



Work From Home Securely with Microsoft 365

NPC Safe Computing Webinar Series

September 13th, 2022

Darren Mar, National Sales Manager
May-May Ogoigbe, Marketing Manager

Presenters



Darren Mar
National Sales Manager

10 years in SMB technology products and services, with emphasis on financial services small office security.



May-May Ogoigbe
Marketing Manager

6+ years experience in marketing leadership for SMBs, startups and multinational organizations.

Thank You!



Agenda

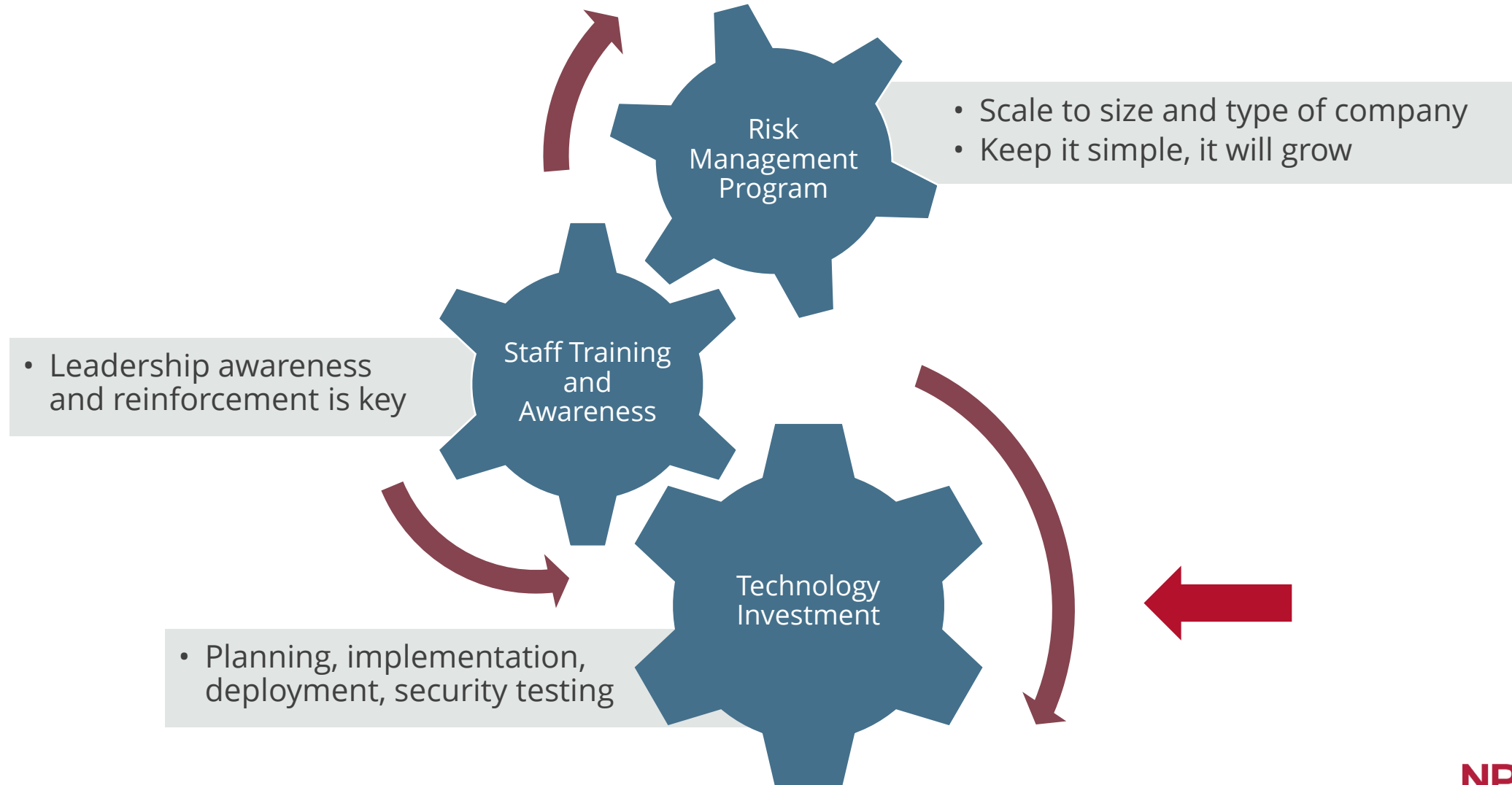
- Current Threats
-

- Microsoft Security
-

- Microsoft 365 Overview
-

- Q&A

SMB Cyber Defense Assets



Spoof Email

Notification



BMO Harris <info@greenpia-yame.com>

To



Wed 2022-01-19 5:34 PM

[EXTERNAL - Use caution when opening attachments or links.]



Dear Customer,

Your password has been disabled due to multiple use of incorrect login details. For your security, we have disabled your Online banking.

To restore your account and continue the use of online banking and stop further disabling of your bank account.

[Click here to restore and protect your accounts online.](#)

If you have any questions, we are available 24 hours a day, 7 days a week ,

Please do not reply to this email.

Sincerely,

You will find a confirmation of this message in your Messages & Alerts inbox.

Bank of Montreal Online Customer Service

Attack Methods

Threats are up

300%

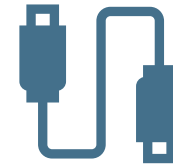
since the pandemic started



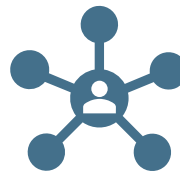
Email and web
browsing



Remote desktop



Improperly Protected Networks



IoT devices



Supply Chain Attacks

Small business is the target...



Forbes

PERSONAL FINANCE

Small Businesses Bearing Brunt Of Ransomware Attacks, Senate Told

Ted Knutson Contributor ◉
I cover financial regulatory issue, cybersecurity, fintech & bitcoin.

