M365 Defender
- Microsoft Defender for Office 365 (Phishing Protection)
- Microsoft Defender for Identity
- Microsoft Defender (Endpoint)

Identities

- Sign-In Security
- Secure Privileged Accounts

Devices

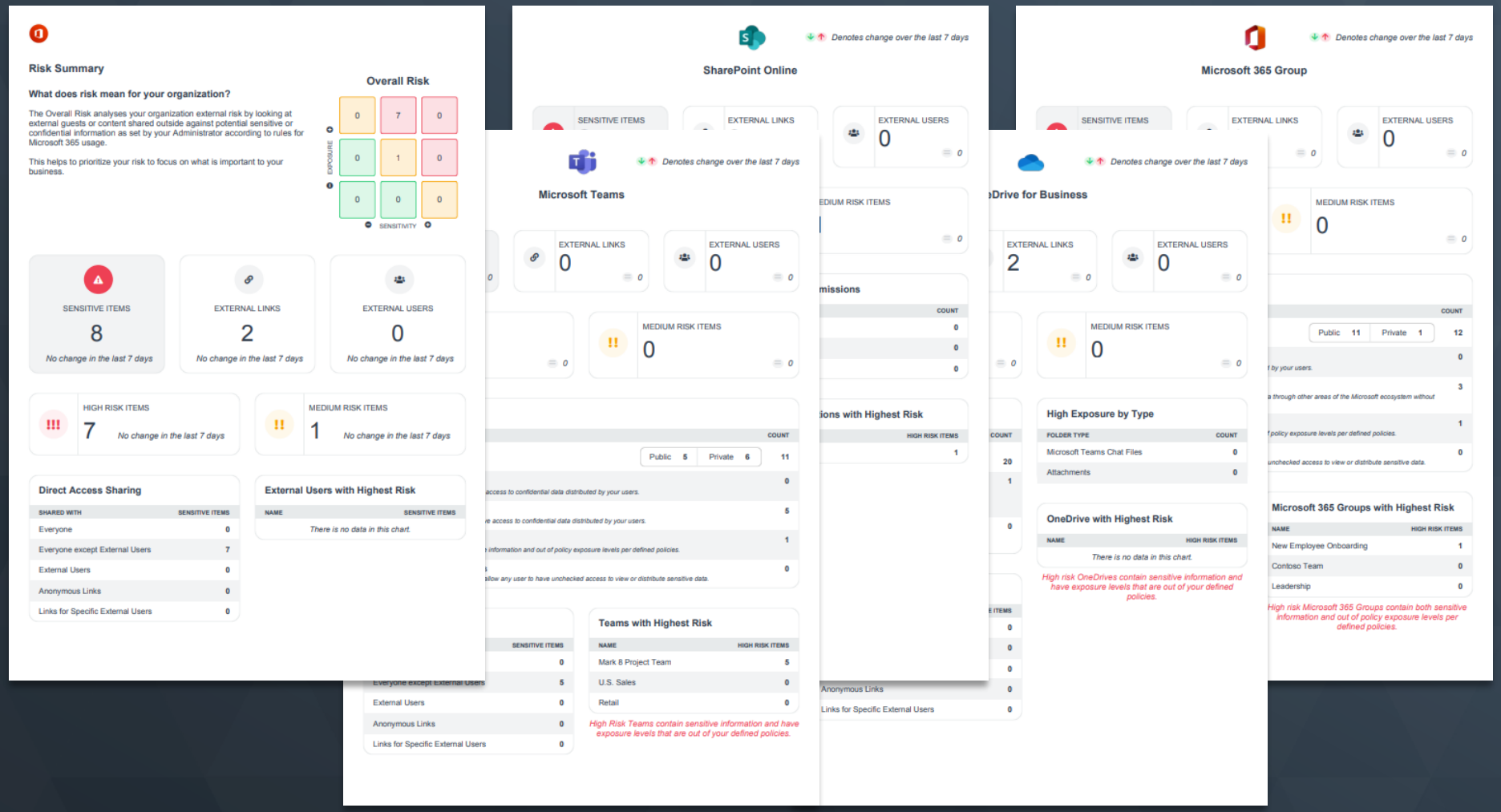
- Firewall & Antivirus

Information

- Identify Sensitive Data
- Restrict Overexposure of Permissions

Deploy ransomware protection for your Microsoft 365 tenant | Microsoft Docs

Executive Reports: Targeting Low-Hanging Fruit



Presenting Risk

Concise and Actionable documentation allowing organizations to conduct remediation independently.

