Using Zero Trust to Protect Intellectual Property in M&E

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.*

Home › Entertainment › Movies

By Chris Smith

December 7th, 2021 at 11:26 PM

Spider-Man: No Way Home leak features the full plot and the big spoilers

10 Major Movie Scripts That Got Leake Online

Movie leaks have become a serious issue for the film industry, and here's 10 instar an entire movie script was released before the film.

BY DEREK DRAVEN

PUBLISHED MAY 05, 2020

BGR

SCIENCE Scientists came up with a crazy plan to make Mars habitable

Home › Movies

By Zach Epstein

December 18th, 2014 at 11:31 AM

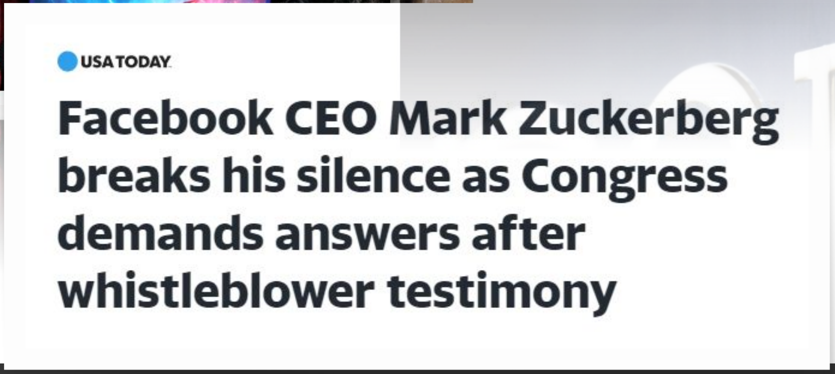
More than 50 scripts from Sony movies have been leaked by hackers

How did new Doctor Who scripts including Deep Breath leak online?

'The very last thing you should do is leave five of the scripts lying around on a public web server that can be indexed...'

The script for Peter Capaldi's first full episode as Doctor Who has leaked, among others. Photograph: Matthew Horwood/FilmMagic Photograph: Matthew Horwood/FilmMagic

The new series of BBC drama Doctor Who returns on 23 August, but some of its scripts have already leaked online, including the hotly-anticipated first episode: Deep Breath.



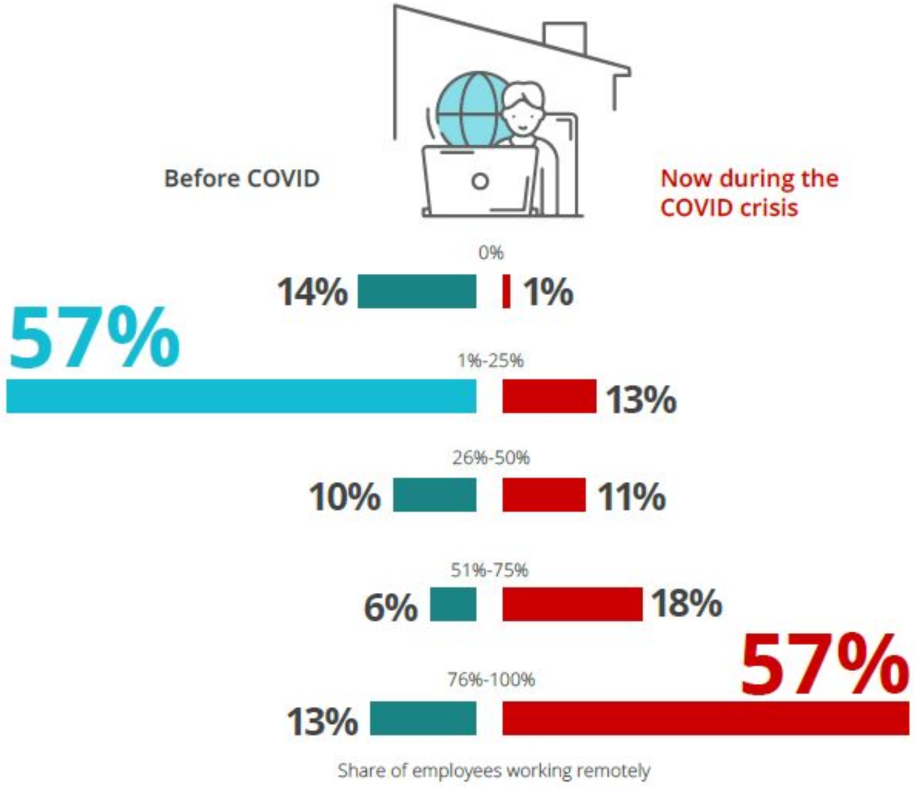
USA TODAY

Facebook CEO Mark Zuckerberg breaks his silence as Congress demands answers after whistleblower testimony