Jul 27, 2021, 01:16pm EDT

Follow



BCBUSINESS

THE LISTS INDUSTRIES PEOPLE YOUR BUSINESS CAREERS LIFESTYLE PODCASTS PROMOTED CONTENT SUBSCRIBE

TECH & SCIENCE

Five Reasons Why Small Businesses Are at Increased Risk of Ransomware Attacks

f t in p

BCBusiness + Uniserve



tech.co

News Reviews & Advice Business Tech Online Security

Home > News >

82% of Ransomware Attacks Target Small Businesses, Report Reveals

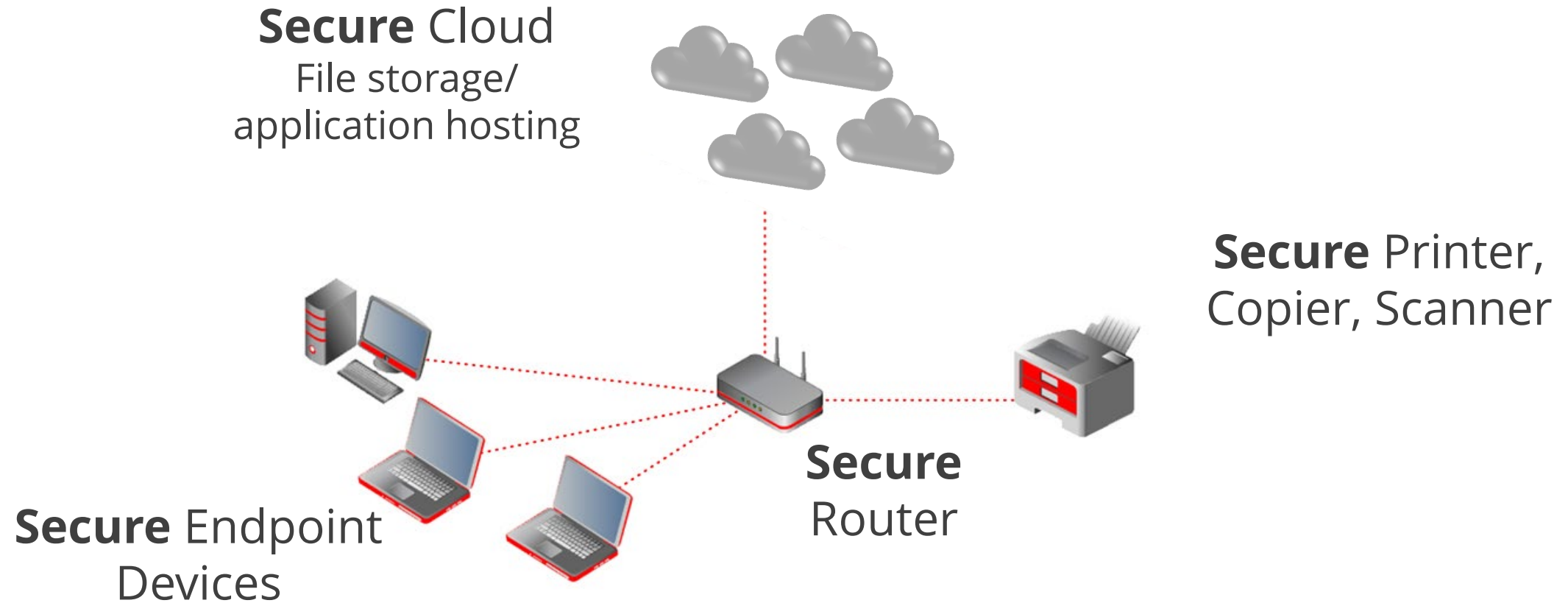
Whilst Ransomware remains a threat to businesses of all sizes, companies with less than 1,000 employees are most at risk.

Aaron Drapkin | February 7th 2022 - 1:10 pm

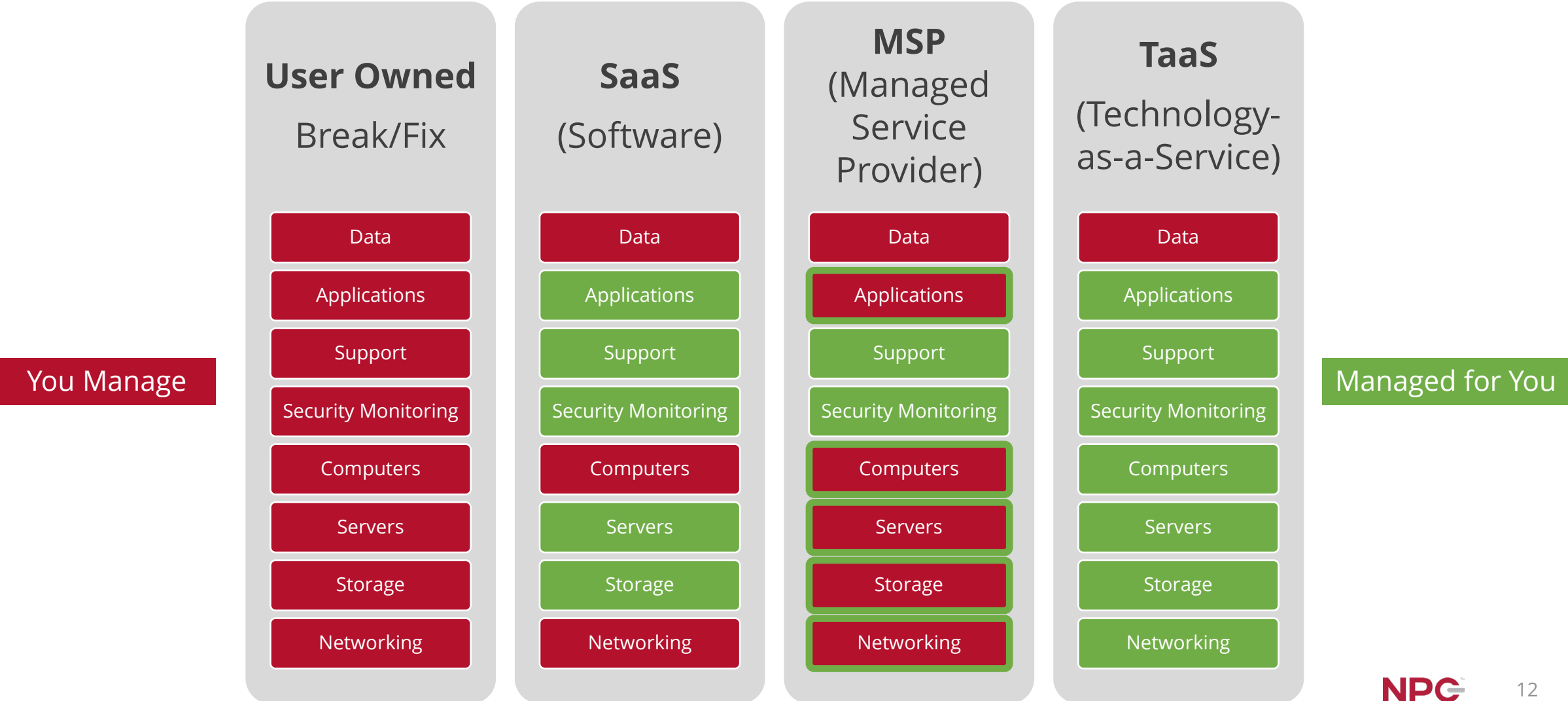


Office and Home Office of the Future

Office of the Future



IT Delivery Models



What's the Benefit?

- As-a-service models remove the cost of custom-building common application, network, server, security, and services needs
- Specialization by the provider allows more features for less cost, improved performance, security, and reliability
- Allows for more economical “scaling up” or “scaling down”

It is difficult to compete with the security, speed, reliability and economics of specialization



Microsoft Security

Microsoft 365 Business Premium Security...