3

Discuss available solutions for early detection of threats and attacks

"With the right education and training, and by setting up automated processes and data rules, businesses are better armed against threats to security." ~ Dr. Tianyi Jiang

Secure score
Learning hub
Trials
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps
App governance
Reports
Audit
Health
Permissions & roles
Settings

Threat policies

Templated policies

Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
Configuration analyzer	Identify issues in your current policy configuration to improve your security

Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Rules

Tenant Allow/Block Lists	Manage allow or block entries for your organization.
DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came fro
Advanced delivery	Manage overrides for special system use cases.
Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to

Home
Incidents & alerts
Email & collaboration alerts
Actions & submissions
Submissions
Secure score
Trials
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Reports
Audit
Health

Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

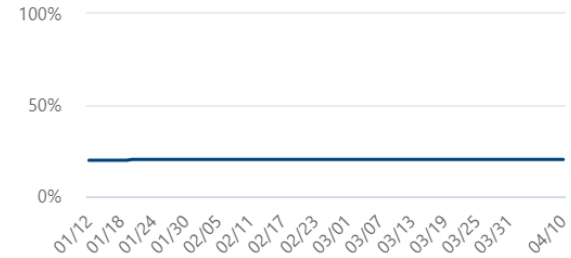
Filter

Your secure score

Include

Secure Score: 20.24%

23.68/117 points achieved



Breakdown points by: Category

Identity	**19.07%**
Apps	**21.31%**

Points achieved Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
1	18	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Require MFA for administrative roles	+8.55%	To address	Identity
Create Safe Links policies for email messages	+7.69%	To address	Apps
Ensure all users can complete multi-factor authentication for s...	+7.69%	To address	Identity
Enable policy to block legacy authentication	+6.84%	To address	Identity
Turn on Safe Attachments in block mode	+6.84%	To address	Apps
Turn on sign-in risk policy	+5.98%	To address	Identity
Turn on user risk policy	+5.98%	To address	Identity
Turn on Microsoft Defender for Office 365 in SharePoint, One...	+4.27%	To address	Apps