*Forrester Consulting survey commissioned by Hiscox

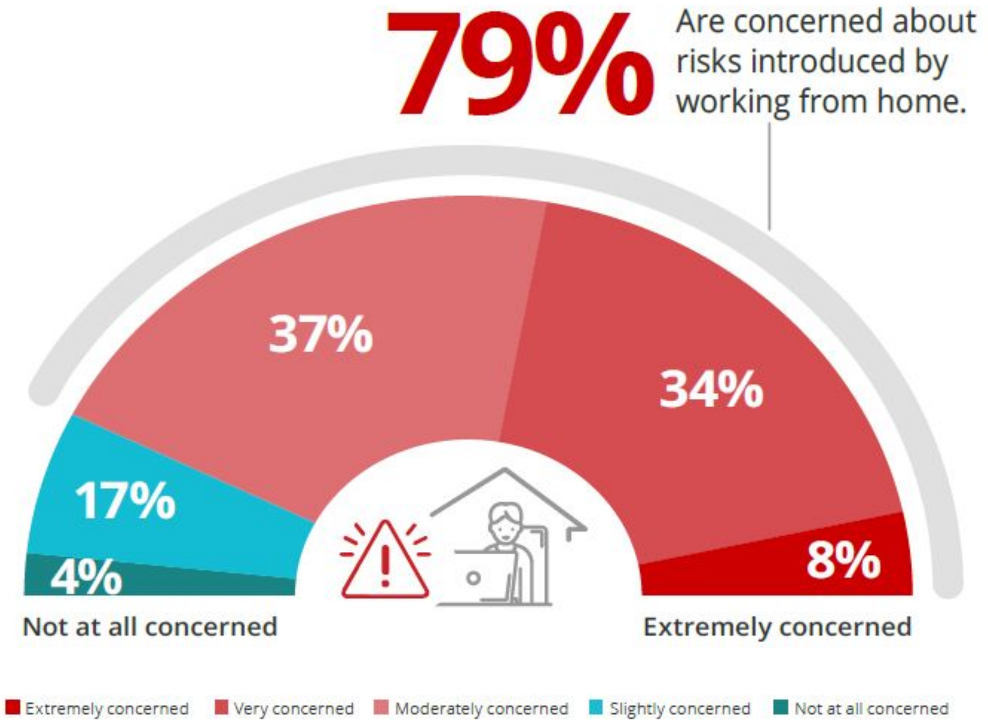
COVID19 Has Changed the Global Workforce