Multi-factor Authentication with phone call, text, or app as second factor



Administrator account control, including user access and password policy management



Location-Based Authentication



Email:

- Auto-forwarding control
- Message encryption
- Advanced anti-phishing capability
- Blocks specific file extensions known to distribute malware
- Data Loss Prevention and Exchange Email Online Archiving



Advanced Threat Protection:

- Increased SPAM and threat filtering through AI
- Safe Attachments
- Safe Link Protection

Multi-Factor Authentication

Definition:

A method of allowing access to applications, websites, systems or devices, only after the user presents two or more pieces of authentication evidence.



Forms of Attacks Prevented

Stops “brute force attacks”, or account compromise from lost or stolen passwords/credentials, or poorly constructed primary authentication systems:

Phishing

Man-in-the-Middle (MITM) Attacks

Spear Phishing

Credential Stuffing

Keyloggers

Brute-Force Attacks

Reverse Brute-Force Attacks

MFA Benefits

“Your account is more than 99.9% less likely to be compromised if you use MFA”

Alex Weinert, Group Program Manager for Identity Security and Protection at Microsoft

August 27, 2019

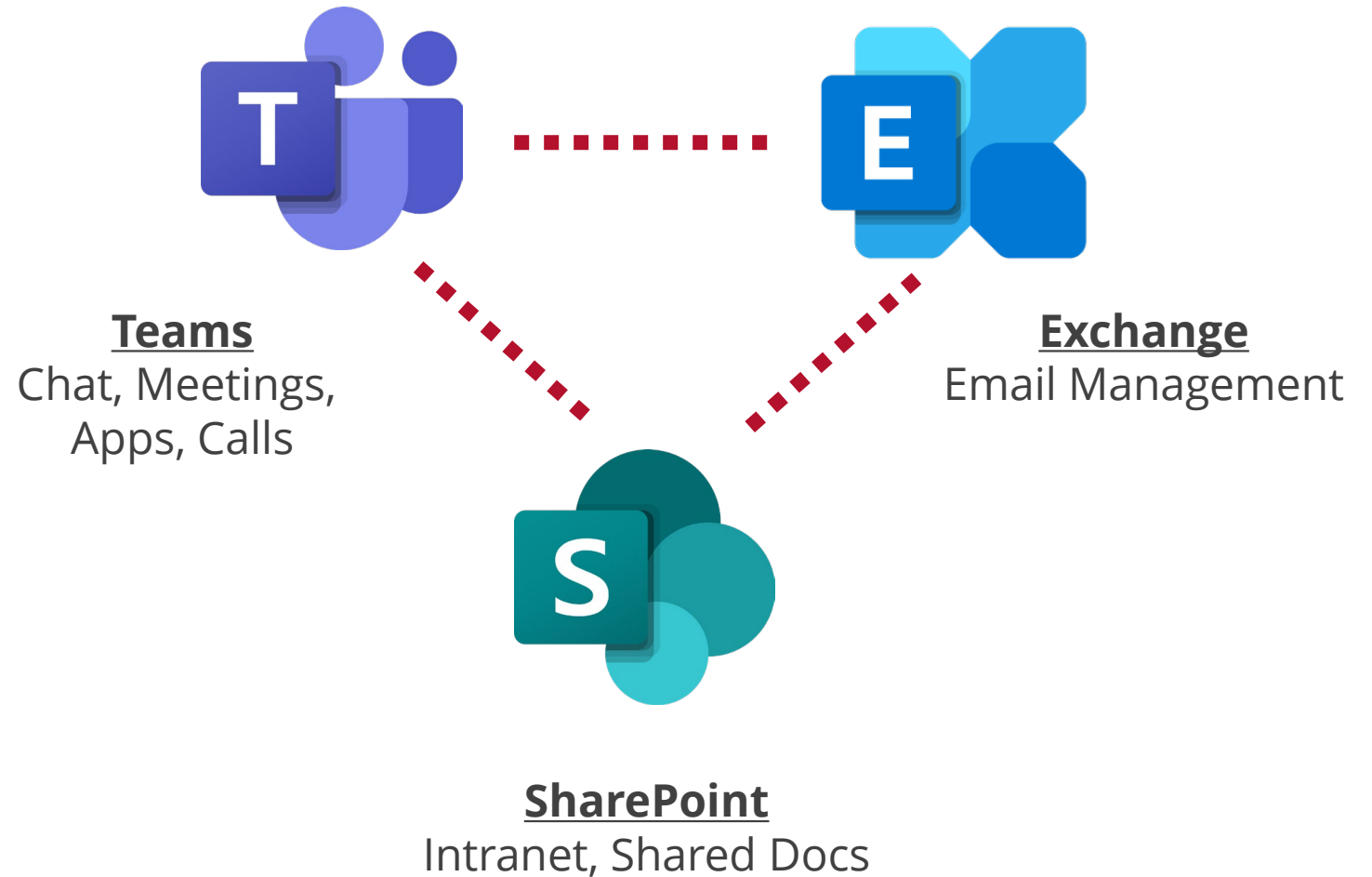
- Microsoft reports that 20+ million accounts are probed daily in Microsoft ID systems for Credential Stuffing



Microsoft 365 Overview

Business Integration of 365 for the SMB

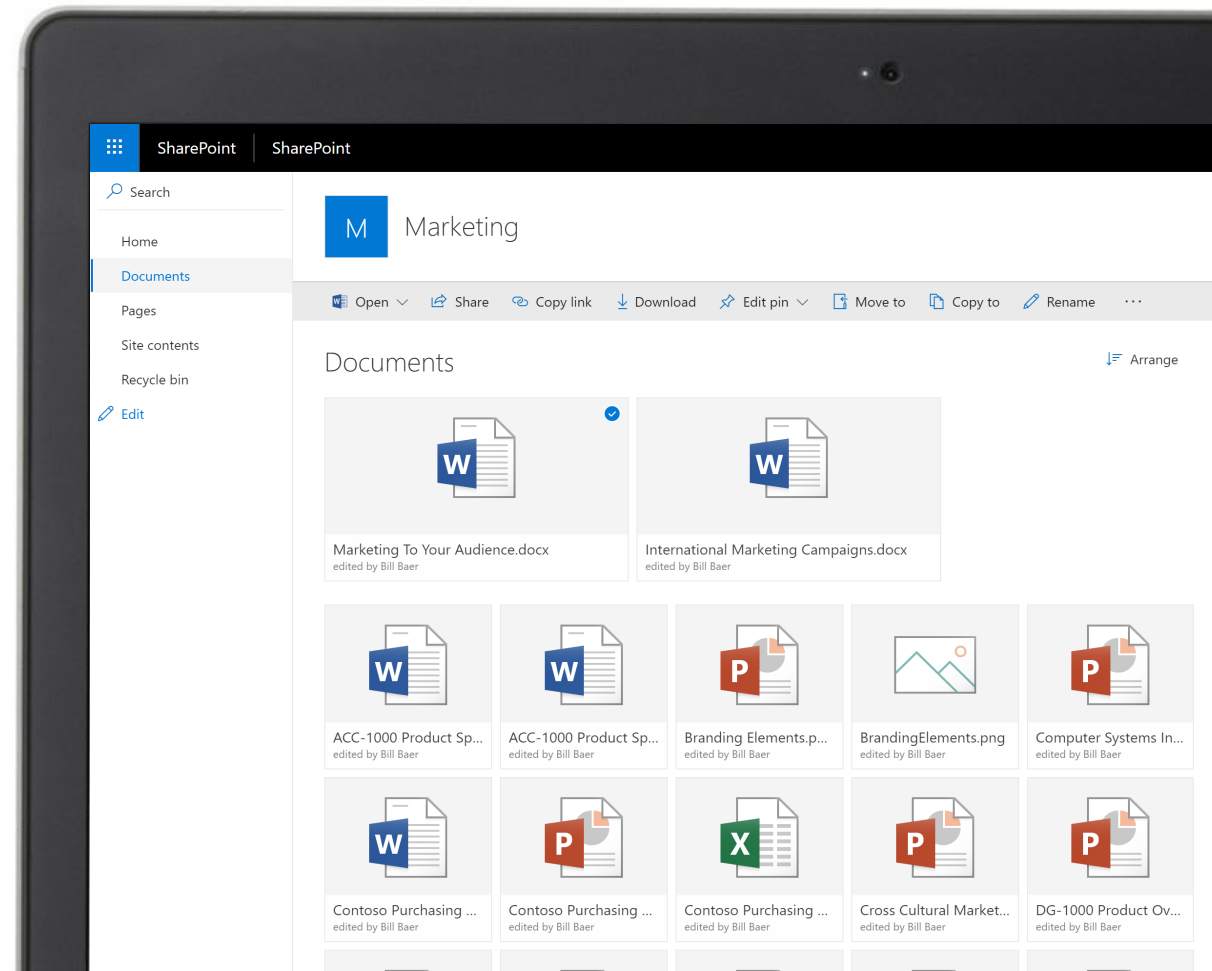
A suite of mobile, desktop and cloud-based productivity tools on a unified communication and collaboration platform



