Reducing the Risk of Account Takeover

Spanning Backup and Dark Web Monitoring
for Office 365

SPANNING
A Kaseya COMPANY

Today's Speakers

Dave Wallen
Director of Product Marketing

Matt McDermott
Director of Product Management
Office 365 MVP

Agenda

Introduction to Spanning

Office 365 and Account Takeover Attacks

Reducing the risk of a successful ATO

Solution Demonstration

Questions and Discussion

SPANNING A **Kaseya** COMPANY

Founded in

2010

Based in

Austin, TX

10,000+

Customers with 1.5M+ Seats

2.8 Billion+

Items protected each week

1.0 Billion+

Items recovered in 2019

SPANNING
BACKUP FOR OFFICE 365

Front and back-end protection for mail, calendar, contacts, OneDrive & SharePoint
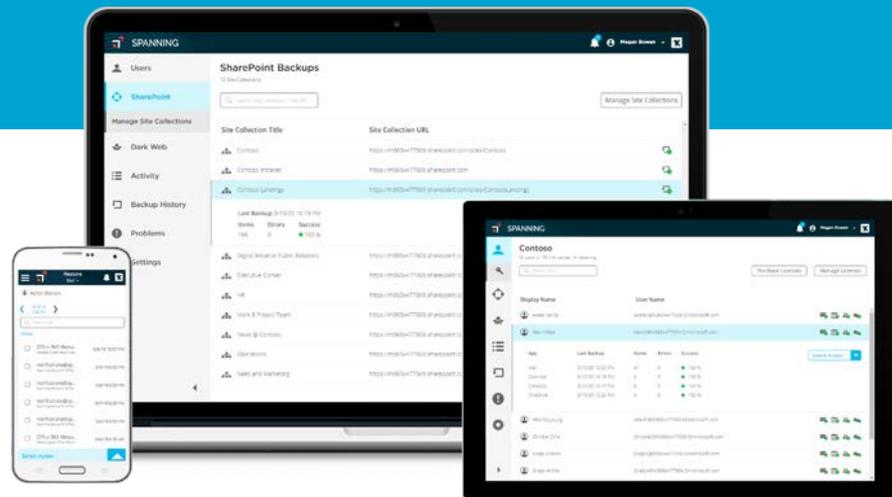
PROTECT

Protect your critical business data with automated and on-demand backups and Dark Web monitoring

RECOVER

Recover data quickly and easily with self-service restore from any point-in-time backup for Office 365

COMPLY

Comply with regulatory and legal controls for data protection and business continuity

Microsoft only covers their mistakes

They won't fix yours

SPANNING
A Kaseya COMPANY

Microsoft's responsibility

- ✓ Hardware failure
- ✓ Software failure
- ✓ Natural disaster
- ✓ Power outage
- ✓ Delete requests

Your Responsibility

- ☐ Human mistakes
- ☐ Programmatic errors
- ☐ Malicious insider activity
- ☐ External hackers
- ☐ Ransomware & viruses

SPANNING
A **Kaseya** COMPANY

Office 365 and Account Takeover Attacks

Spanning Dark Web Monitoring
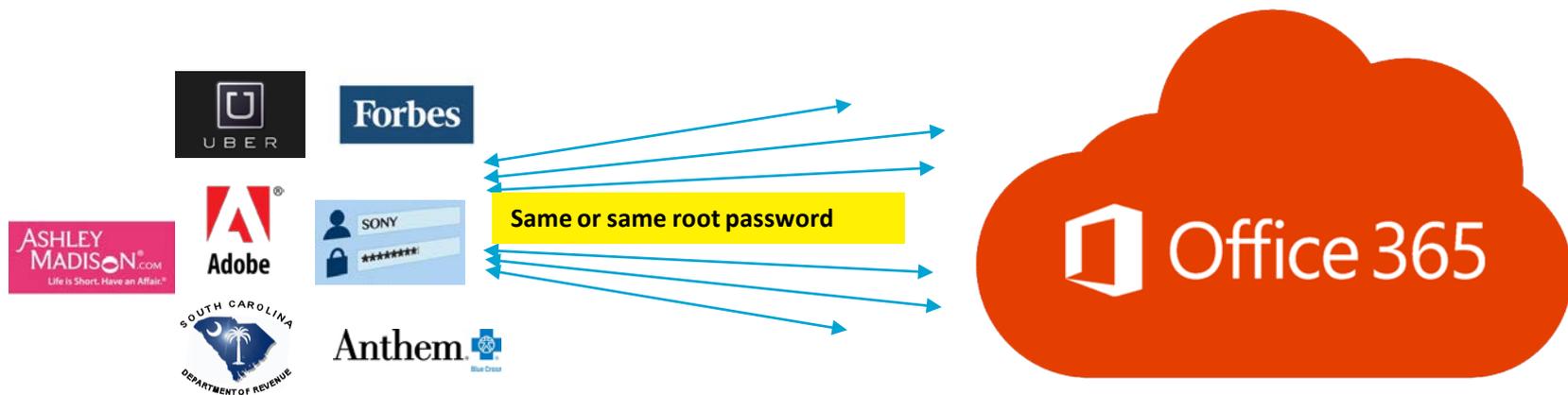
Account Takeover (or ATO) is a type of identity theft where a bad actor gains unauthorized access to an account belonging to someone else.

