Information Protection

Protect and manage your sensitive data throughout its lifecycle

Sanzhar Myrzagalym

Microsoft

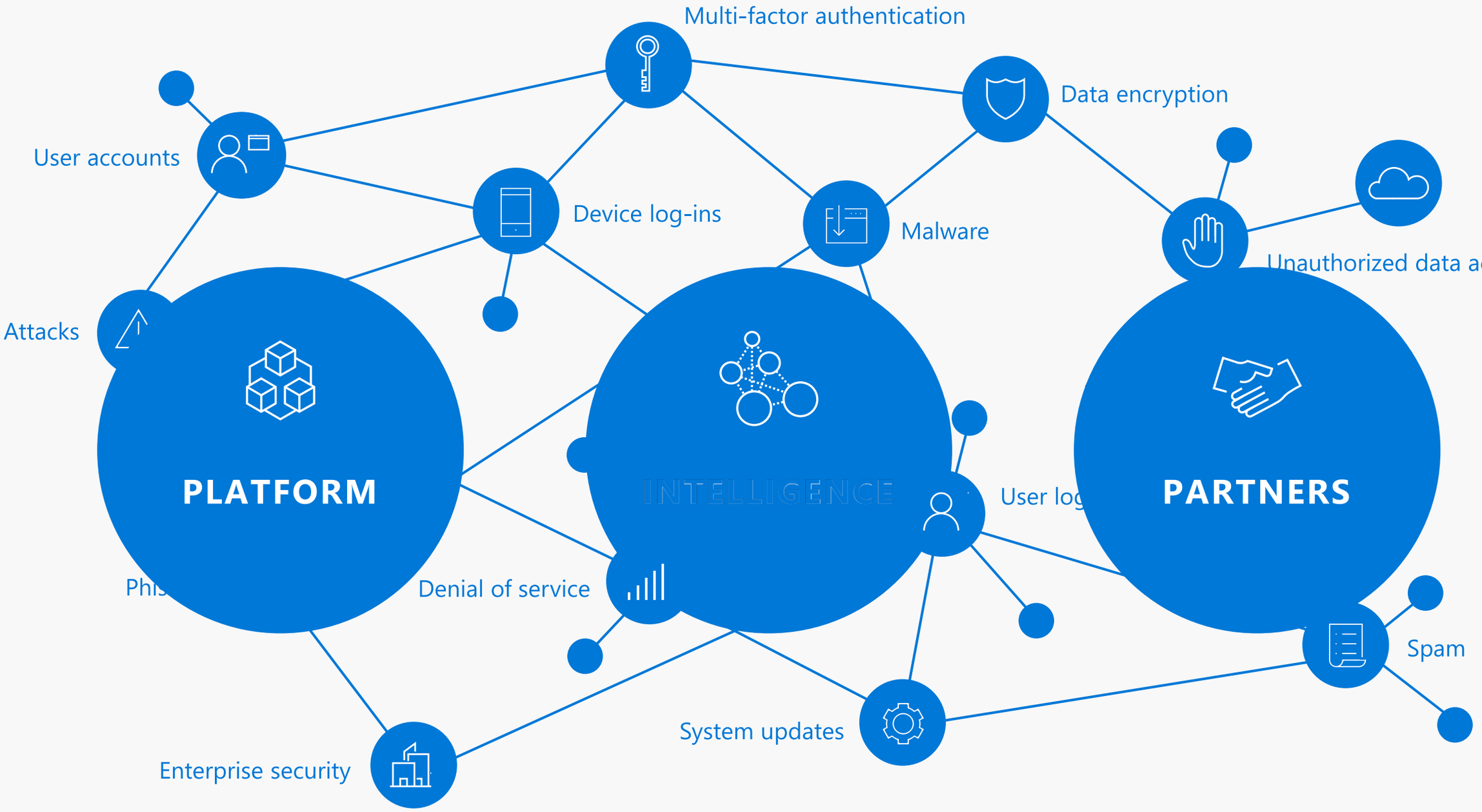
OUR **UNIQUE** APPROACH

Identity & Access Management
Protect users' identities and control access to valuable resources based on user risk level

Threat Protection
Protect against advanced threats and recover quickly when attacked

Information Protection
Ensure documents and emails are seen only by authorized people

Security Management
Gain visibility and control over security tools


Multi-factor authentication
Data encryption
User accounts
Device log-ins
Malware
Unauthorized data access
Attacks
PLATFORM
INTELLIGENCE
PARTNERS
Denial of service
Spam
System updates
Enterprise security

NEW WORLD OF WORK IS **DRIVING CHANGE**

41 % of employees say mobile business apps change how they work

85 % of enterprise organizations keep sensitive information in the cloud

88 % of organizations no longer have confidence to detect and prevent loss of sensitive data

58 % Have accidentally sent sensitive information to the wrong person

Cybersecurity. In the news. In the boardroom.