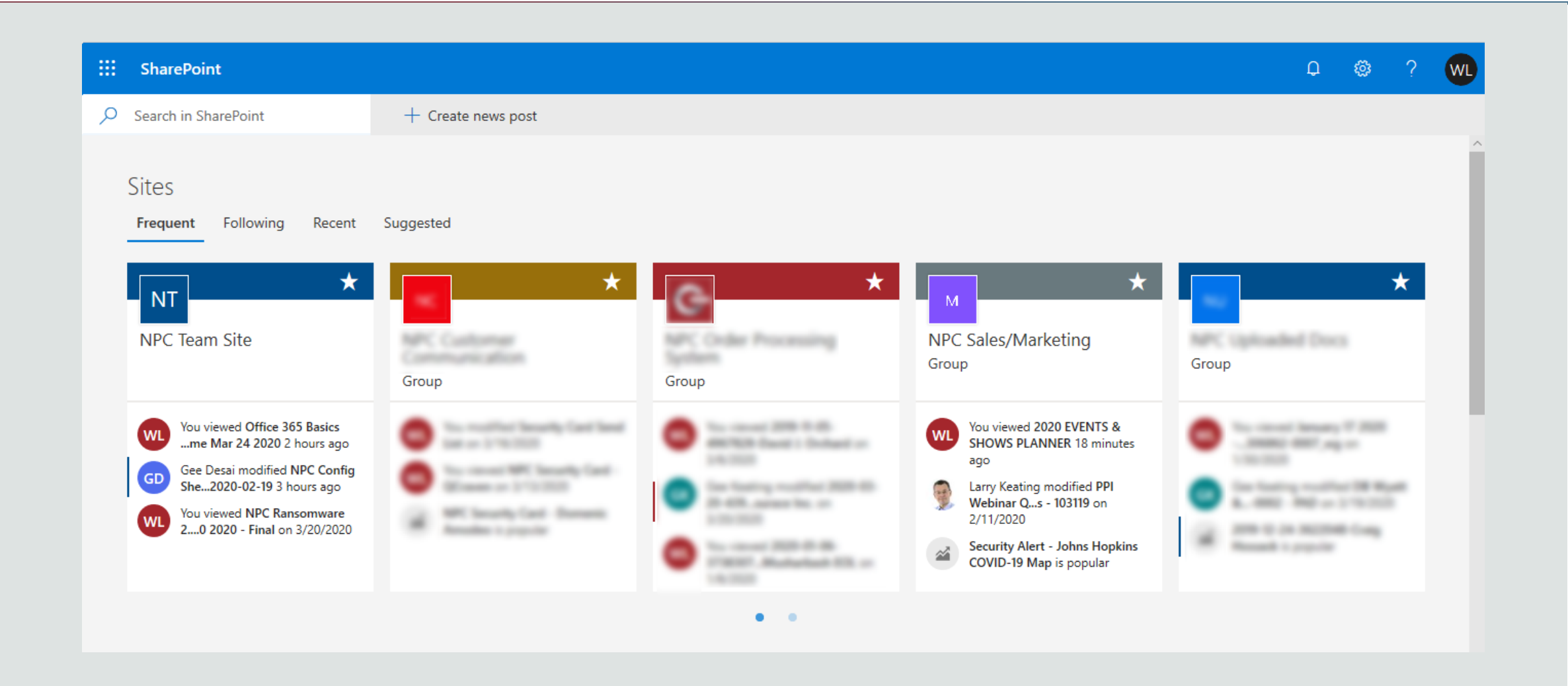
Securely Connect to Your Data with SharePoint