SPANNING
A Kaseya COMPANY

76% of people will use the same password for most, if not all, websites.

Same or same root password
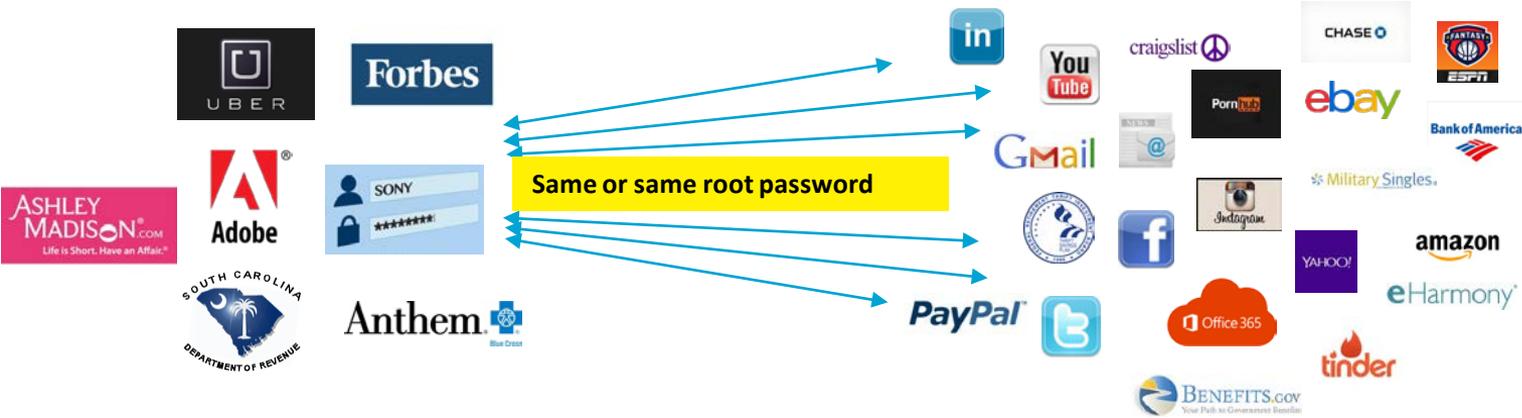
Office 365 is no exception.

Same or same root password

It's not just email

Calendar
Schedule and share meeting and e...

Delve
Get personal insights and relevant...

Dynamics 365
Break down the silos between you...

Excel
Discover and connect to data, mo...

Forms
Create surveys, quizzes, and polls ...

Kaizala
A simple and secure mobile chat a...

MyAnalytics
Create better work habits with insi...

OneDrive
Store, access, and share your files i...

OneNote
Capture and organize your notes a...

Outlook
Business-class email through a ric...

People
Organize your contact info for all ...

Planner
Create plans, organize and assign ...

Power Apps
Build mobile and web apps with th...

Power Automate
Create workflows between your ap...

Power BI
Create actionable, dynamic, and e...

PowerPoint
Design professional presentations.

SharePoint
Share and manage content, knowl...

Stream
Share videos of classes, meetings, ...

Sway
Create and share interactive repor...

Tasks
Create and manage tasks in Outlo...

Teams
The customizable, chat-based tea...

To Do
Manage, prioritize, and complete t...

Video
Share videos of classes, meetings, ...

Whiteboard
Ideate and collaborate on a freefo...

Word
Bring out your best writing.

Yammer
Connect with coworkers and class...

