



Using Zero Trust to Protect Intellectual Property in M&E

Introduction

Using Zero Trust to Protect Intellectual Property in M&E

Intellectual property (IP) protection is vital to your bottom line. A leaked script, clip or game design can be disastrous to the success of any project. While today's collaboration tools have made it easier than ever to exchange ideas and information—it's also all too easy for deliberate and accidental data leakage to occur.

Learn how applying a Zero trust methodology to data access and sharing can help safeguard your most vital assets and ensure they don't accidentally or deliberately walk out the door.

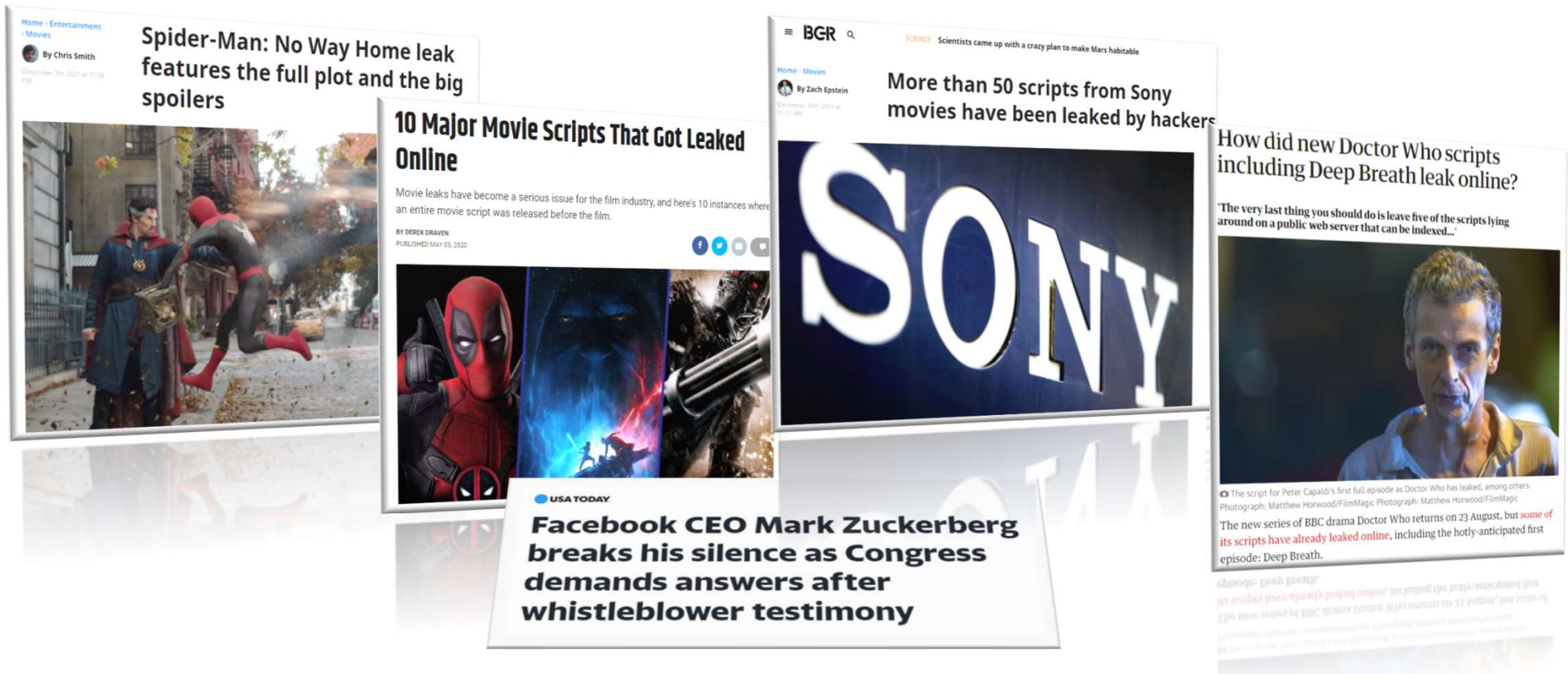
Agenda

- IP Theft in M&E Facts & Figures
- Remote Work & Collaboration Tool Impact on Data Loss
- Extending Zero Trust Principles to Data Access and Collaboration
- NC Protect Intro