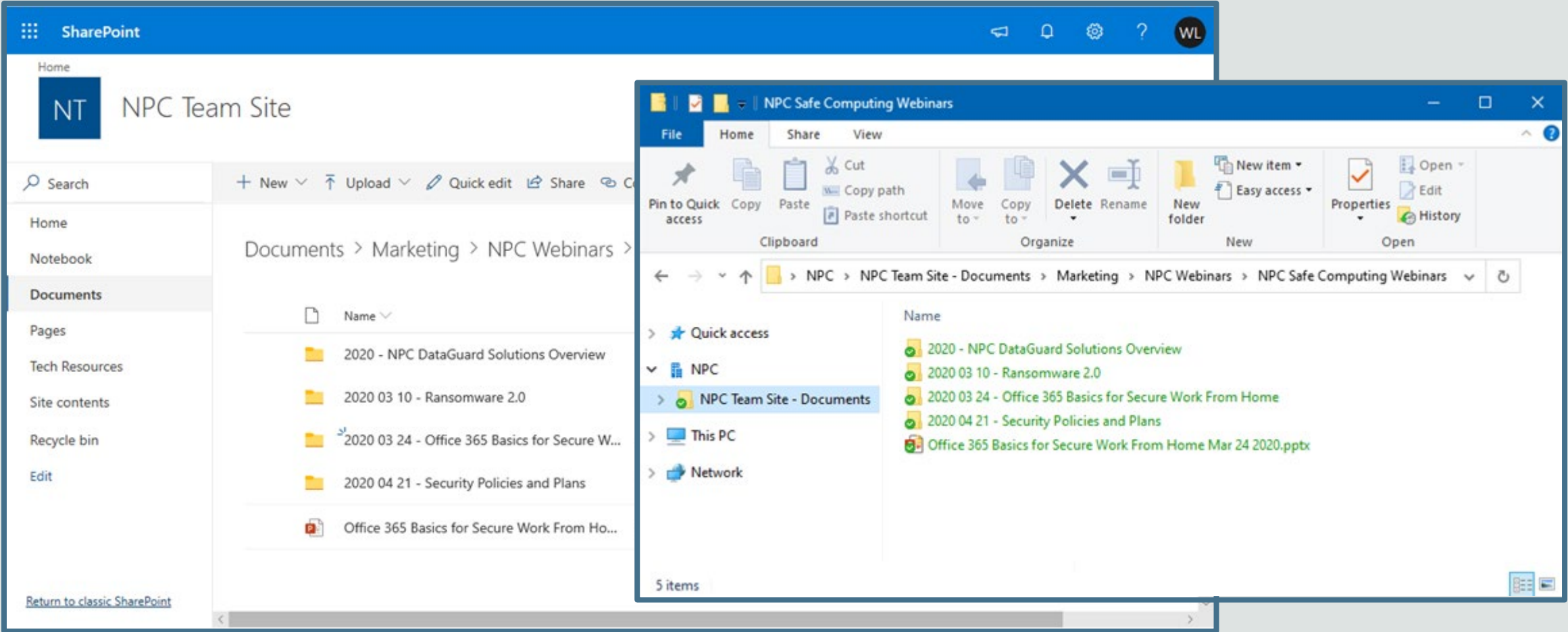
- Replaces your file server, USB drives, or email file sharing
- Mobile access everywhere
- Powerful collaboration and integrated tools and apps
- Generate links for secure file sharing, or grant controlled access
- Data sovereign



Using SharePoint: Sites



Using SharePoint Documents Seamlessly



Using SharePoint: Secure Share

The image displays a sequence of four overlapping screenshots illustrating the OneDrive secure share process:

- First Screenshot (Request Verification):** Shows the OneDrive interface with the heading "Request Verification". It states, "You've received a secure link to:" followed by a folder icon and "ITI Test Folder". Below, it says, "To verify your identity, we'll send you a verification code at **dengoulet@rogers.com**." A blue "Send Code" button is visible. At the bottom, there is a Microsoft logo and copyright text: "© 2017 Microsoft Privacy & Cookies".
- Second Screenshot (Email):** Shows an email from "no-reply@sharepointonline.com" dated "August 17, 2020 5:07 p.m.". The email body says, "28674989 is your Microsoft verification code." It includes a "OneDrive" logo and a yellow box containing "Account verification code: 28674989". Below, it says, "Having problems with the code? View the error and make sure that the email identifier matches an updated email or try requesting a new code." At the bottom, it says "© 2017 Microsoft Privacy & Cookies".
- Third Screenshot (Enter Verification):** Shows the OneDrive interface with the heading "Enter Verification". It states, "You've received a secure link to:" followed by a folder icon and "ITI Test Folder". Below, it says, "To open this link, enter the code you received via email at **dengoulet@rogers.com**." A text input field contains "28674989". A blue "Verify" button is visible. At the bottom, there is a "Keep me signed in" checkbox and copyright text: "© 2017 Microsoft Privacy & Cookies".
- Fourth Screenshot (File View):** Shows the OneDrive file view for "Files > ITI Test Folder". It displays a list of files with a header "Name" and a dropdown arrow. A single file is listed: "ITI Test Word doc.docx" with a Word document icon.

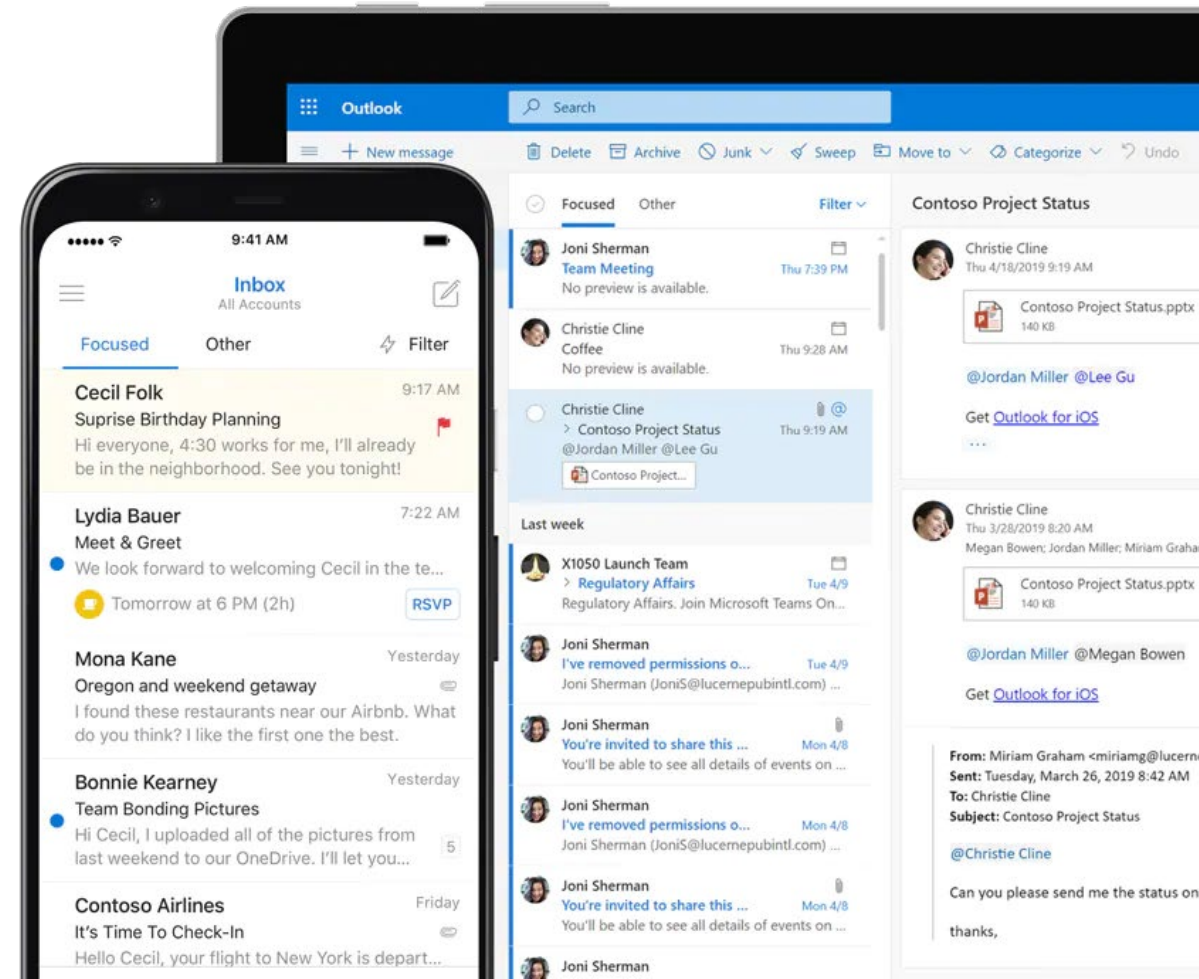
Using SharePoint: Setup Pointers

- Know specific levels of access by user, what configuration settings you require
- Ensure the source data is malware and corruption free
- SharePoint is not a backup
- Very long files names (name and path exceeds 400 characters) will not migrate
- Certain illegal file extensions such as .lock .con .prn, or special characters like *:<>?/, etc. will not migrate
- PST files in the folders will replicate on each synchronization
- Multi-GB files may not sync at some license levels