SPANNING
A Kaseya COMPANY

10.1% Microsoft PowerPoint

2.4% Microsoft Outlook (MSG, PST)

29.2% Microsoft Excel

16.7% Microsoft Word

58.4%

OF SENSITIVE DATA STORED
IN THE CLOUD IS STORED IN

OFFICE DOCUMENTS

18.8% Adobe PDF

22.8% Other
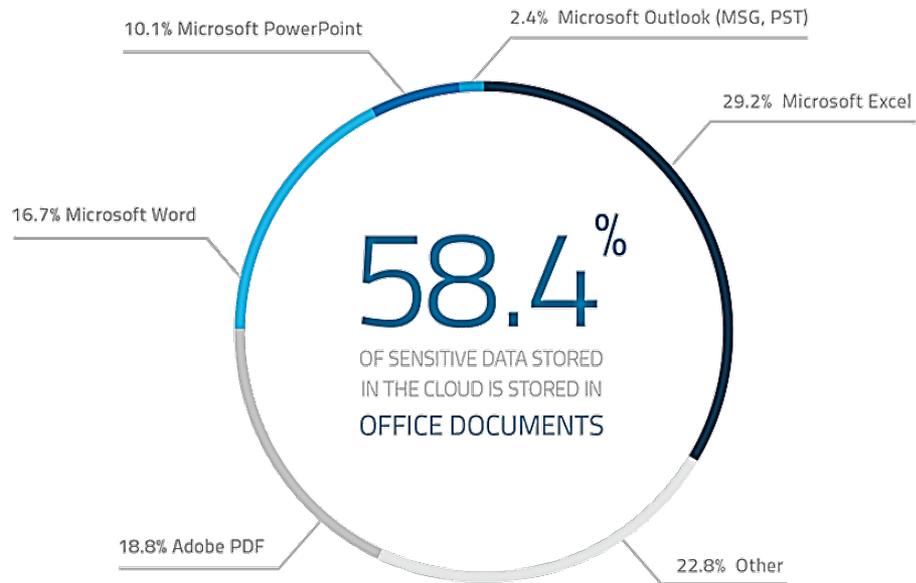
Office 365 Targeted

" There are **over 300 million** fraudulent sign-in attempts to our cloud services every day. Cyberattacks aren't slowing down, and it's worth noting that many attacks have been successful without the use of advanced technology. All it takes is one compromised credential or one legacy application to cause a data breach.

Melanie Maynes Senior Product Marketing Manager,
Microsoft Security

SPANNING

40%

of enterprises experienced Office 365 credential theft.

Report: Cyren and Osterman Research

SPANNING
A Kaseya COMPANY

+476%
Increase in attacks on businesses

14,000
Email scams per year

$12B
Cost to businesses

" 81% of confirmed data breaches in 2018 leveraged weak or stolen passwords.