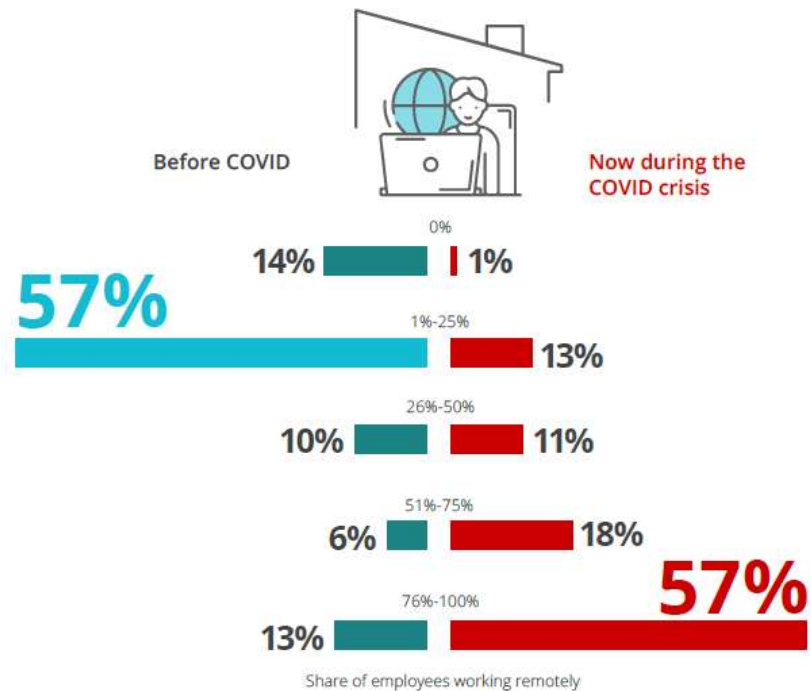
IP Theft Costs a Total US\$1 Trillion Per Year

More than half (51%) of media and entertainment firms experienced three or more cyber attacks over a 12-month period.*



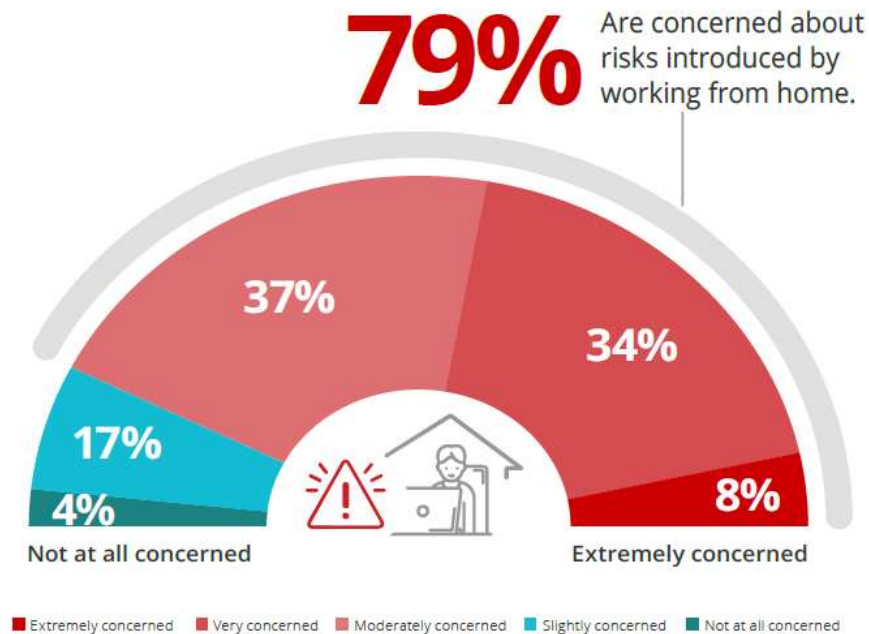
COVID19 Has Changed the Global Workforce

► What percentage of your workforce is working remotely/at home NOW during the COVID crisis compared to before (on average)?