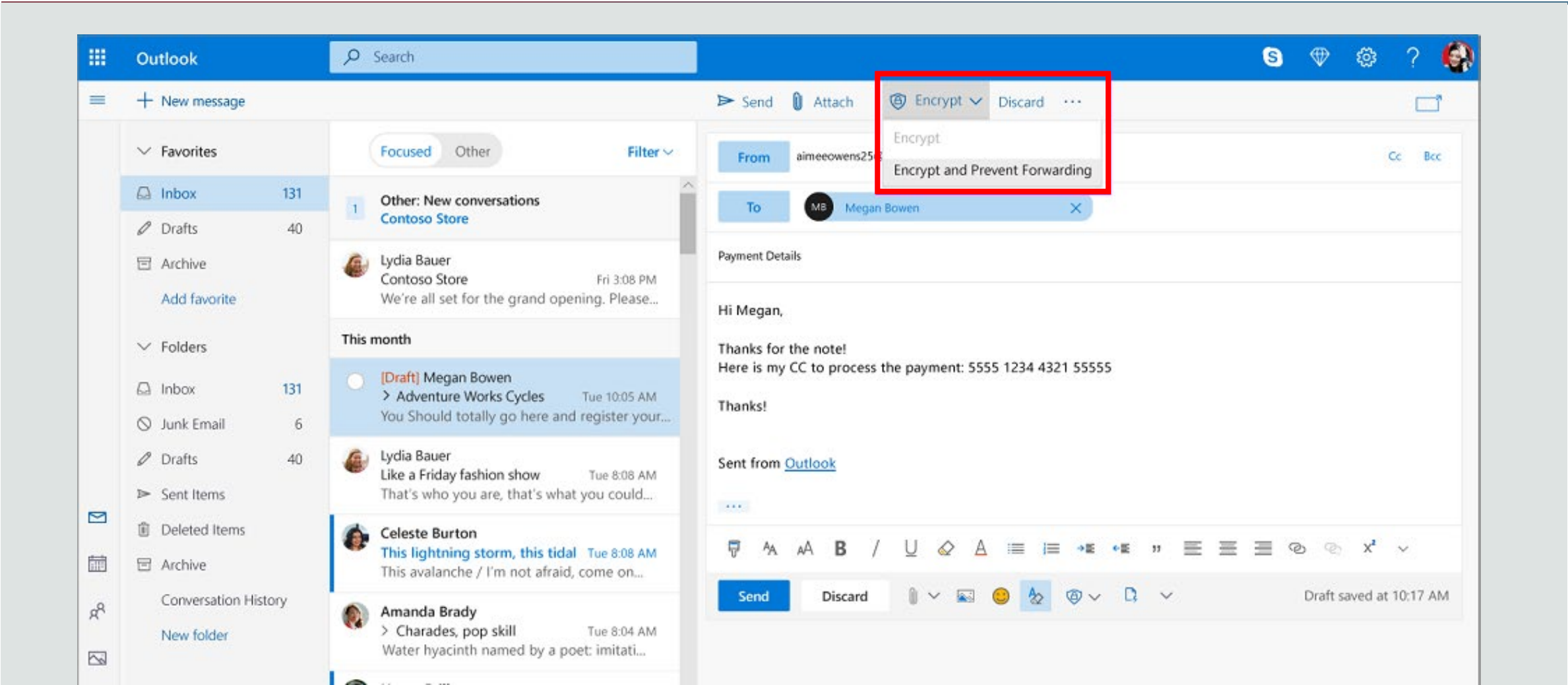
Secure Email and Email Management with Exchange Email



- Professional-grade email system for your team's improved performance and security
- Both in-the-cloud and integrated device access for mobility and organization
- In-Canada or U.S. data sovereignty to meet your compliance requirements
- Seamlessly integrated with Teams, SharePoint, OneDrive and your calendar
- Integrated advanced capabilities such as DLP and Email Archiving