View all

Home
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps

Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

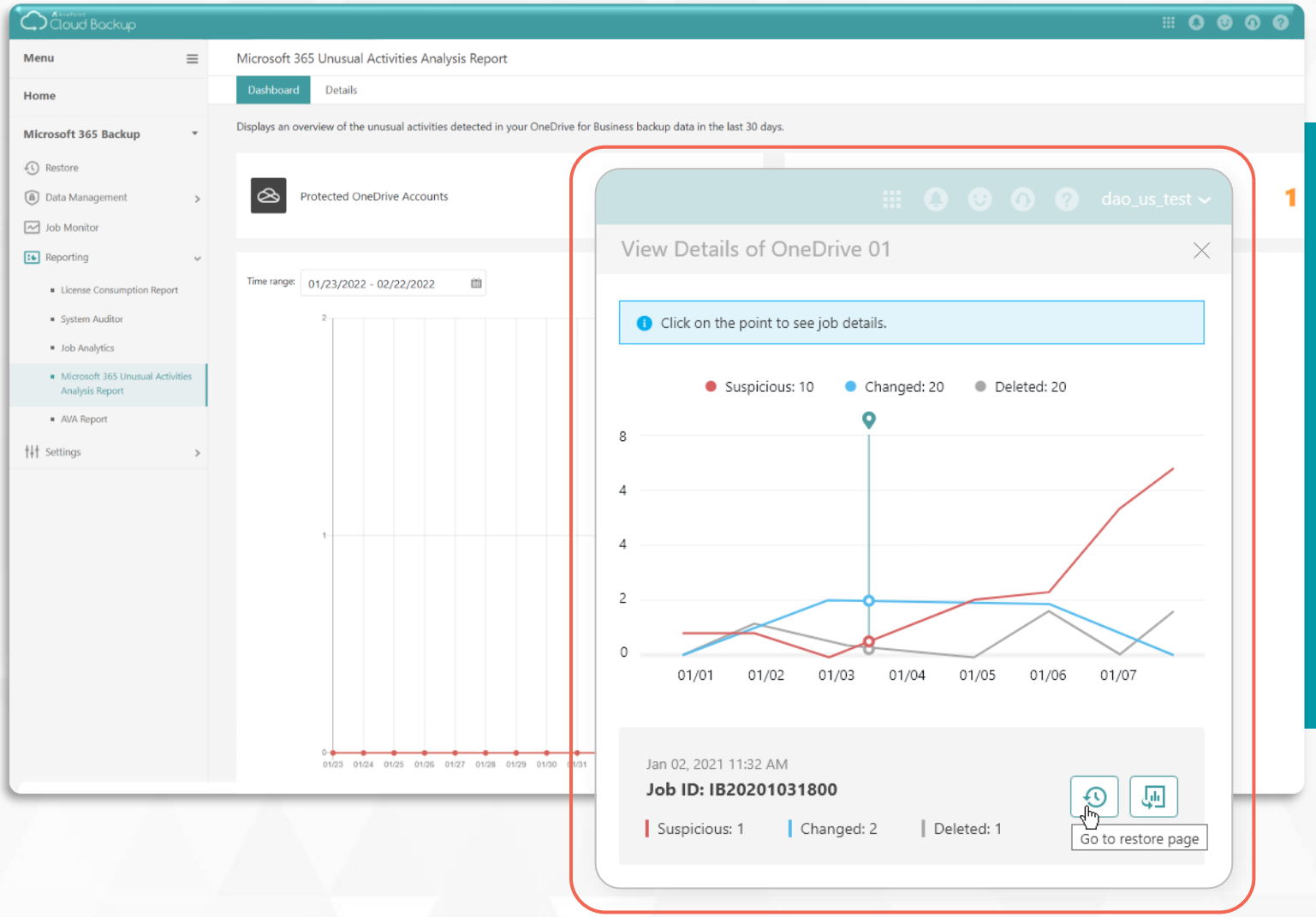
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:

Export 26 items Search Filter Group by

Rank	Improvement action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
1	Require MFA for administrative roles	+8.55%	0/10	To address	No	Yes	Identity	Azure Active Direct
2	Ensure all users can complete multi-factor authentication for ...	+7.69%	0/9	To address	No	Yes	Identity	Azure Active Direct
3	Create Safe Links policies for email messages	+7.69%	0/9	To address	No	Yes	Apps	Defender for Office
4	Enable policy to block legacy authentication	+6.84%	0/8	To address	No	Yes	Identity	Azure Active Direct
5	Turn on Safe Attachments in block mode	+6.84%	0/8	To address	No	Yes	Apps	Defender for Office
6	Turn on user risk policy	+5.98%	0/7	To address	No	Yes	Identity	Azure Active Direct
7	Turn on sign-in risk policy	+5.98%	0/7	To address	No	Yes	Identity	Azure Active Direct
8	Do not allow Exchange Online calendar details to be shared ...	+4.27%	0/5	To address	No	Yes	Apps	Exchange Online
9	Turn on the common attachments filter setting for anti-malw...	+4.27%	0/5	To address	No	Yes	Apps	Defender for Office
10	Do not allow users to grant consent to unmanaged applicatio...	+3.42%	0/4	To address	No	Yes	Identity	Azure Active Direct
11	Create an app discovery policy to identify new and trending c...	+2.56%	0/3	To address	No	Yes	Apps	Microsoft Defende

Ransomware Detection



Proactively detect ransomware events

- Early event detection
- Quick investigation
- Faster restore with AvePoint Cloud Backup

4

Deliver a checklist for response and recovery

for WHEN you or your customers encounter your next bad actor

"Considering the number of ransomware attacks nearly doubled last year, having a proactive solution in place is critical for businesses across the globe." ~ Dr. Tianyi Jiang

Hoping for the best… planning for the worst!