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



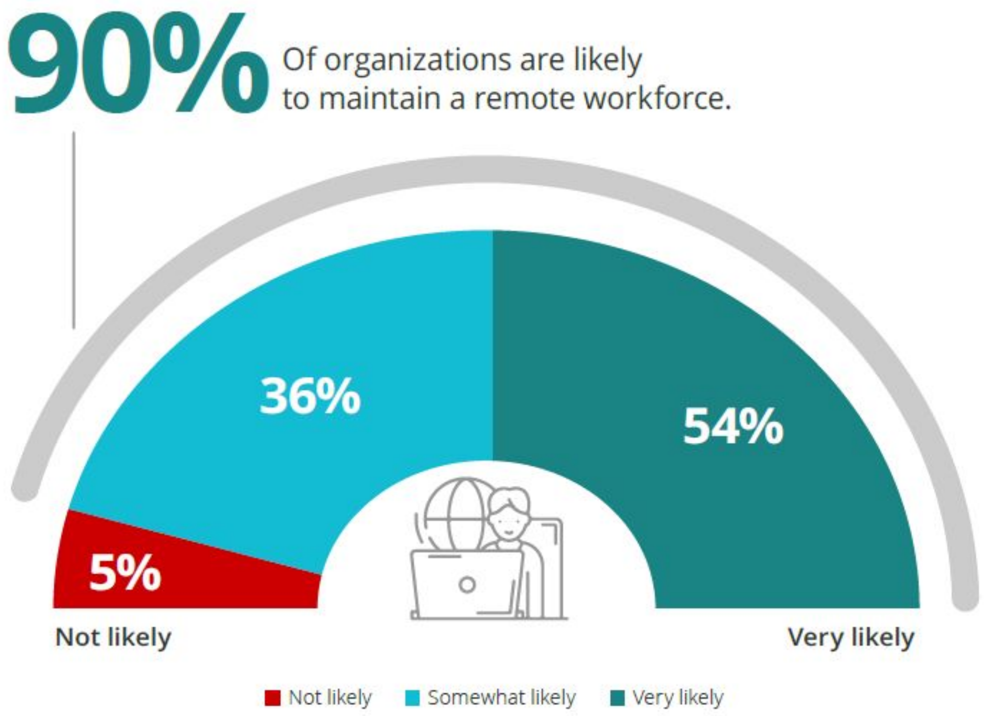
Remote Work Benefits Outweigh the Risk

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



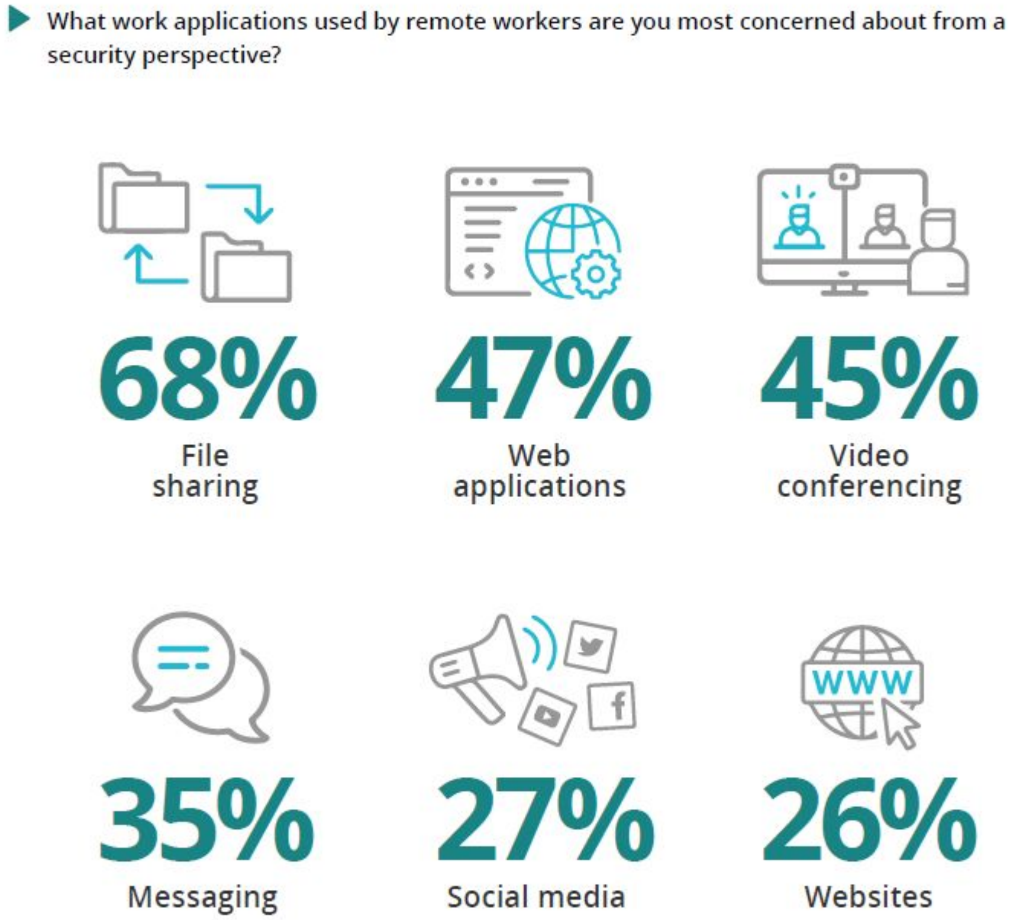
79% Are concerned about risks introduced by working from home.

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



90% Of organizations are likely to maintain a remote workforce.