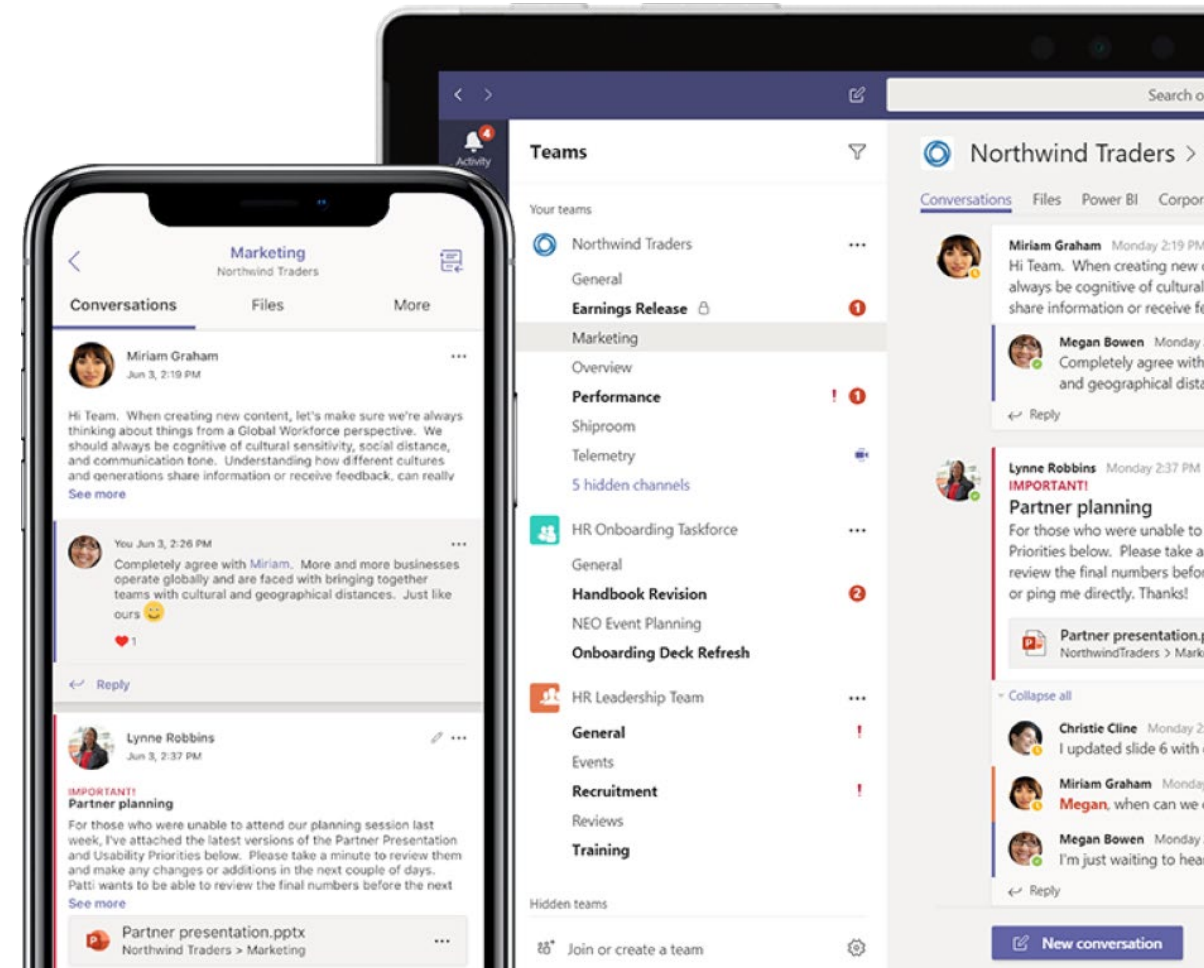
Encrypting Email



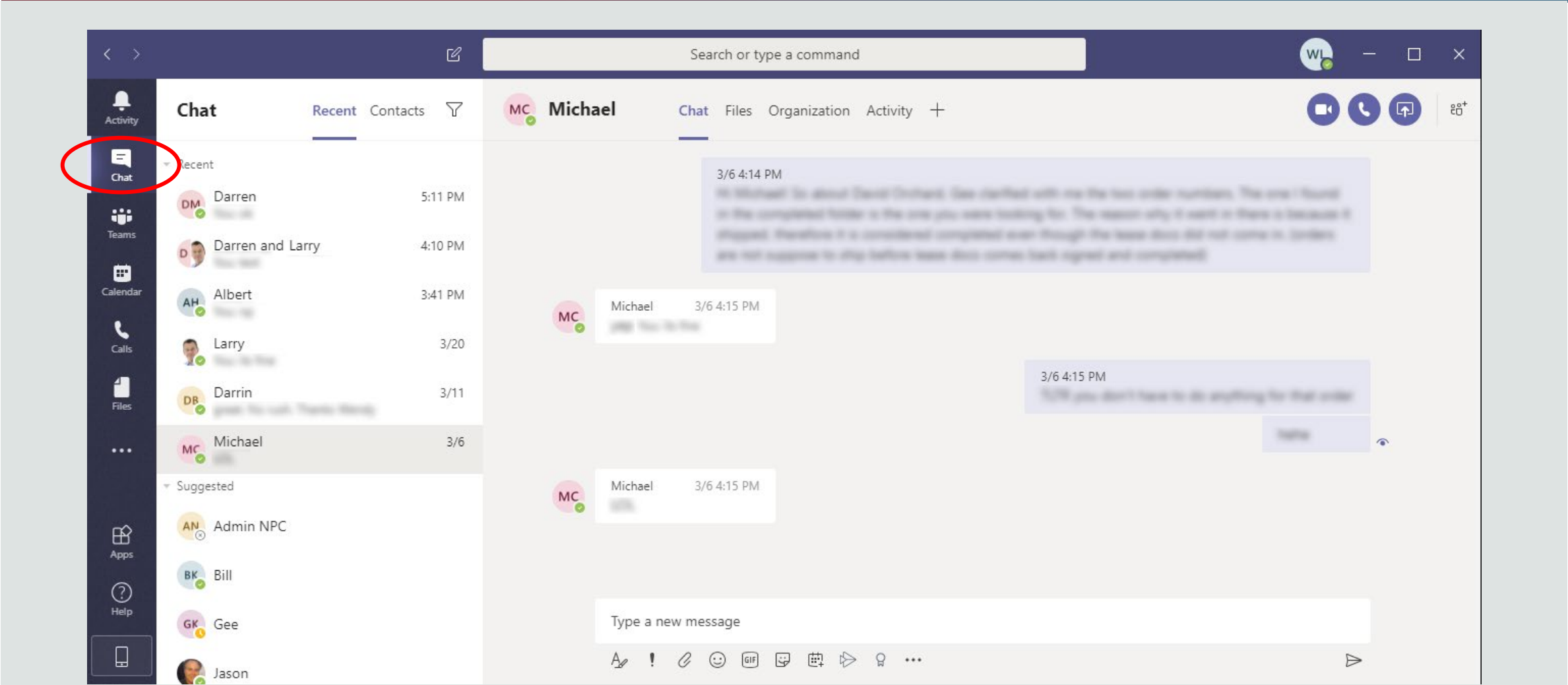
Securely Connect People with Teams



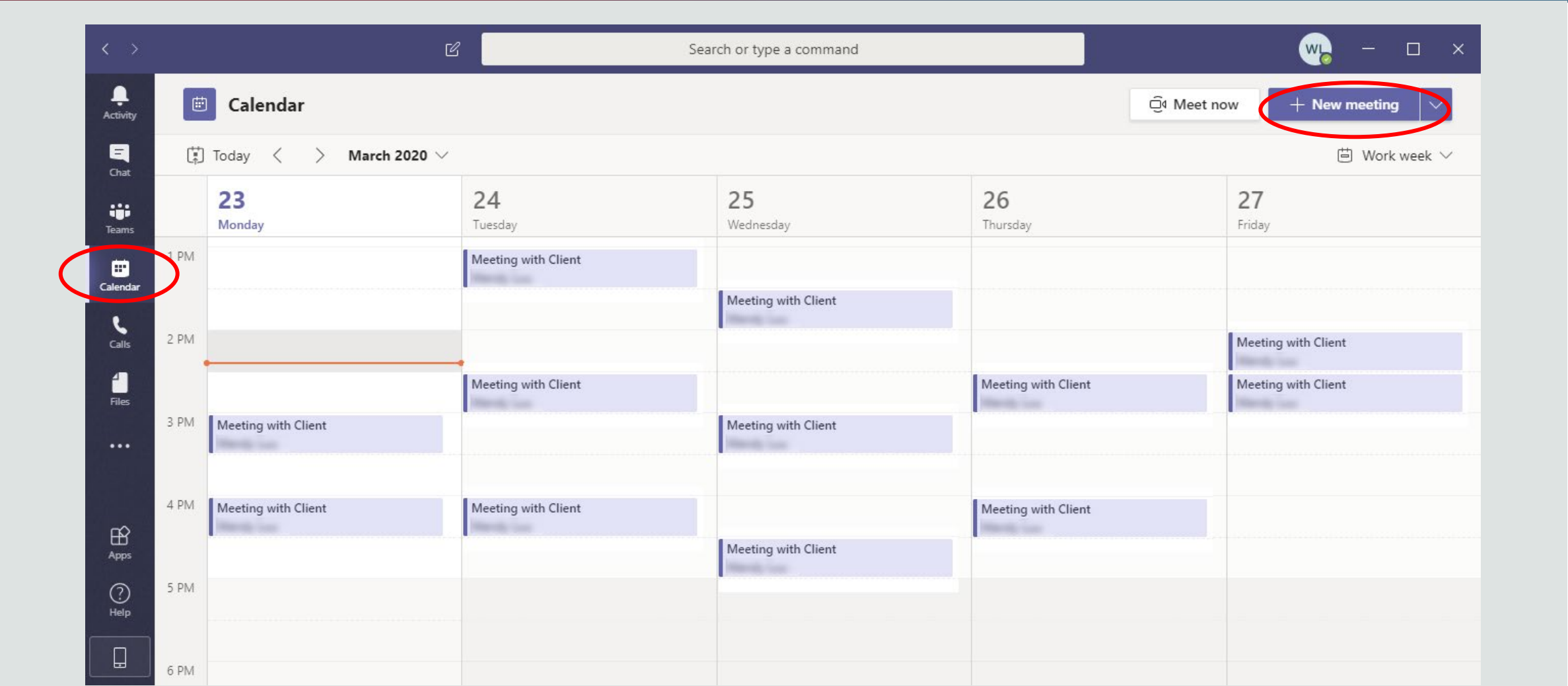
- Everything brought together, unified communications
- Chat, video, calls, conference calls, screen sharing, set appointments, mark events, share files, create groups, call recording, guest access



Using Teams: Chat



Using Teams: Calendar



Using Teams: Apps Integration

The screenshot displays the Microsoft Teams interface, specifically the 'Apps' section. The left-hand navigation pane is visible, with the 'Apps' icon highlighted by a red circle. The main content area is titled 'Browse available apps and services' and features a search bar at the top. Below the search bar, there are several app cards, each with an icon, name, and a brief description. The apps shown include Opsgenie, Smartsheet, ScrumGenius, Trello, Flow, Polly, Azure DevOps, Zoom, Cisco Webex Meetings, Jira Cloud, and Yammer. The 'Apps' icon in the navigation pane is circled in red.

Apps

Search all

Browse available apps and services

Add your favorite app for yourself or for a team.

See our top picks

- Opsgenie**
- Smartsheet**
- ScrumGenius**
- Trello**
Project management
Trello lets your team work more collaboratively and get more done. Trello's boards, lists, and cards enable you to organize and prioritize your...
- Flow**
Workflow + business management
Automate time-consuming and repetitive tasks by integrating your favorite apps and services with Microsoft Flow.
- Polly**
Communication
Gather real-time insights with simple polls that work where you work
- Azure DevOps**
Developer tools
Plan better, code together and ship faster using Azure DevOps. Search, find work, and collaborate better with your team.
- Zoom**
Communication
Seamlessly start, schedule and join Zoom meetings from Microsoft Teams. Meet happy with flawless video, clear audio, and easy content...
- Cisco Webex Meetings**
Communication
The Cisco Webex Meetings integration makes it easy to add a link for your Webex meeting or Personal Room meeting to your message in you...
- Jira Cloud**
Project management
- Yammer**
Communication
- MindMeister**
Productivity

NPC Managed Microsoft 365 Plans

Apps For Business	Business Standard	Business Premium	E3 + Defender for O365 - Plan 1
<ul style="list-style-type: none"> • Included with each NPC • Basic “desktop” suite • Word/Excel/PPT/Outlook • No access to web-portal (OneDrive) 	<ul style="list-style-type: none"> • 1st level upgrade from the included suite • Includes Apps + SharePoint + Teams • Professionally managed, monitored with 24/7/365 support • Includes Business OneDrive 	<ul style="list-style-type: none"> • 2nd level upgrade, includes Apps + Standard + Exchange email management • Hosted email domain • Hosted email data w/ 50Gb inbox • Advanced email threat protection and management 	<ul style="list-style-type: none"> • Alternate to Business Premium • Includes 100Gb email inbox • Email encryption • Advanced email threat protection and management