SPANNING
A Kaseya COMPANY
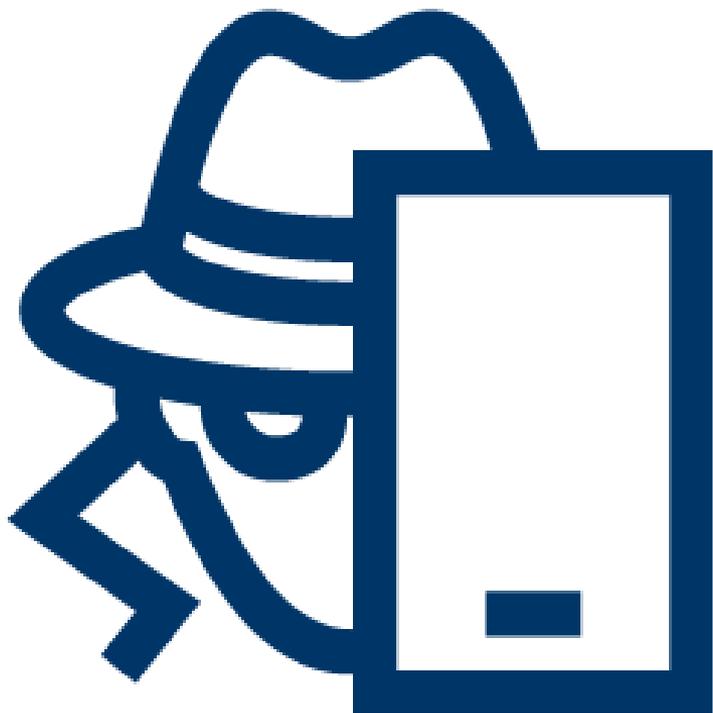
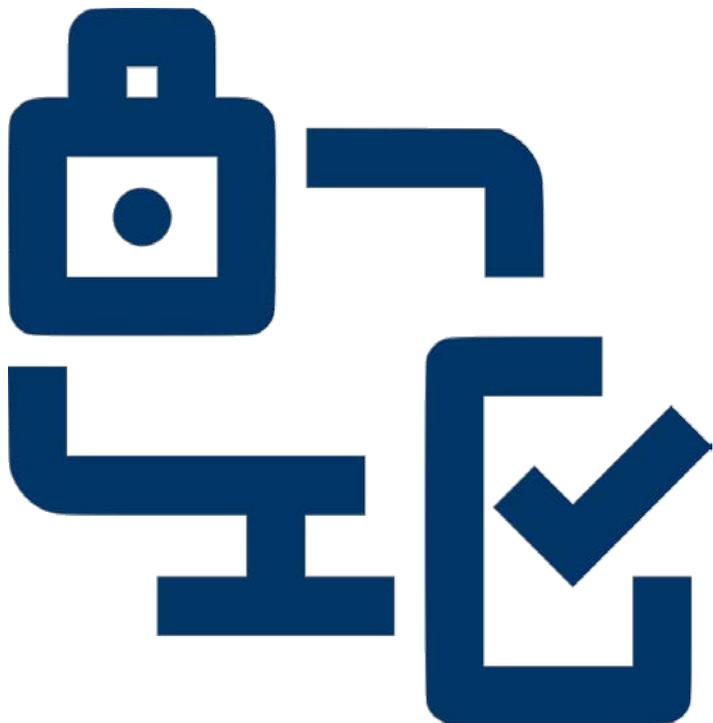"They bide their time to monitor email and track activity in the company, to maximize the chances of executing a successful attack.

SPANNING
A Kaseya COMPANY

"Steal IP, perpetrate business email compromise, gain access to financial accounts and commit other types of cyber fraud.

Reducing your risks with Spanning

Spanning Dark Web Monitoring

" Implementing multi-factor authentication is the most important action you can take to help prevent account takeover.

Spanning Backup for Office 365

Now with Dark Web Monitoring for Office 365
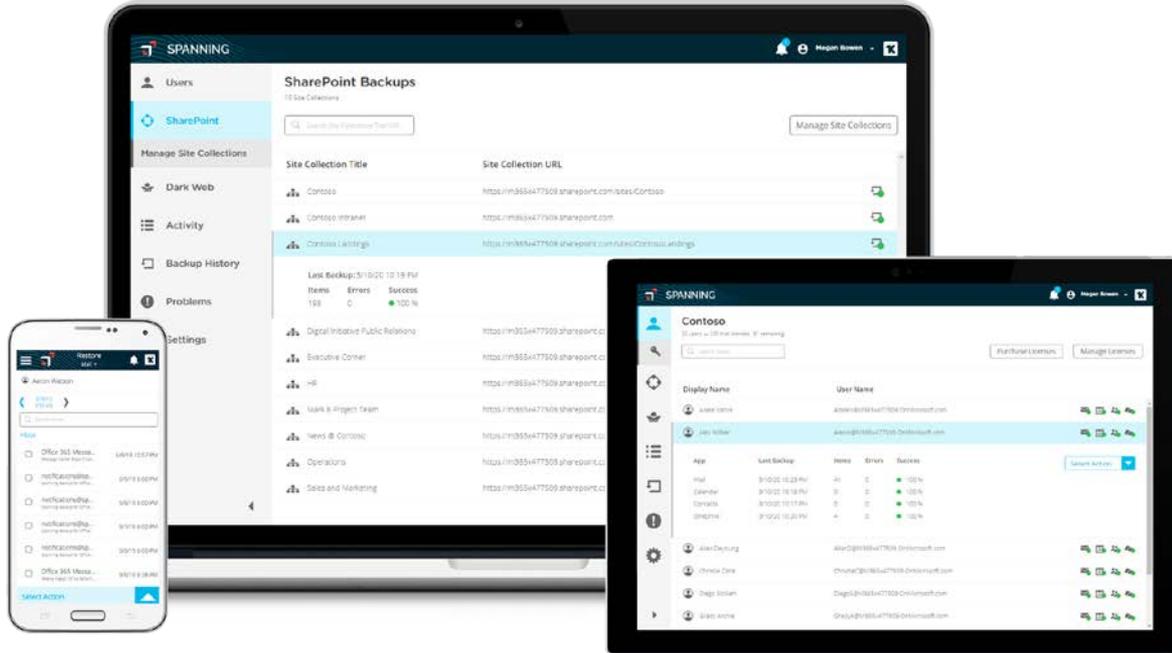
How we are different

