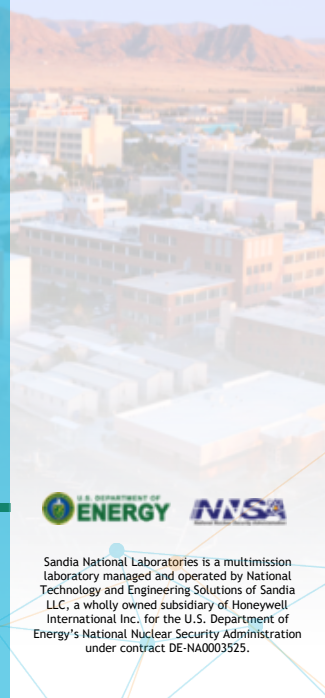
SAND2022-12677C

Sandia National Laboratories

Sandia's Journey to O365– How we moved SNL's first enterprise IT services to the cloud

PRESENTED BY

Sandia National Labs, Enterprise Collaboration Services



U.S. DEPARTMENT OF ENERGY | NNSA

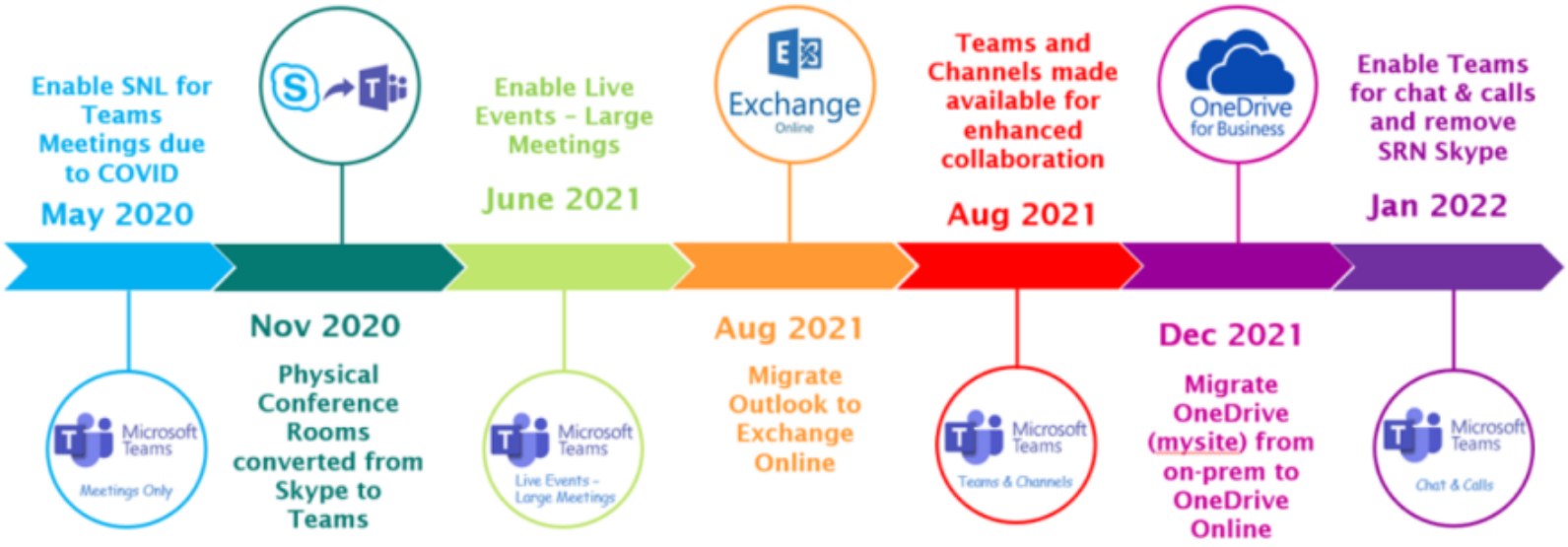
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Agenda

- What We Have Done so Far
- Security Approvals
- Building Blocks and Technical Challenges
- Cloud Agility
- Challenges Operating in the Cloud
- Security and Operational Advantages
- What's coming....
- Q/A

What have we done in O365 so far …



Fun Facts!