In addition, provided by NPC at all levels:

- More secure Tenants, managed and configured by NPC, vs. retail customer subscriptions
- Included 365 technical support and help desk
- NPC backup of all 365 files

Recap

Hybrid Work From Anywhere

- Consider the Three Pillars of Risk Governance:
 - Policy, Training, Technology
- Embrace a small footprint, secure-cloud strategy
- Consider the power of Microsoft 365 integrated products to enable your team

**Secure Work From Anywhere Can Enable Your Team,
and Protect Your Business**



Additional Resources

NPC Solutions

Secure managed computers and Microsoft 365 for the professional and SMB office.



- NPC Secure Managed Computers
 - Hardware, encryption, backup, system software, security, technical support, managed and monitored for you
- NPC Managed Microsoft 365
 - SharePoint, Exchange Email, Teams, and a host of productivity tools
- Dedicated Account Manager
 - A custom and consultative approach

NPC Webinars Recordings



npcdataguard.com/webinars

[Enhancing Password Security and the Power of MFA](#)

[Building an Incident Response Plan for the SMB](#)

[Protecting Your Identity Online](#)

[10 Steps to Secure Your Business from Ransomware](#)

& more, and new topics will be added

Upcoming NPC Webinars



npcdataguard.com/webinars

September 15th
1:00 PM ET (30 mins)

NPC DataGuard Solutions Overview

September 22nd
1:00 PM ET (60 mins)

Joint webinar with SideDrawer

How 'Office of the Future' and Secure Document Management Can Protect and Improve Your Business

October 18th
1:00 PM ET (60 mins)

How to Protect Your Business from Email Compromise Attacks

NPC Security Alerts



npcdataguard.com/alerts

What the Log4j Vulnerability Means for SMB Professionals



NPC Security Alerts



2021-12-21

[EXTERNAL - Use caution when opening attachments or links.]

[Préférez-vous voir ce courriel en Français?](#)

NPC Security Alerts



What the Log4j Vulnerability Means for SMB Professionals

A major security flaw in an application used by programmers to record activities for applications and software in devices and various services is making the headlines. National cybersecurity agencies and experts are calling for urgent action after it was reported last week.

Log4j is a component of software that developers use to record activities in an application. It is used in millions of Java applications and when located by hackers it can be exploited with relative ease. Hence, it has received a very high threat rating.

Q&A

Darren Mar

dmar@npcdataguard.com

905-305-6513

May-May Ogoigbe

mogoigbe@npcdataguard.com

905-305-6530



Thank You

Please Be Safe & Stay Healthy



NPC[™]
Smarter Computing