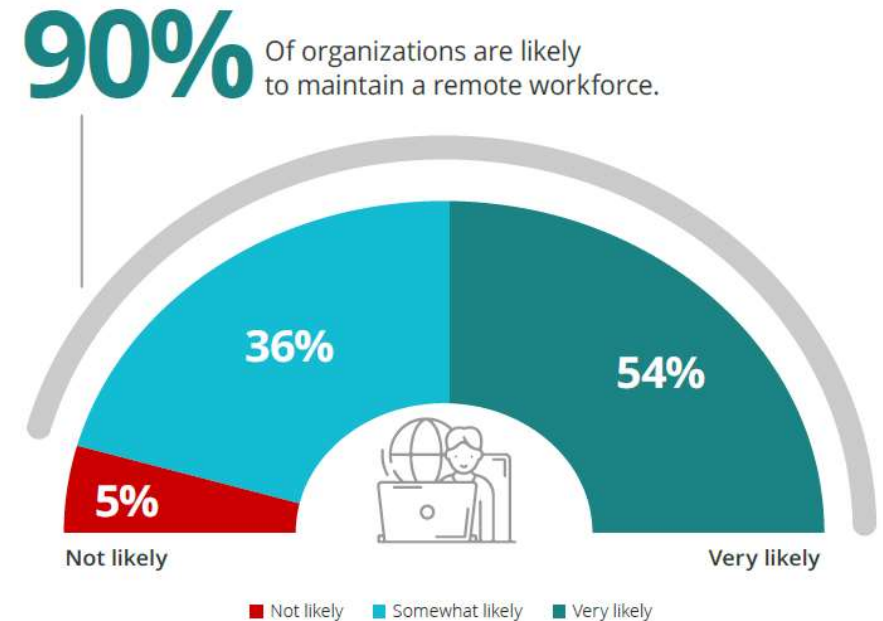


Remote Work Benefits Outweigh the Risk

► How concerned are you about the security risks introduced by users working from home?



► Do you expect to continue to support increased work from home capabilities in the future (due to increased productivity and other business benefits)?



Applications of Most Concern

► What work applications used by remote workers are you most concerned about from a security perspective?