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

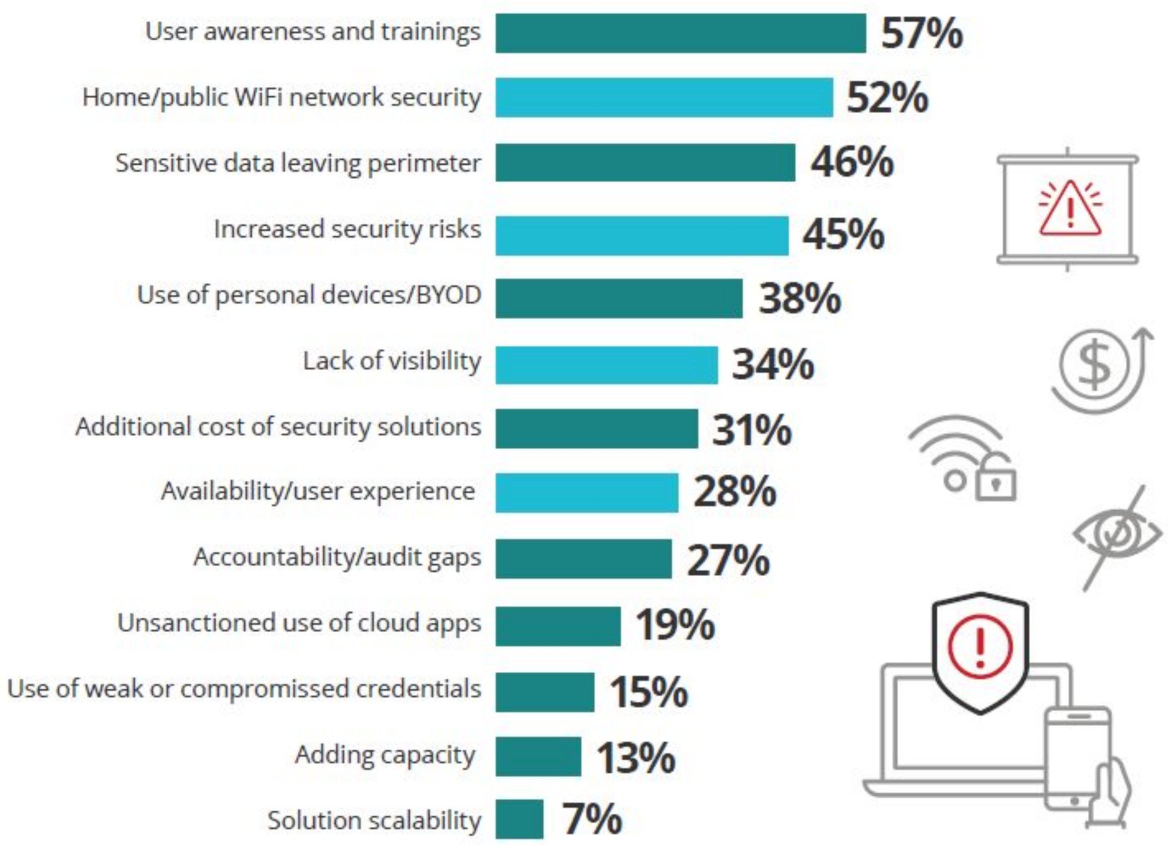
35%
Messaging

27%
Social media

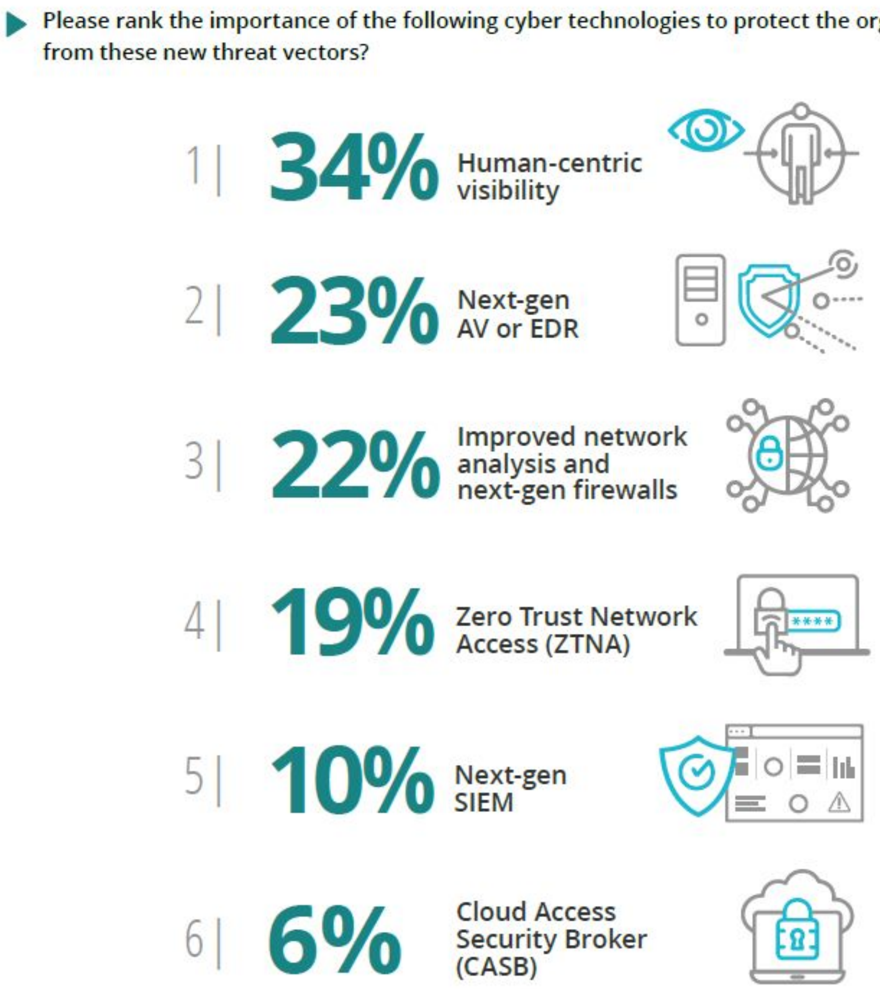
26%
Websites

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?

1| **34%** Human-centric visibility

2| **23%** Next-gen AV or EDR

3| **22%** Improved network analysis and next-gen firewalls

4| **19%** Zero Trust Network Access (ZTNA)

5| **10%** Next-gen SIEM

6| **6%** Cloud Access Security Broker (CASB)

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)

Office of the Australian Information Commissioner (OAIC) bi-annual Notifiable Data Breaches Report: July–December 2020