Dark Web Monitoring for Office 365
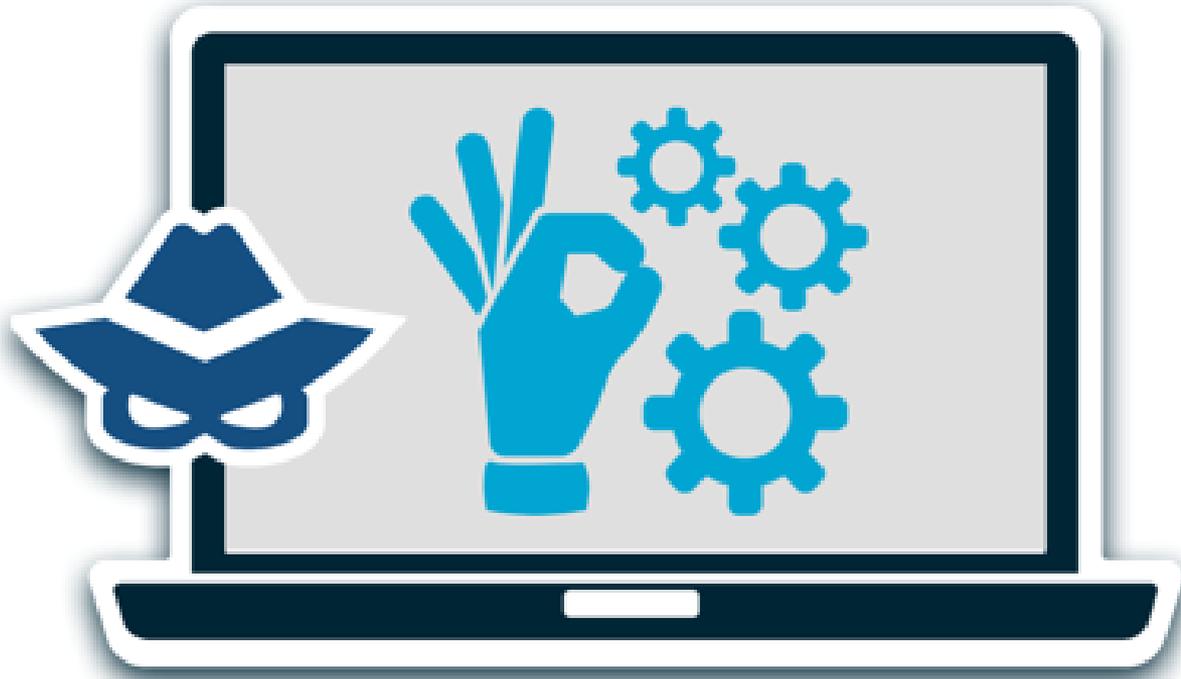
Industry-Leading Monitoring Platform

Dark Web Monitoring for Office 365

Demonstration

Spanning Dark Web Monitoring

01

Per Backup User Pricing

Dark Web Monitoring is priced per licensed Spanning Backup User

02

All Tenant Domains Monitored

Spanning will monitor all domains associated with your Office 365 tenant

03

Reporting on Any Domain Account

Reporting on *any* email address associated with your domains even if they are *not* licensed for Spanning Backup

50 Office Workers

Licensed for Spanning Backup for Office 365

150 Warehouse Workers and Drivers

Licensed for Office 365

Coverage

All 3 Domains
All 200 Current Employees
Plus any other account associated with those three domains

Proactive Defense Against Account Takeover

Spanning Dark Web Monitoring for Office 365

Questions?

Spanning Dark Web Monitoring for Office 365

Ready to activate Dark Web Monitoring?

Current Spanning customers - Reach out to your account manager!

Not currently a Spanning customer - Follow the below link to get started!

https://spanning.com/dark-web-monitoring-new-customers/

Upcoming Webinar

The Business Case for Office 365 and G Suite Backup

Wednesday, April 15, 2020 @ 10:00 AM EDT | 9:00 AM CDT

SPANNING
A Kaseya COMPANY