68%

File sharing



47%

Web applications



45%

Video conferencing



35%

Messaging



27%

Social media

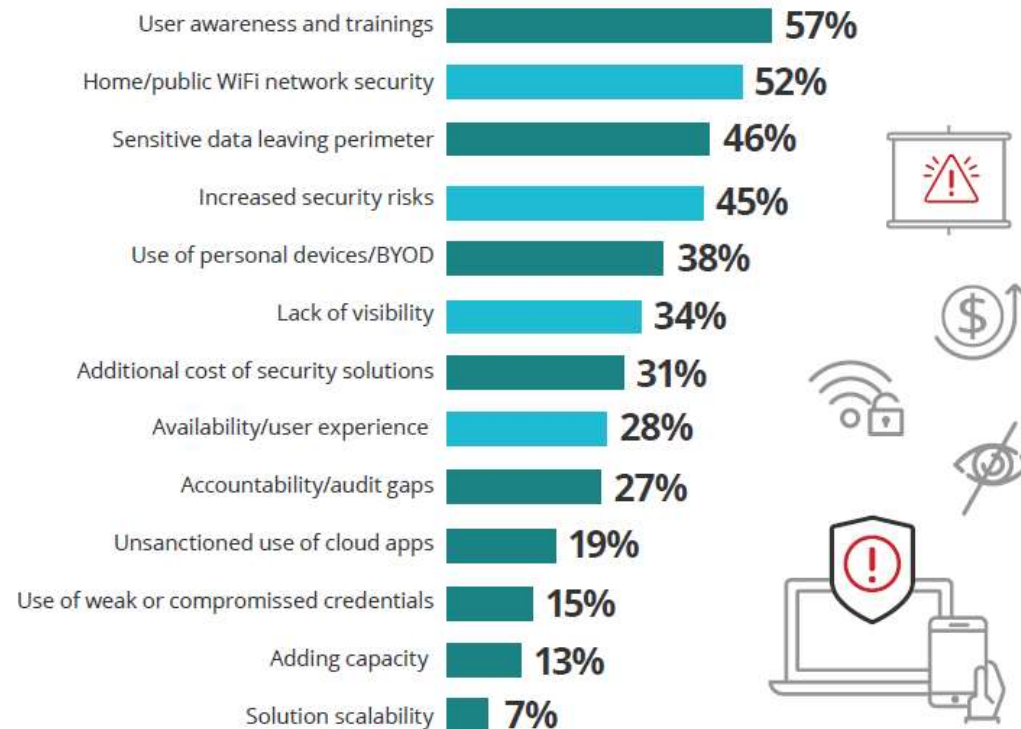


26%

Websites

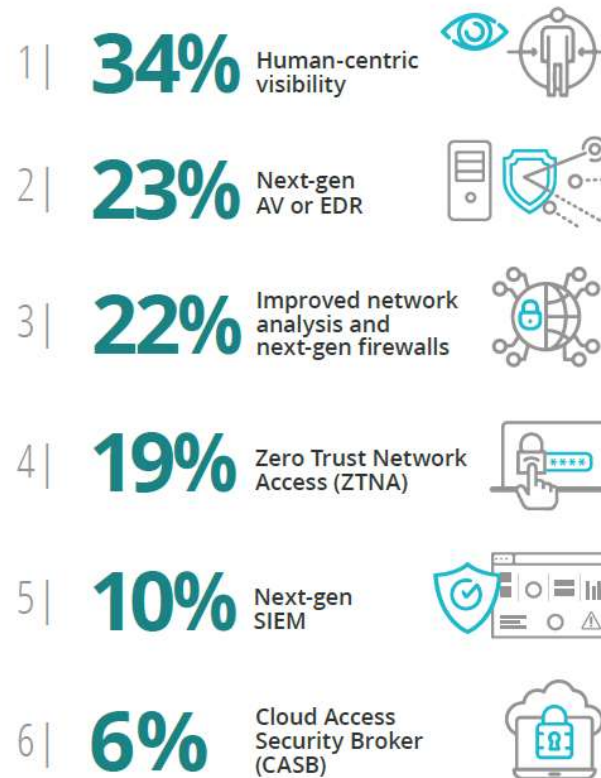
Top Security Challenges Identified

► What would you consider your organization's biggest security challenge regarding increasing the remote workforce?



Technologies Used to Combat the Risks

► Please rank the importance of the following cyber technologies to protect the organization from these new threat vectors?



And don't forget human error...

- Personal Information (PII) sent to wrong recipient (email or other)
- Unauthorized disclosure (unintended release or publication)
- Failure to use BCC when sending email
- Unauthorized disclosure (failure to redact)



Zero Trust & Data Security

Extending the methodology to
Data Access



What is Zero Trust?



The strategy around Zero Trust boils down to don't trust anyone.

We're talking about, 'Let's cut off all access until the network knows who you are.'

Don't allow access to IP addresses, machines, etc. until you know who that user is and whether they're authorized.