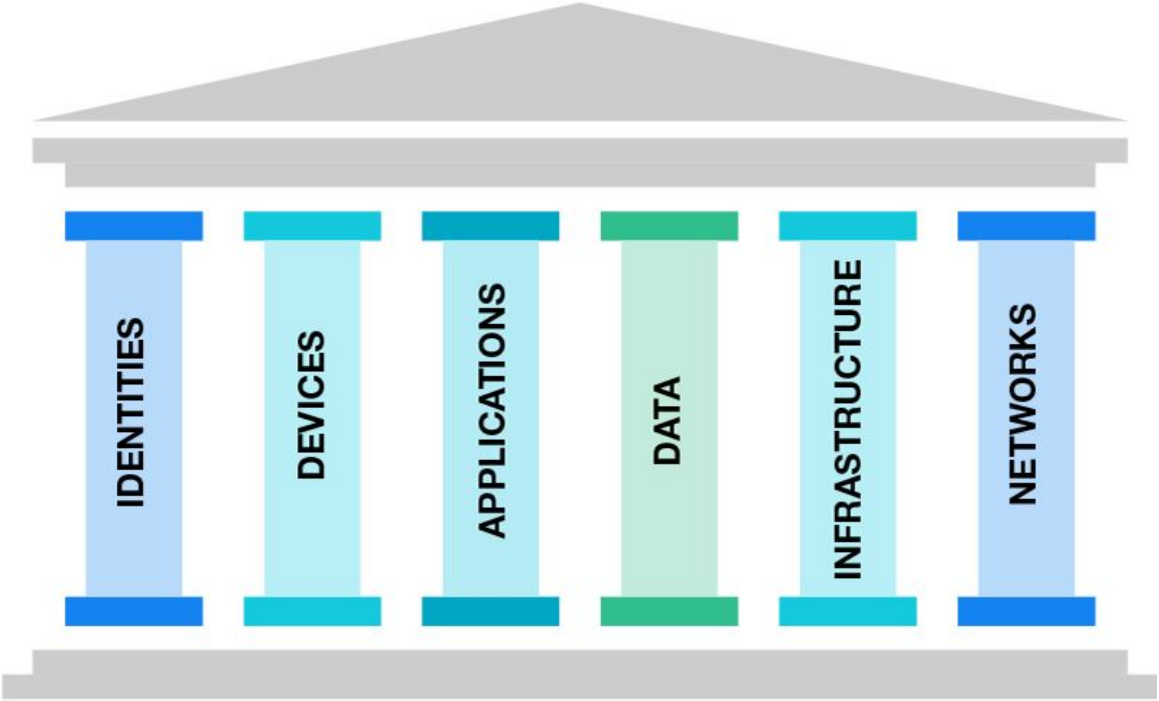
Zero Trust & Data Security

Extending the methodology to Data Access

Data-Centric Zero Trust

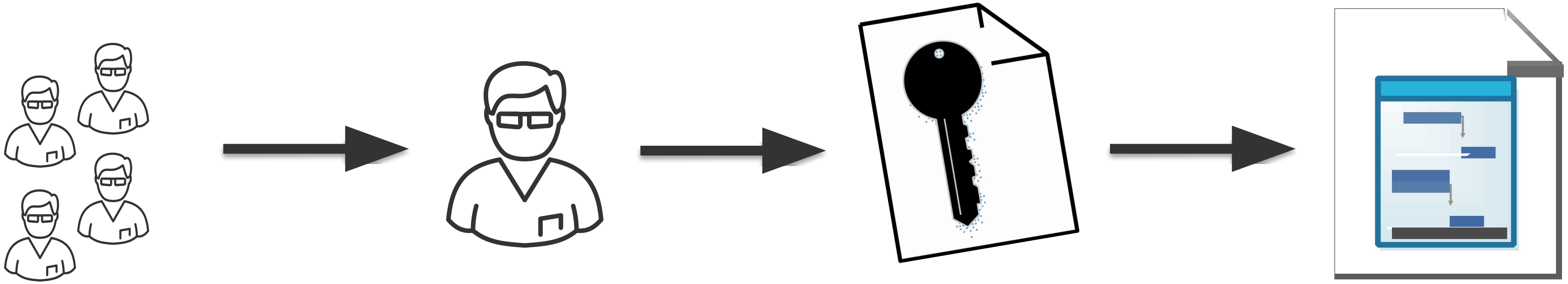
The Zero Trust Methodology: Trust no one, verify everything

- Six Foundational Pillars
  - **Identities** may be users, services or devices
  - **Devices** create a large attack surface as data flows
  - **Applications** are the way that data is consumed
  - **Networks** should be segmented
  - **Infrastructure** whether on-premises or cloud-based, represents a threat vector
  - **Data** should be classified, labelled and encrypted based on its attributes



VERIFY EXPLICITLY | LEAST PRIVILEGED ACCESS | ASSUME BREACH

Traditional Role Based Access Control (RBAC)



User or Groups

Role

Permissions

Resources

Attribute-based Access Control (ABAC)

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

Any Attributes + Policy = Conditional Access

User
- Name
- Nationality
- Security Clearance
- Organization
- Group

+

Location
- Country
- State
- Address

+

Network/Device
- Name
- Credential
- Classification
- MAC address

+

Data
- Documents, Videos. Raw Data. Images
- Classification
- Sensitivity Level
- Metadata

+

Access Policy

Allow requests with … abc attributes access to information asset…. with xyz permissions.