- **NNSA mandated that we move our email to the cloud.**
- **We were planning to migrate email first "Exchange Online" prior to COVID. We had to rapidly get Teams ready to keep the communication and collaboration going. Our MOW couldn't use their cameras at the start of COVID.**
- **We migrated 130 TB of email data, 9 months of migration work, 17K mailboxes, in 32 batches/bricks and nearly 1 Billion email records. We went from 5GB mailboxes to 100GB mailboxes.**
- **We migrated over 17K users and 1.75 TB of data to OneDrive Online. Expanded storage capacities from 150GB max to 25 TB max per user.**

What have we done in O365 so far continued …

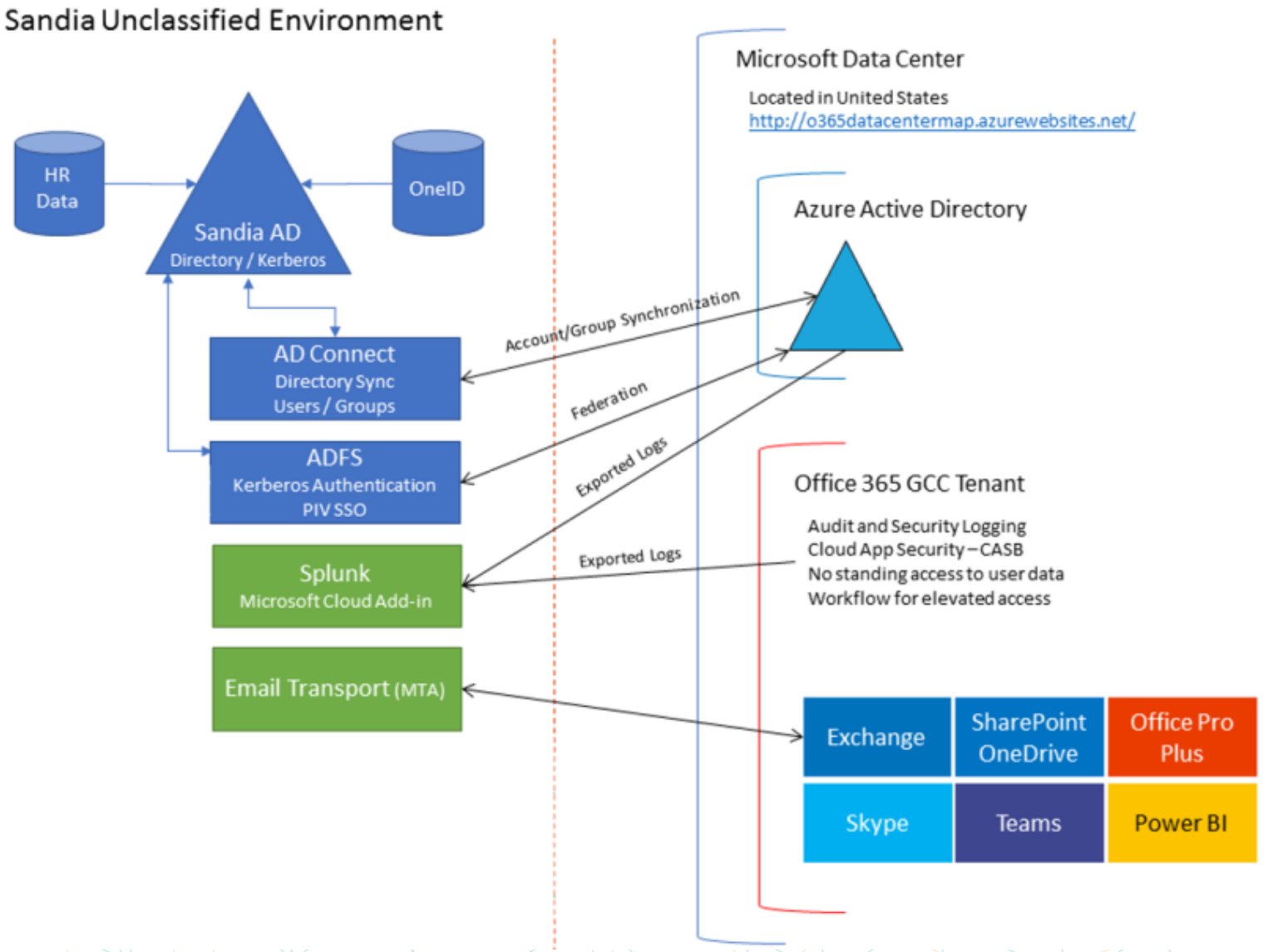
*SharePoint Online includes the Power Platform (PowerBI, Power Apps, Power Automate, and MS Lists). These capabilities will be used to develop new SRN based collaboration solutions and over this time period SRN and ECN solutions will be incrementally redeveloped in SharePoint Online.