$3 trillion

Yearly estimated market value destroyed from cybercrime industry[2]

1 million

New pieces of malware created each day[3]

140+ days

Median # of days between infiltration and detection[4]

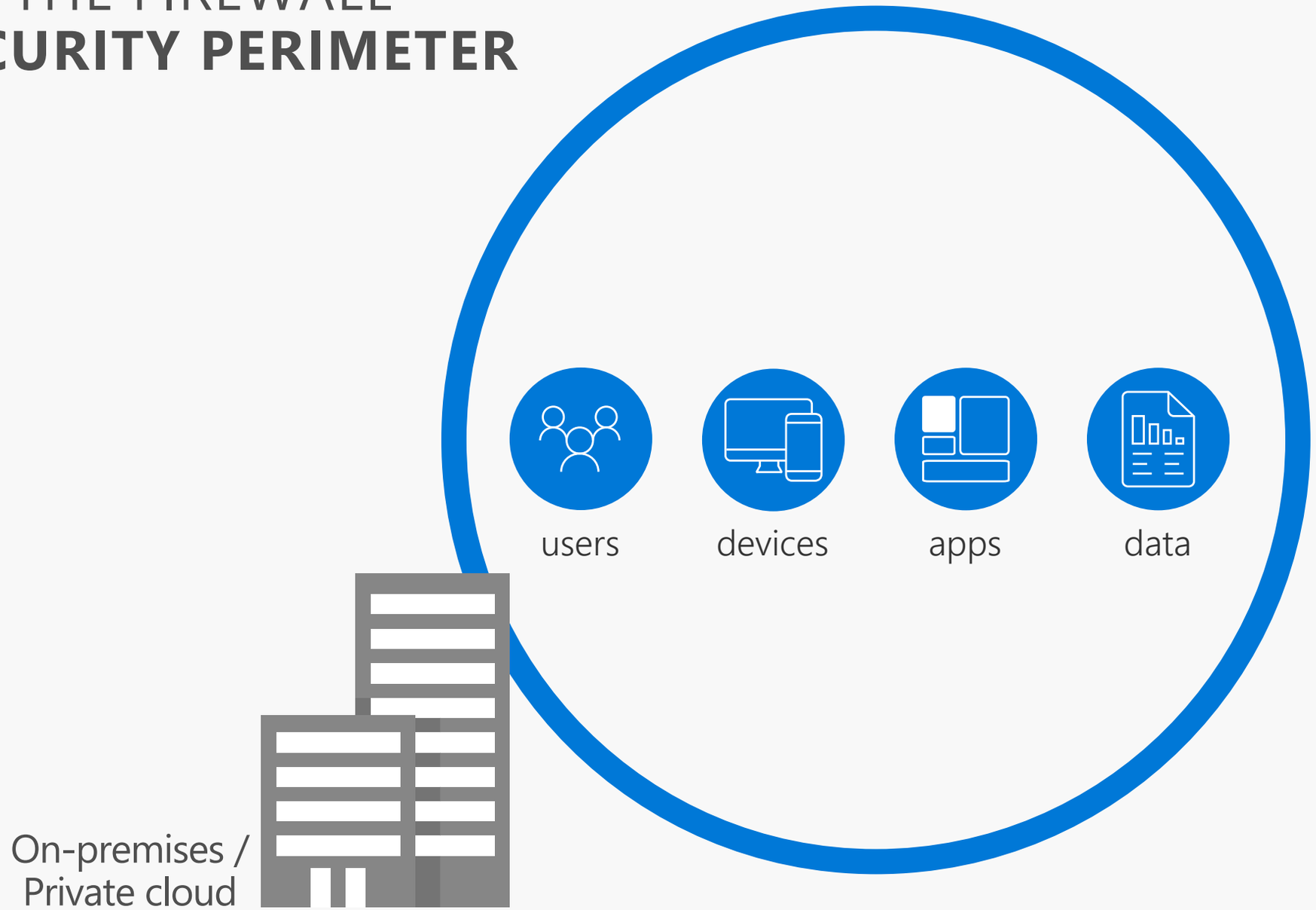
$15m

Average annual amount companies paid as a result of cybercrime[1]

82%

Of all companies expect to face a cyber attack[5]

IN THE PAST, THE FIREWALL WAS THE **SECURITY PERIMETER**



NOW THERE'S **FEWER BOUNDARIES**, MORE DATA, MORE COMPLEXITY

HOW DO I PROTECT **SENSITIVE INFORMATION?**

INFORMATION PROTECTION LIFECYCLE

Detect

Scan & detect sensitive data based on policy

Classify

Classify data and apply labels based on sensitivity

Protect

Apply protection actions, including encryption, access restrictions

Monitor

Reporting, alerts, remediation

THE LIFECYCLE OF A **SENSITIVE FILE**

Data is created, imported, & modified across various locations

Data is detected
Across devices, cloud services, on-prem environments

Sensitive data is classified & labeled
Based on sensitivity; used for either protection policies or retention policies