=

Deny or Approve Digital Asset or Service

⊘ ✓

Sensitivity: Confidential

Location: Office

Approve Access

✓

Sensitivity: Confidential

Location: Airplane

Deny Access

✗

NCPROTECT™

Zero Trust Data Access to Dynamically Secure Collaboration

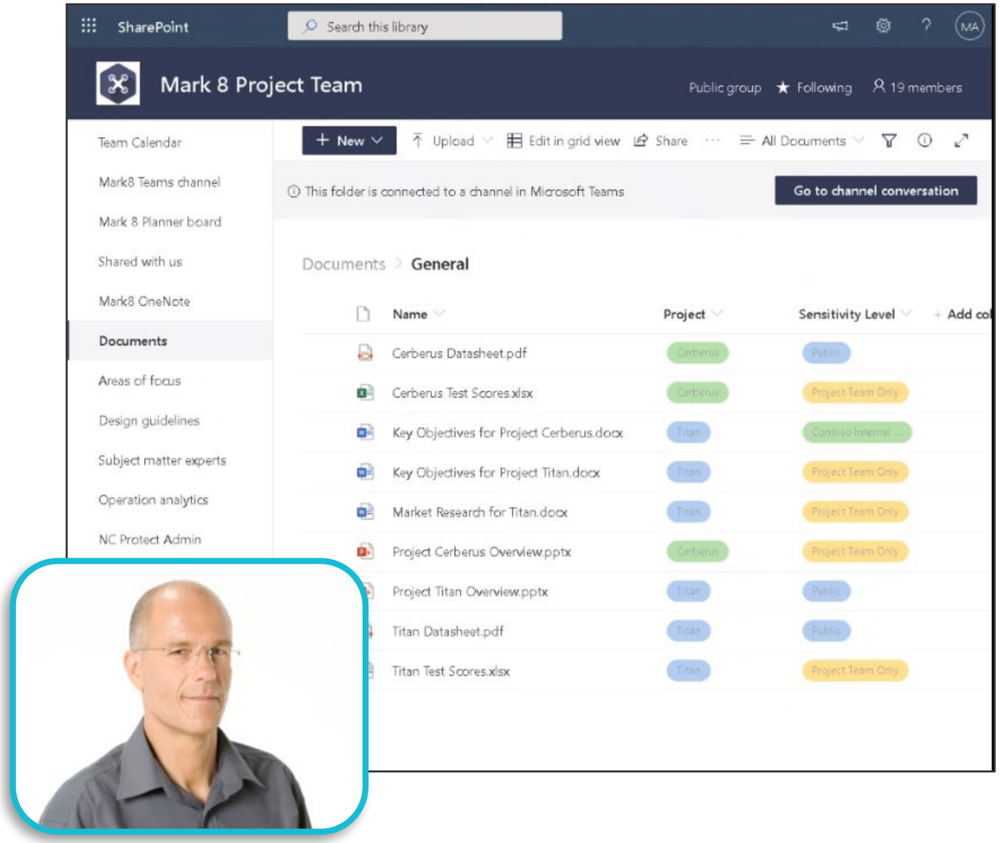
What We Solve

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

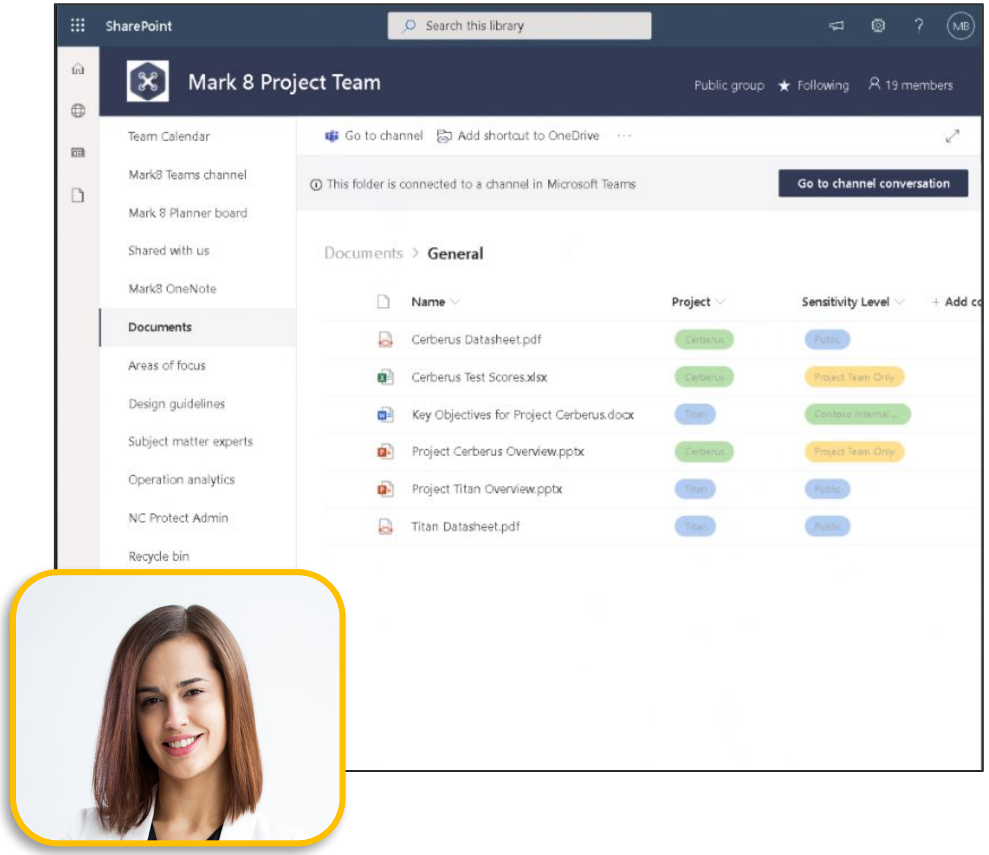


This folder is connected to a channel in Microsoft Teams

Documents > General

Name	Project	Sensitivity Level	+ Add col
Cerberus Datasheet.pdf	Cerberus	Public	
Cerberus Test Scores.xlsx	Cerberus	Project Team Only	