Dates are subject to change

How we got security approval

- **Started security approvals in January 2018.**
- **Sandia had to get two Authorizations to Use – One for Azure and one for Office 365.**
- **Multiple year effort with collaboration including Microsoft, cyber, Sandia Field Office, and IT partners to research, develop and implement security controls needed to get the first approval of this kind.**
- **Understand detailed security requirements. We became very familiar with NIST!**
- **We added a dedicated ISSO and a project manager to our team.**
- **Approval is not yet finished. We are iterating through approvals for the various Office 365 solutions.**

What are the building blocks?



What have been the technical challenges?

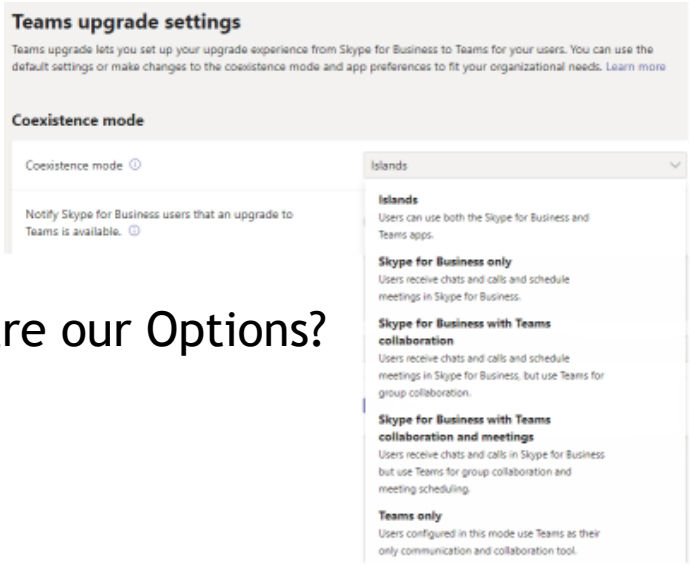
- **User Principal Name (UPN) updates** – all users' accounts previously had a UPN of <userid>@srn.sandia.gov. Sandia had to update all user accounts to have the format of <userid>@sandia.gov.
- **Account Provisioning** – Sandia's account provisioning services had to be updated to account for mailboxes having been migrated to Exchange Online.
- **Voicemail services** – Microsoft discontinued voicemail services from the Exchange Product both on-premises and in Exchange Online. As a result, Sandia had to migrate 12k+ user voicemail services from Exchange to Office IX
- **Forward Proxy Tenant Header configurations** – Due to Sandia's requirements to prevent access to other email services, Sandia needed to enact custom configurations to access to it's own o365 services, but prevent access to other o365 tenants.
- **Exchange Mailbox Migrations** – Over individual 30 issues were identified after a mailbox was migrated to Exchange Online. All show-stopping issues were resolved prior to migrations
- **Email client connectivity Authorization / Authentication** – By default, access to o365 services is very permissive. Access needed to be configured to grant access to o365 services from authorized devices and networks.

Cloud Agility – Skype & Teams

Pre-Covid Skype Infrastructure

Teams – Cloud Alternative

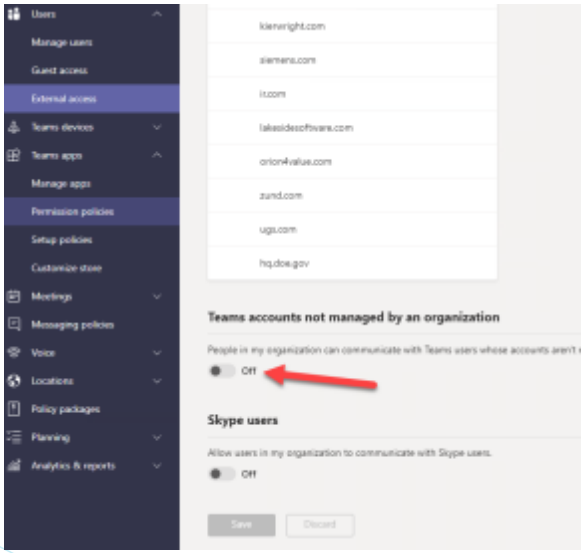
What are our Options?