CISA – US Government's Recommendations

Identify & Isolate:

- Determine which system affected and disconnect them from your network
- Begin communication plans with managers, authorities quickly

Investigate & Record:

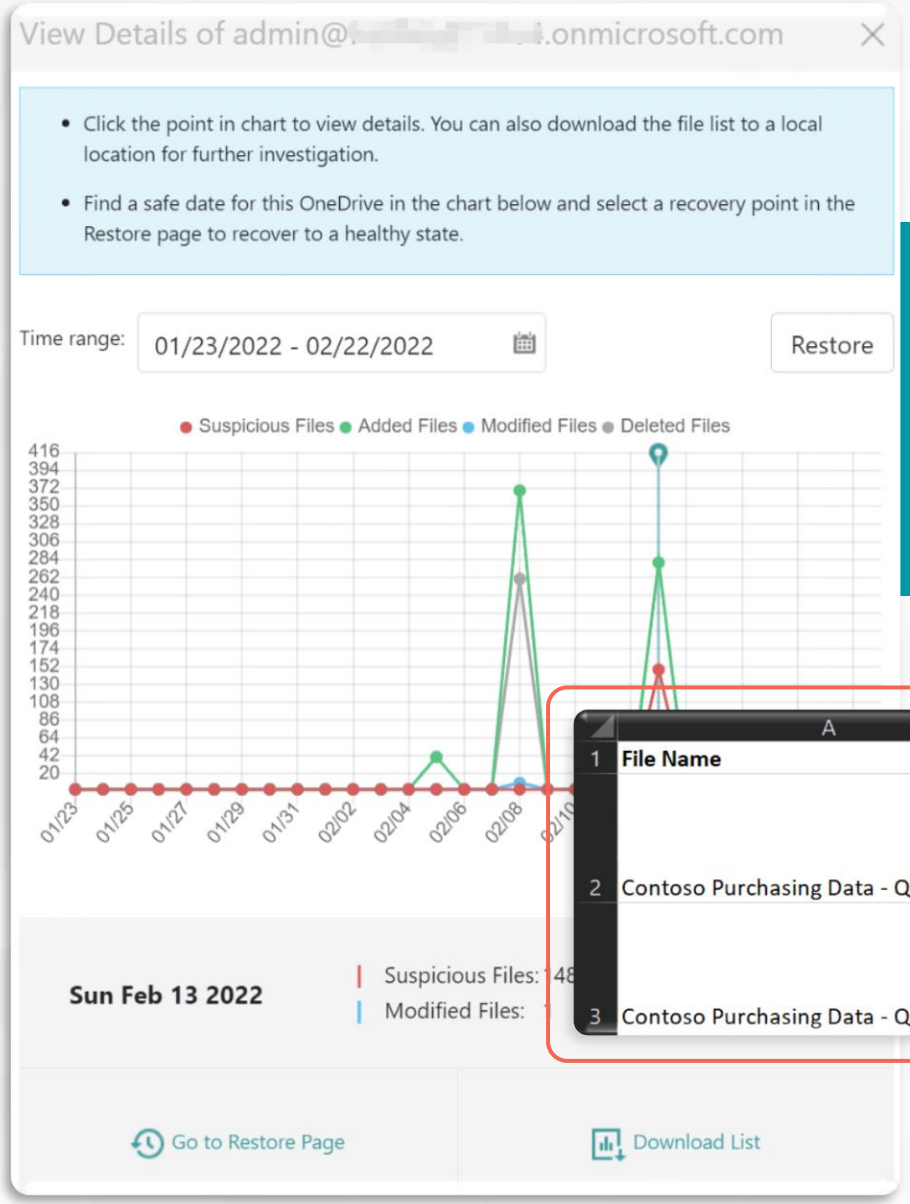
- Work to identify criticality of the systems affected
- Preserve backups, logs, and images of the affected systems to present to security