Key Objectives for Project Cerberus.docx	Titan	Contoso 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



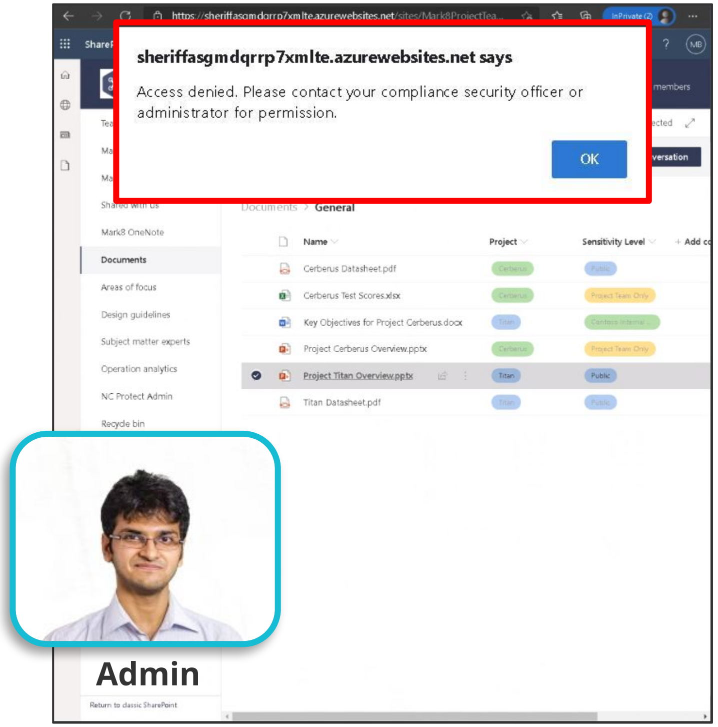
This folder is connected to a channel in Microsoft Teams

Documents > General

Name	Project	Sensitivity Level	+ Add c
Cerberus Datasheet.pdf	Cerberus	Public	
Cerberus Test Scores.xlsx	Cerberus	Project Team Only	
Key Objectives for Project Cerberus.docx	Titan	Contoso 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



sheriffasgmdqrrp7xmlte.azurewebsites.net says

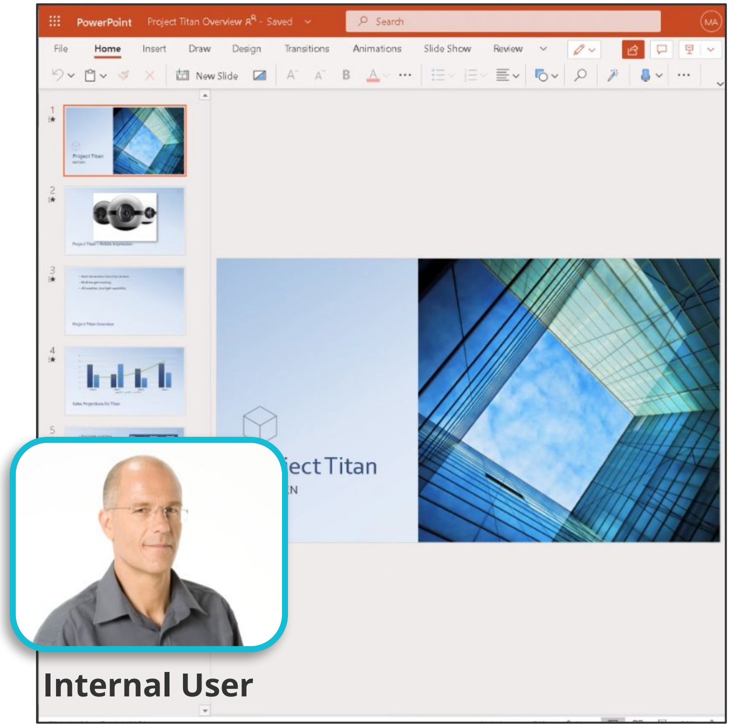
Access denied. Please contact your compliance security officer or administrator for permission.