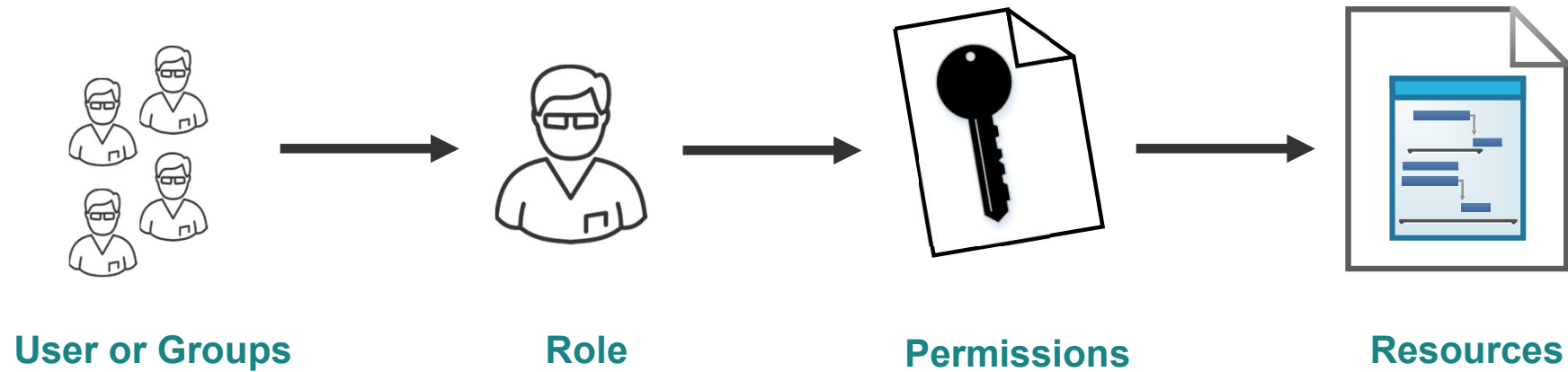
Charlie Gero, CTO of Enterprise and Advanced Projects Group at Akamai Technologies



Never Trust, Always Verify



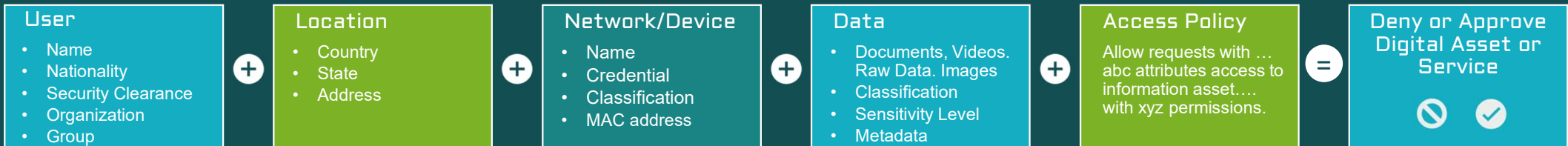
Traditional Role Based Access Control (RBAC)



Attribute-based Access Control (ABAC)

Security is built around the combination of User, Environmental and Resource attributes

Any Attributes + Policy = Conditional Access



Sensitivity: Confidential
Location: Office
Approve Access

✓

Sensitivity: Confidential
Location: Airplane
Deny Access

✗

The logo for NCPROTECT, featuring the word "NCPROTECT" in a white, sans-serif font with a trademark symbol. The letter "N" is highlighted in a light blue color. The logo is positioned on a dark grey background with a pattern of faint, overlapping hexagons. A bright blue chevron shape points from the logo towards the right side of the slide.

NCPROTECT™

Zero Trust Data Access
to Dynamically
Secure Collaboration

What We Solve

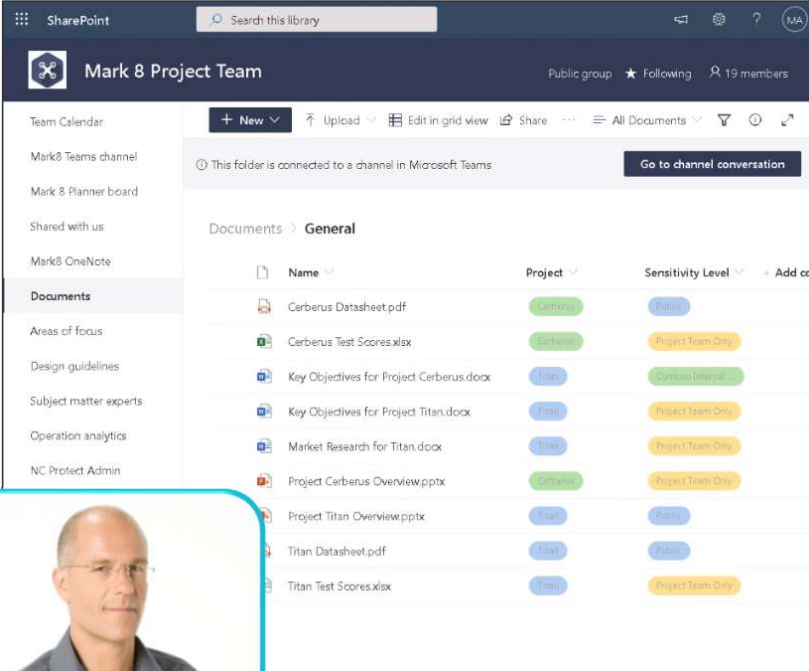
1. Who should have access to data
2. What users should be able to do with it once they have access