Recovery of Systems:

- Prioritize business-critical assets first
- Identify gaps in security that lead to infiltration (check that secure score!)
- Restore systems from last known "clean" state

Quick Investigation

- Detailed zoom-in on key activities
- Suspicious Files (suspected encryption)
- Events Detection (add / delete / modify)
- Evidence-based reports for investigation



	A	B	C	D
1	File Name	Location	File Status	Unusual Activity Detected Time
2	Contoso Purchasing Data - Q1.xlsx	https://m365x[redacted]-my.sharepoint.com/personal/admin_m365[redacted]_onmicrosoft_com/Documents/Contoso Purchasing Data - Q1.xlsx	Suspicious, Modified	08/10/2021 9:00 AM (UTC)
3	Contoso Purchasing Data - Q2.xlsx	https://m365x[redacted]-my.sharepoint.com/personal/admin_m365x[redacted]_onmicrosoft_com/Documents/Contoso Purchasing Data - Q2.xlsx	Added	08/10/2021 9:00 AM (UTC)

5 Recommended solutions to aid in response and recovery

“Don’t ask if it’s backed up. Ask if you can restore it.” ~ Dr. Tianyi Jiang

FBI's #1 Best Practice to Minimize Ransomware Risks:

"**Backup** your data, system images, and configurations, test your backups and keep the backups offline…"

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

"The cornerstone of all the best ransomware defense strategies is having a **reliable online backup** […]"

https://www.cloudwards.net/ransomware-statistics/

"Your organization has **backups that work**. You don't need to worry about the ransomware. You restore your data completely and get back to work"

https://cyberreadinessinstitute.org/wp-content/uploads/20-CRI-Ransomware-Playbook.pdf

But… Doesn't Microsoft Have Me Covered?

Malware and ransomware protection in Microsoft 365

Article • 02/14/2022 • 13 minutes to read • 4 contributors

Protecting customer data from malware

Malware consists of viruses, spyware and other malicious software. Microsoft 365 includes protection mechanisms to prevent malware from being introduced into Microsoft 365 by a client or by a Microsoft 365 server. The use of anti-malware software is a principal mechanism for protection of Microsoft 365 assets from malicious software. The anti-malware software detects and prevents computer viruses, malware, rootkits, worms, and other malicious software from being introduced into any service systems. Anti-malware software provides both preventive and detective control over malicious software.

Each anti-malware solution in place tracks the version of the software and what signatures are running. The automatic download and application of signature updates at least daily from the vendor's virus definition site is centrally managed by the appropriate anti-malware tool for each service team. The following functions are centrally managed by the appropriate anti-malware tool on each endpoint for each service team:

- Automatic scans of the environment
- Periodic scans of the file system (at least weekly)
- Real-time scans of files as they're downloaded, opened, or executed
- Automatic download and application of signature updates at least daily from the vendor's

- Microsoft Defender!
- Exchange Online Protection!
- SharePoint and OneDrive versioning:

"Versioning helps to protect SharePoint Online lists and SharePoint Online and OneDrive for Business libraries from some, but not all, of these types of ransomware attacks."

- SharePoint and OneDrive Recycle Bin:

"Versioning doesn't protect against ransomware attacks that copy files, encrypt them, and then delete the original files. However, end-users can leverage the Recycle Bin to recover OneDrive for Business files after a ransomware attack occurs."

https://docs.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

AvePoint Cloud Backup

Get Backup. Period.