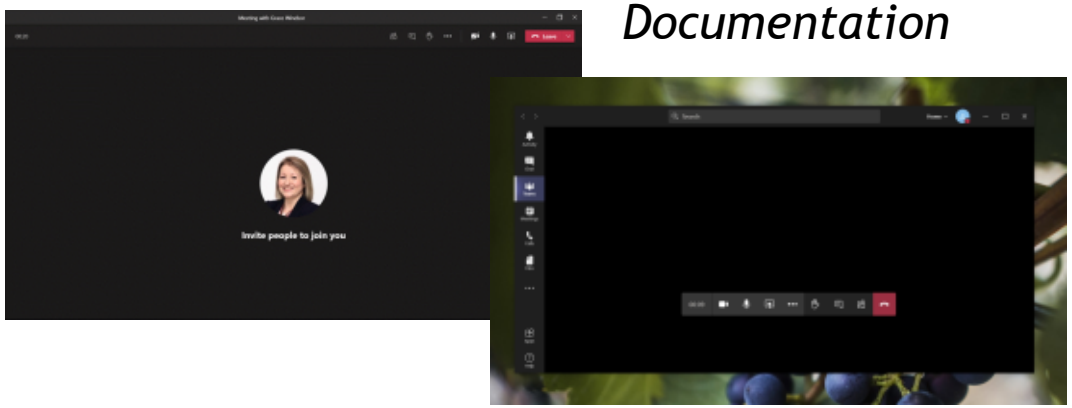
Rapid Deployment:
Teams Meetings Only

What are the Challenges in providing services via SaaS?

Controlling Changes



Documentation



Alerts and Outages

Microsoft 365 suite service alert

Incident information
Title: Users may experience intermittent access issues to multiple Microsoft 365 services
ID: MO305726

Status
Service Degradation

Microsoft 365 suite service alert

Incident information
Title: Users may experience intermittent access issues to multiple Microsoft 365 services
ID: MO305726

Status
False Positive

Microsoft

Exchange Online service alert

Advisory information
Title: We're looking into a potential problem
ID: EX301404

Status
Investigating

Details
Title: We're looking into a potential problem

User Impact: We're checking for potential impact to your users.

Current status: We're investigating a potential issue and checking for impact to your organization. We'll provide an update within 30 minutes.

Are you experiencing this issue?

Microsoft Intune service alert

Advisory information
Title: Devices not providing correct Mobile Application Management (MAM) reporting following MAM enrollment
ID: IT305678

Status
Service Restored

Security and Operational Advantages

- **Operational Activities**
  - Cyber, SIMP, Legal requests
  - custom scripts, processes
- **Cloud Tools**
  - Microsoft 365 Defender
  - Microsoft 365 Compliance
- **Advantages**
  - Built-in
  - Ease of Use
  - Custom development
- **Conclusion and the Future**
  - Much improved operational benefits
  - Future growth... Anti-Spam/Anti-Phishing

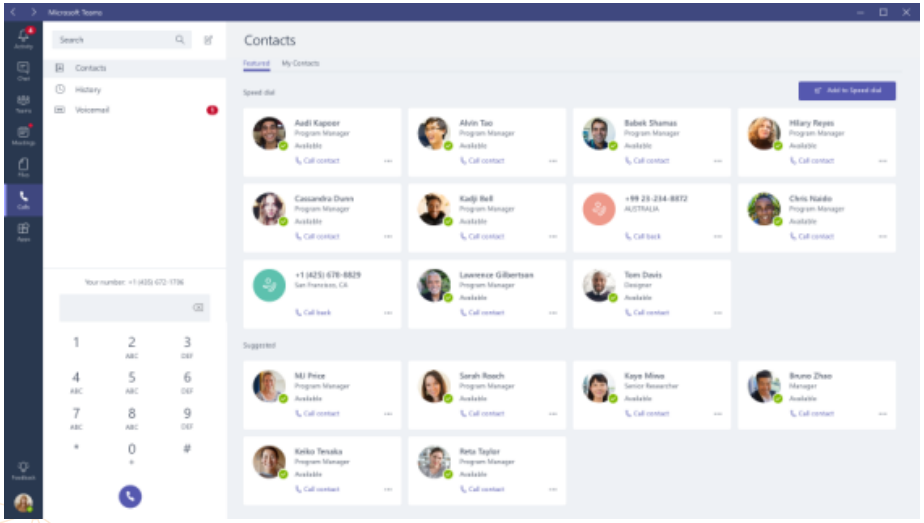
What's Next: SharePoint Online Migrations Path Forward