Key Capabilities

- Provides dynamic, real-time data-centric protection
- Limits access based on both user and file context
- Controls file usage and sharing rights
- Uses existing MIP sensitivity labels
- Adds Personalized Security Watermarks
- Forces Secure Read-Only Viewing
- Time limits access to data
- Build smart Information Barriers between workgroups, contractors, etc.



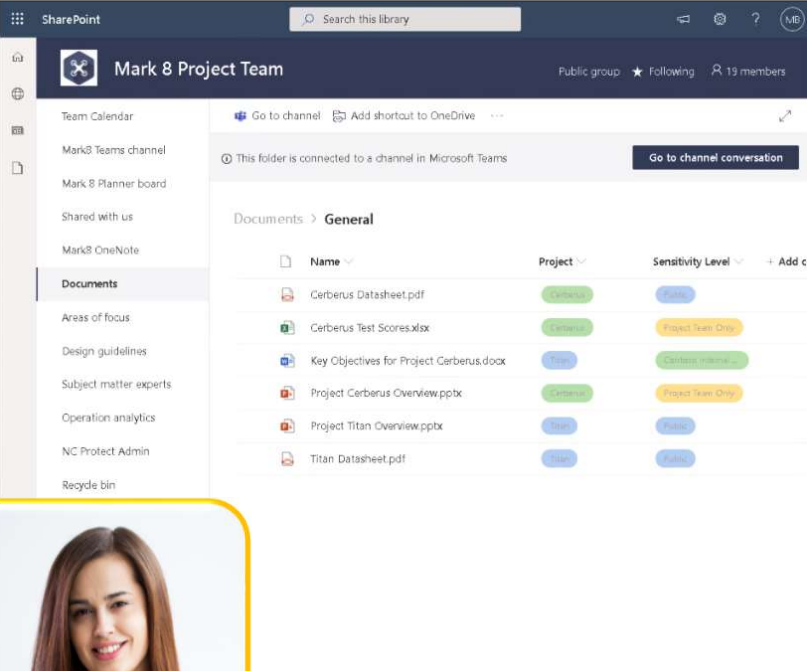
Proactively Control SharePoint Collaboration with Dynamic Rules



The screenshot shows the SharePoint interface for the 'Mark 8 Project Team' public group. The 'Documents' list is visible, showing files with their respective project and sensitivity levels. The user has full access and editing rights.

Name	Project	Sensitivity Level
Cerberus Datasheet.pdf	Cerberus	Public
Cerberus Test Scores.xlsx	Cerberus	Project Team Only
Key Objectives for Project Cerberus.docx	Titan	Cerberus Internal
Key Objectives for Project Titan.docx	Titan	Project Team Only
Market Research for Titan.docx	Titan	Project Team Only
Project Cerberus Overview.pptx	Cerberus	Project Team Only
Project Titan Overview.pptx	Titan	Public
Titan Datasheet.pdf	Titan	Public
Titan Test Scores.xlsx	Titan	Project Team Only