Unlimited, automated backup for your Microsoft Cloud assets

Automatic backups, up to 4X per day, for Dynamics 365, Office 365 - SharePoint Online, OneDrive for Business, Exchange Online, Project Online, and Groups. Unlimited options give you flexibility to protect content as your organizational needs dictate.

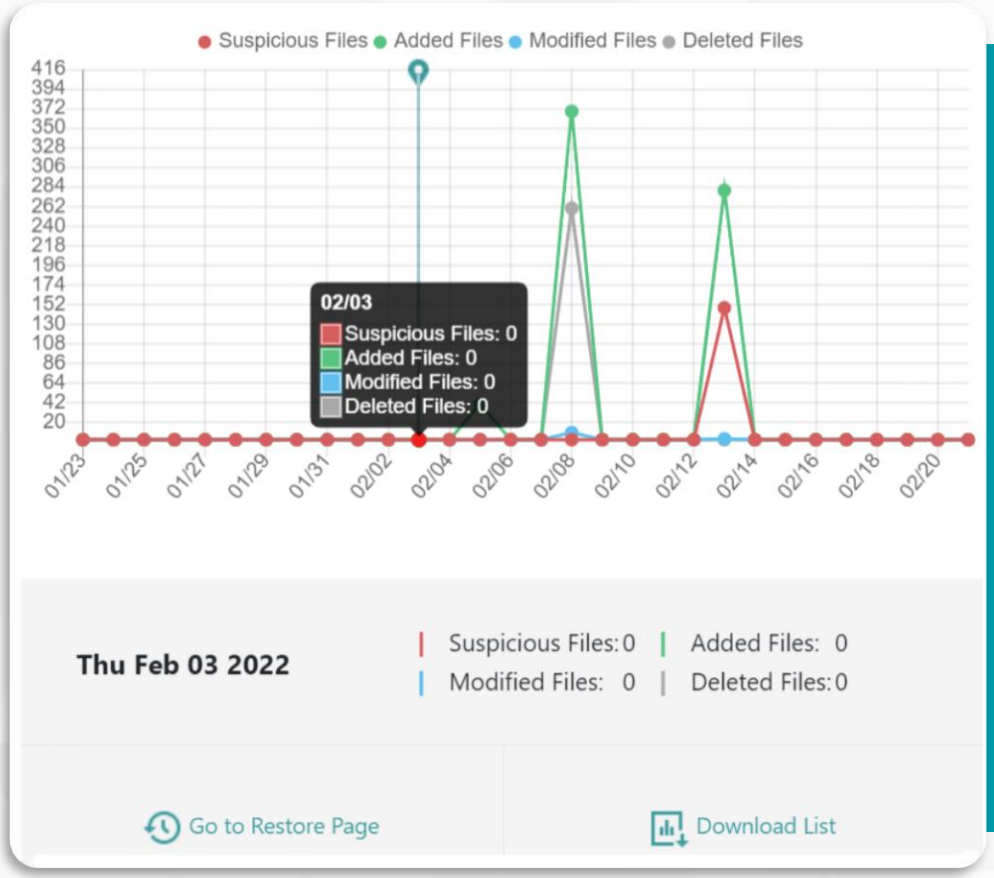
Granular restore, in or out of place

Search for and filter content for restore based on properties—including content type, owner, date created, file size, parent list name, parent folder name, email subject, date sent, and more. Restore granular content in place or out of place – even to your file system or export as a PST!

Visibility and control over protected content

Simple dashboard display gives immediate insight into what services are covered – and where you may be exposed. Whether you bring your own storage – or use AvePoint's Azure storage – you retain full control over your protected content!