- Long-Term Effort completed by 2025
  - User Impact: URL Change, UI Changes, Digital Transformation, Feature Parity
  - Scope
    - ~ 6000 Site Collections, varying degrees of complexity
    - Significant Refactoring of Features, Applications, and Processes
- Categorized Sites based on Features, Risk, and Utilization
  - Unused Sites
  - Features that migrate cleanly ("Vanilla Sites")
  - Moderate Risk and/or Refactoring
  - Business Critical Sites
  - High Risk and/or Extensive Refactoring
- Beginning SPO Migration Pilot this FY
  - 7 sites w/Site Collection Administrator providing end user support
  - Test migration tools and processes
  - Better understanding of UX for transition
- Citizen Developers performing Early Testing (non-production)
- Next steps… focus on the Vanilla Sites w/no customization
  - Easy to migrate, less operational risk, more control over volume
- Roll in phases to more difficult sites with higher risk in parallel

What's Next : Teams Telephony & External Access

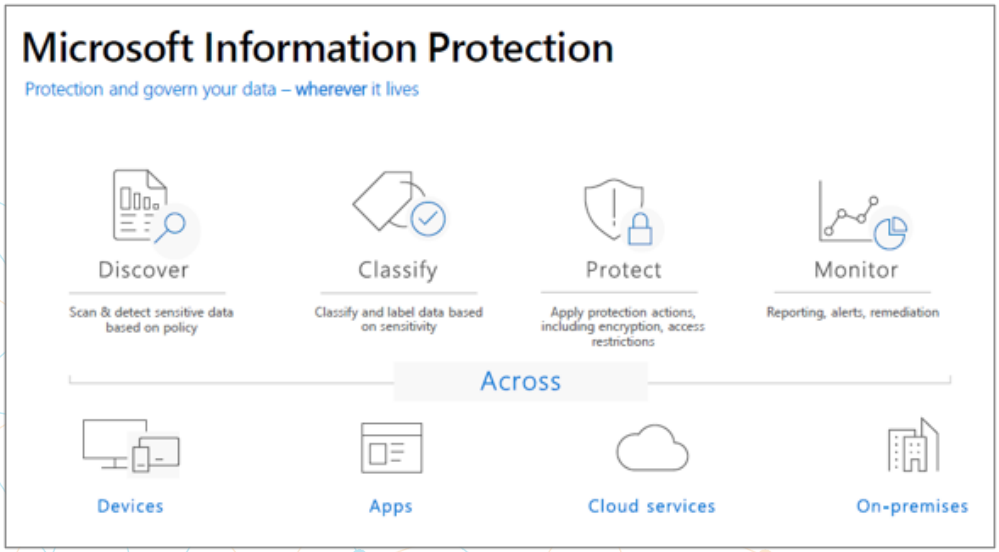
- External Access
  - Joint effort between O365 and Azure Teams
    - Azure Team manages Identity management and User Validation
    - O365 Team manages Access Packages Administration
  - Pilot in design phase, hoping to rollout broadly next CY

- Teams Telephony
  - Currently requesting Security Approvals, joint effort w/ Sandia's telephony team
  - Working on Pilot configuration
    - Dial plans for remote users to leverage dial-out capabilities
    - Working to Mitigate CNSSI 5000 Annex J in Secure Spaces
      - Physical Disconnect Devices