Internal User

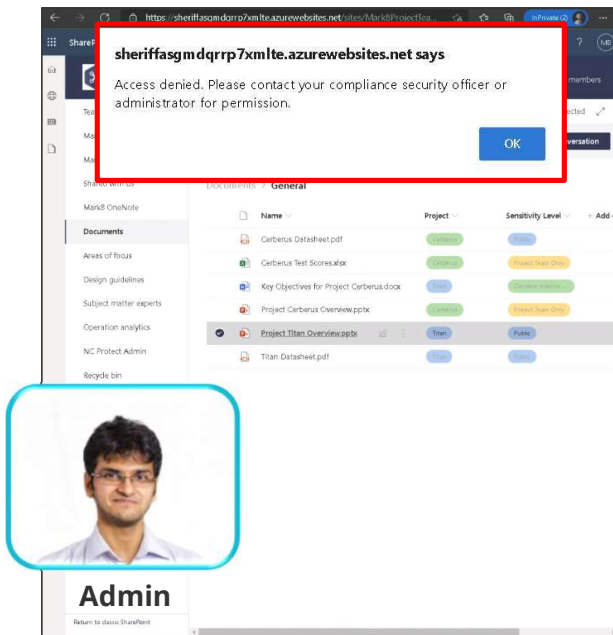


The screenshot shows the SharePoint interface for the 'Mark 8 Project Team' public group. The 'Documents' list is visible, showing files with their respective project and sensitivity levels. The user has limited access, and sensitive data is trimmed out.

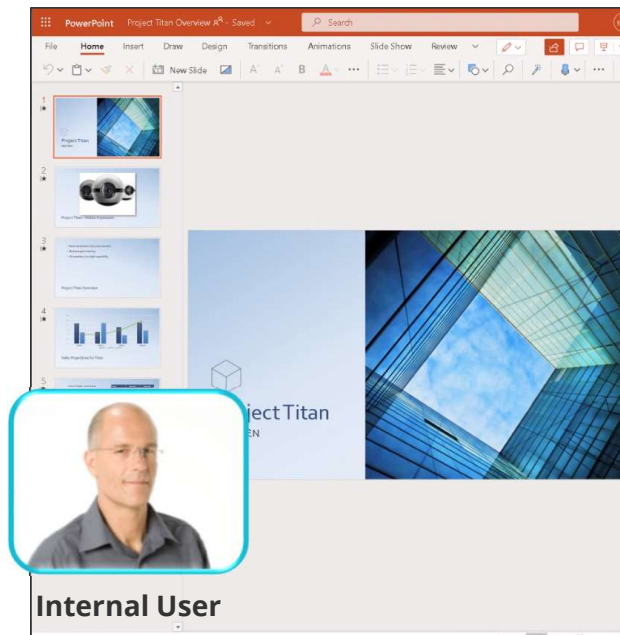
Name	Project	Sensitivity Level
Cerberus Datasheet.pdf	Cerberus	Public
Cerberus Test Scores.xlsx	Cerberus	Project Team Only
Key Objectives for Project Cerberus.docx	Titan	Cerberus Internal
Project Cerberus Overview.pptx	Cerberus	Project Team Only
Project Titan Overview.pptx	Titan	Public
Titan Datasheet.pdf	Titan	Public

Guest User

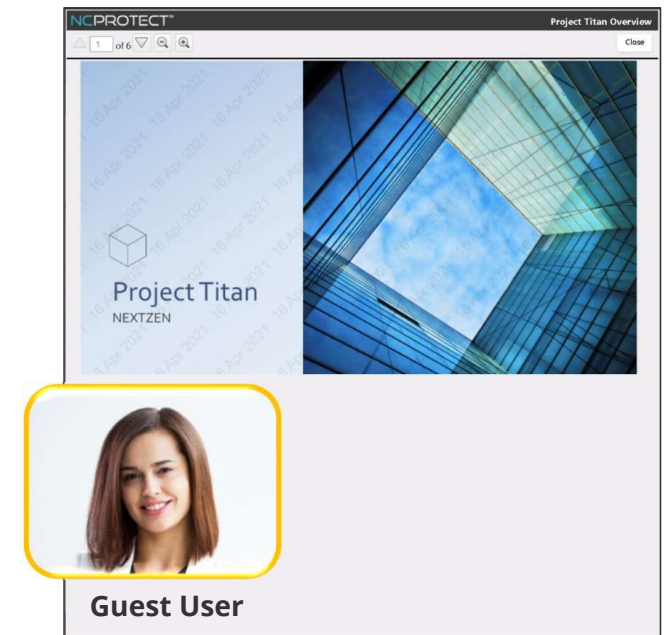
Proactively Control SharePoint Collaboration with Dynamic Rules