Getting your data to safety – Quick Restore



Contact the user:

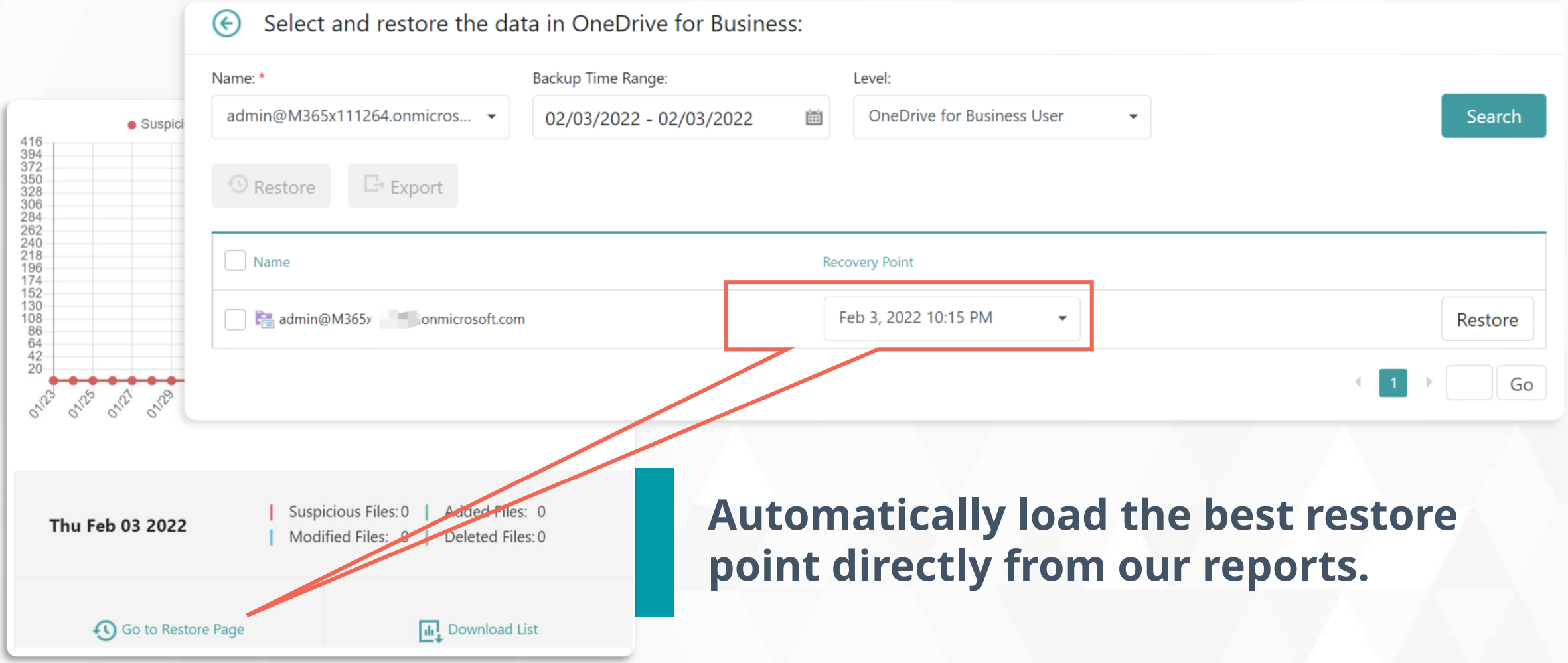
- Eliminate potential big change events (migrations, change of role, etc.)

Coordinate with security:

- Check with sensitivity label roll-outs
- Investigate suspicious files lists
- Remove source of the issue FIRST

Identify a safe place to recover the user

Getting your data to safety – Quick Restore



Automatically load the best restore point directly from our reports.

Case Study: Ransomware

Following their roll out of Office 365 and SharePoint Online, Walls experienced an incident with one of their members of staff being hit with a malicious ransomware attack. The staff member's OneDrive was replicated and then deleted, resulting in the complete loss of that user's data.

> *"With the amount of control that Office 365 brings to end users, it is not realistic for a company to completely monitor every deletion. So we had to have a way to very quickly and easily recover from something like this, and began evaluating Office 365 backup products…*

Source: https://www.avepoint.com/case-studies/walls-construction

Questions?

thank you

AvePoint®

Sales@AvePoint.com | +1 800.661.6588

www.AvePoint.com