OK

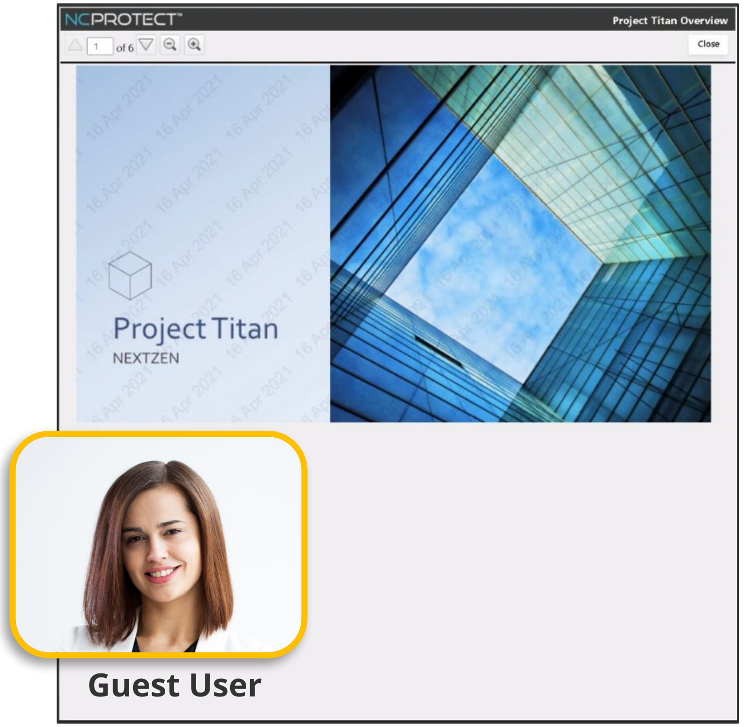
Documents > General

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

Can see file exists, can't read content



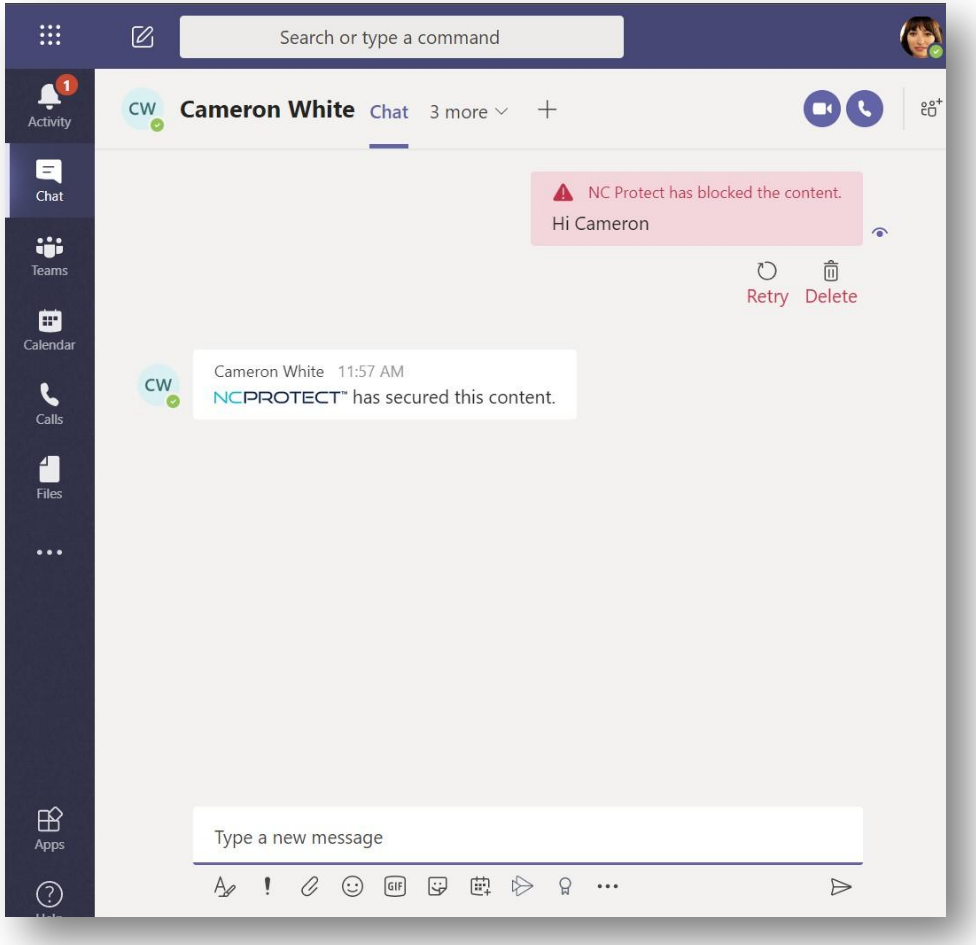
Full access & editing rights



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



NC Protect has blocked the content.

Hi Cameron

Cameron White 11:57 AM

NCPROTECT™ has secured this content.

Applying Zero Trust Access with NC Protect

Location: Home Office

Device: Secure Laptop

Sensitivity: Confidential

✓

Location: Conference Centre

Device: Mobile Phone

Sensitivity: Confidential

✗

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
Microsoft

> 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**

Virgin mobile

archTIS

Thank You

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