Can see file exists,
can't read content



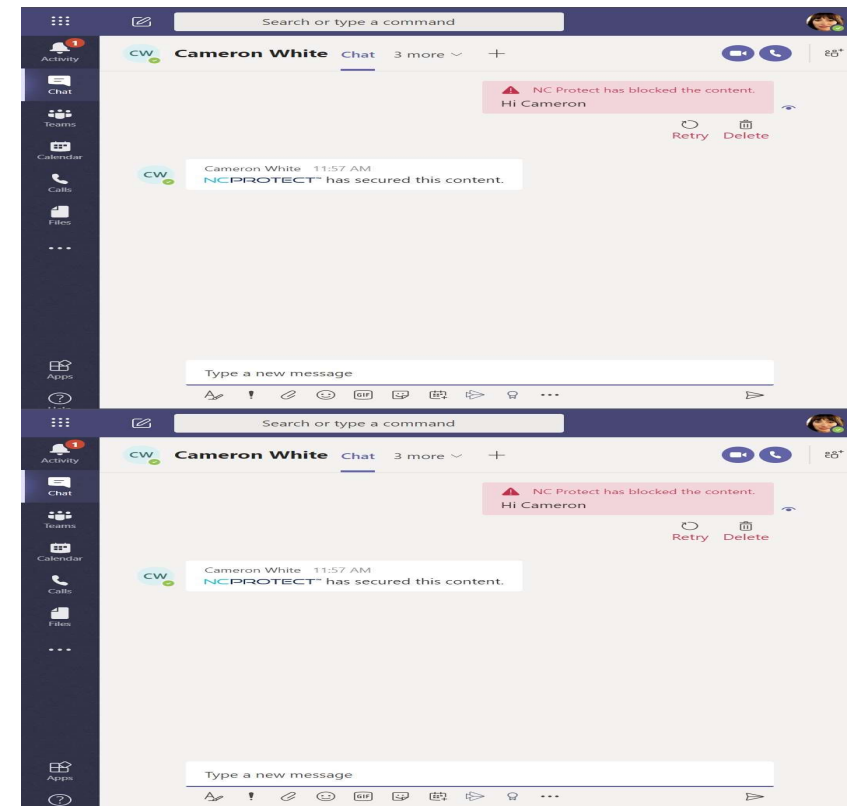
Full access & editing rights



Secure read-only access with
security watermark

Proactively Control Microsoft Teams Collaboration with Built-in Rules

- Dynamic Information Barriers
- Protect file & chat content in Teams
- Control guest access
- Set channel security
- Archive a channel or chat as read-only
- Retroactively remove access in chat history
- Apply the same policies to the SharePoint sites beneath Teams



Applying Zero Trust Access with NC Protect



Sensitivity: Confidential

Location: Home Office

Device: Secure Laptop



Sensitivity: Confidential

Location: Coffee Shop

Device: Cell Phone



Scalable - Secure ALL Your Collaboration With a Single Solution



SHAREPOINT



TEAMS



YAMMER



ONEDRIVE



EXCHANGE



WINDOWS
FILE SHARES



DROPBOX



NUTANIX
FILES

The NC Protect Difference – Simple. Fast. Scalable.

SIMPLE



Manage information protection without the complexity of native tools

FAST



Automatically apply information protection to content, teams and sites

SCALABLE



Extensible across Office 365 apps, SharePoint on-premises, Windows file shares, Dropbox and Nutanix Files



“Secure collaboration is always a top priority for our customers, and Nucleus Cyber’s integrations can help customers with highly sensitive data to ensure it remains protected as it is shared through the collaboration lifecycle.”

Ryan McGee
Security Product Marketing,
Microsoft Corp

Member of
Microsoft Intelligent
Security Association




Nucleus Cyber has become the best product for securing unstructured information that provides coverage for data and files moving in and out of various Microsoft apps, namely O365, SharePoint, OneDrive, Teams and Exchange. Microsoft has nothing like it, and the granular flexibility NC Protect provides is unmatched.

Robert MacMillan
Head of Cyber Security
Virgin Mobile





Questions

Dave Matthews
Technical Solutions Manager
dave.matthews@archtis.com