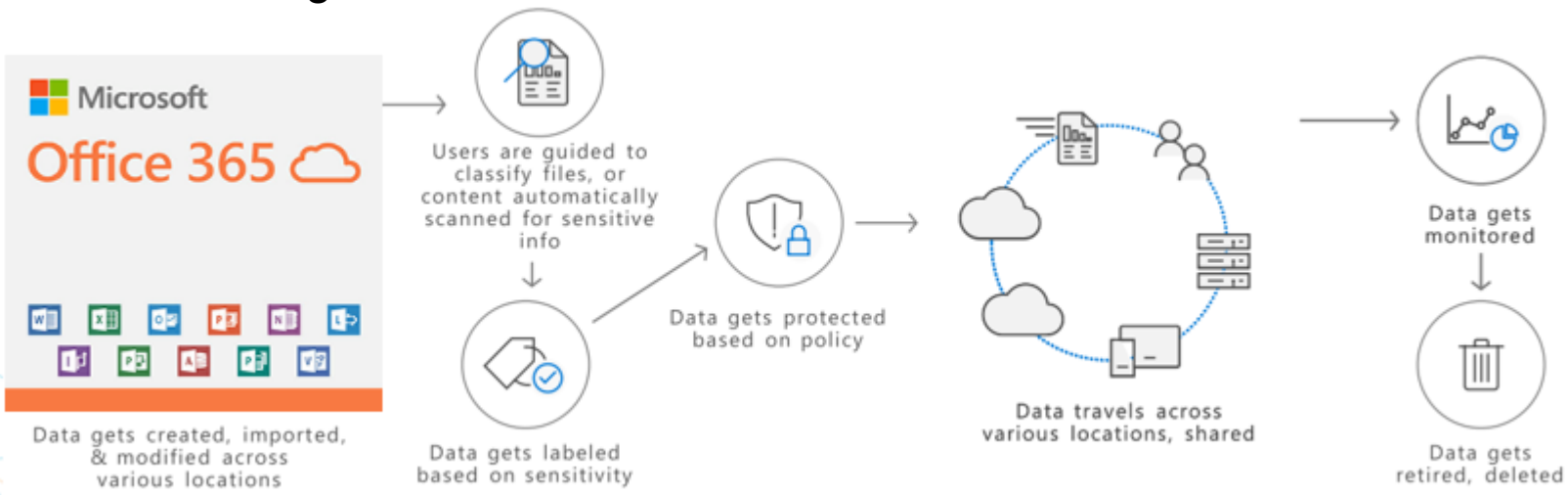
What's Next: Data Sensitivity, Labeling, and Information Protection

- Moving Toward a Zero Trust Architecture
- Challenges of separating from a network-boundary approach for protecting data (such as Export Controlled information)
- Address challenges for Foreign Nationals while ensuring compliance with contractual and legal obligations



What's Next: Data Protection

- Information Engineering's cross-departmental work on Sensitivity Labels that will appear throughout the Office suite of products.
- Aligns with Zero Trust Architecture
- Provide document level data protections in lieu of network-boundary or user managed access controls.



Using Azure Information Protection for Labeling

Pattern #1 — Low

Primary element
Keyword list: keyword_ouo-eci-header-footer

Character proximity
Detect primary AND supporting elements within unlimited characters

Pattern #2 — Medium

Primary element
Keyword list: keyword_ouo-eci-header-footer

Character proximity
Detect primary AND supporting elements within 1000 characters

Supporting elements
Dictionary (large keywords): dictionary_eci-marking

Pattern #3 — High

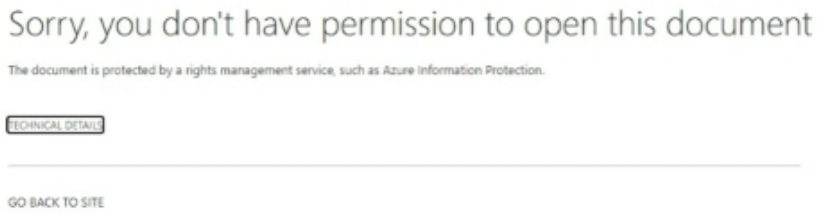
Primary element
Keyword list: keyword_eci

Character proximity
Detect primary AND supporting elements within 1000 characters

Supporting elements

Minimum 3 match should be found from following element(s):

- Keyword list: keyword_eci-law
- Keyword list: keyword_eci-usc
- Keyword list: keyword_eci-violation-notice



Q/A

Backup

Data Sensitivity and Moving Toward Zero Trust