Data is protected based on policy
Protection may in the form of encryption, permissions, visual markings, retention, deletion, or a DLP action such as blocking sharing

Data travels across various locations, shared
Protection is persistent, travels with the data

Data is monitored
Reporting on data sharing, usage, potential abuse; take action & remediate

Retain, expire, delete data
Via data governance policies

SENSITIVITY LABELS **PERSIST WITH THE DOCUMENT**

Document labeling – what is it?
Metadata written into document files

Travels with the document as it moves

In clear text so that other systems such as a DLP engine can read it

Used for the purpose of apply a protection action or data governance action – determined by policy

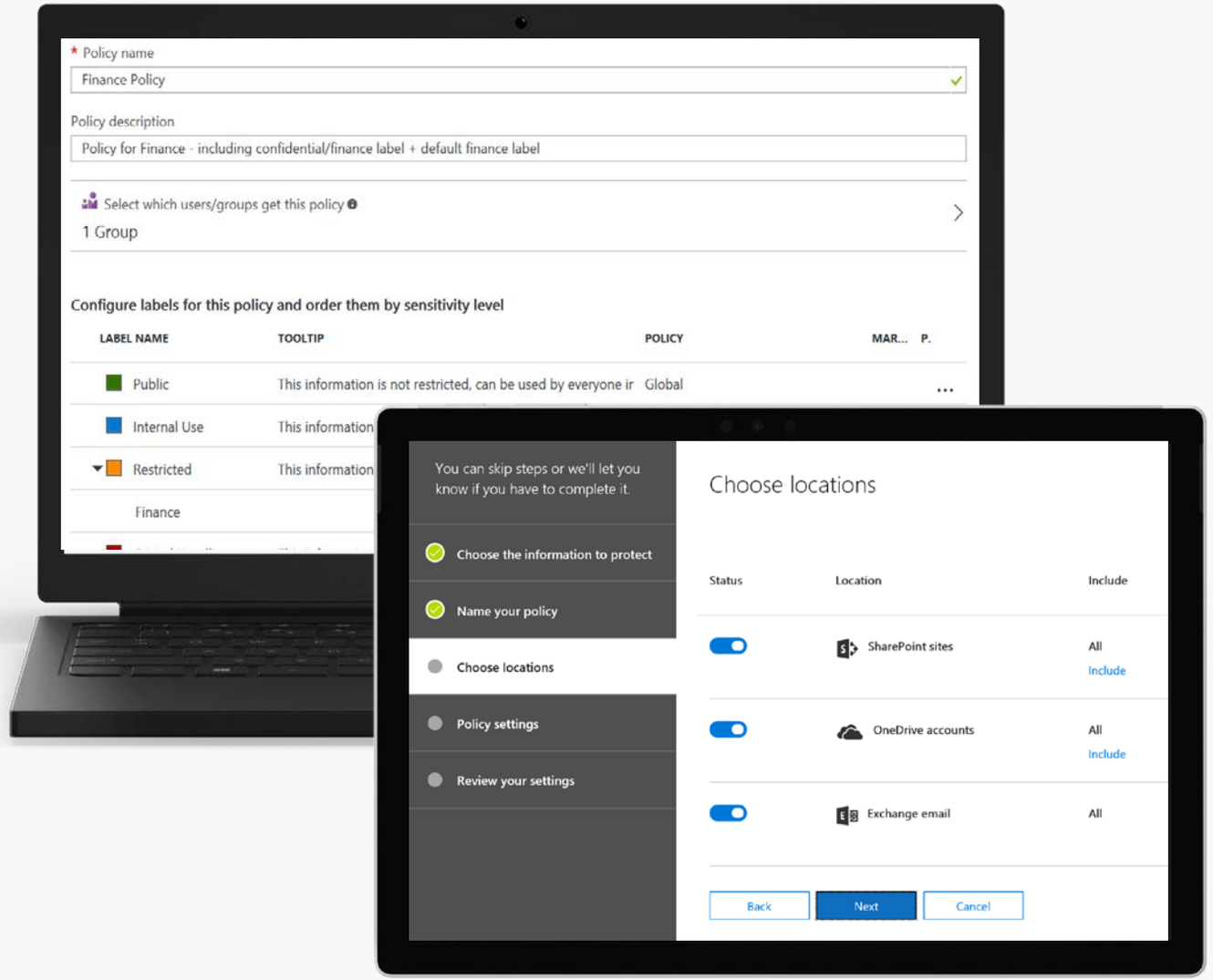
Can be customized per the organization's needs

DEFINE AND CUSTOMIZE POLICIES

Policies for specific groups or departments
Can be viewed and applied only by members of that group

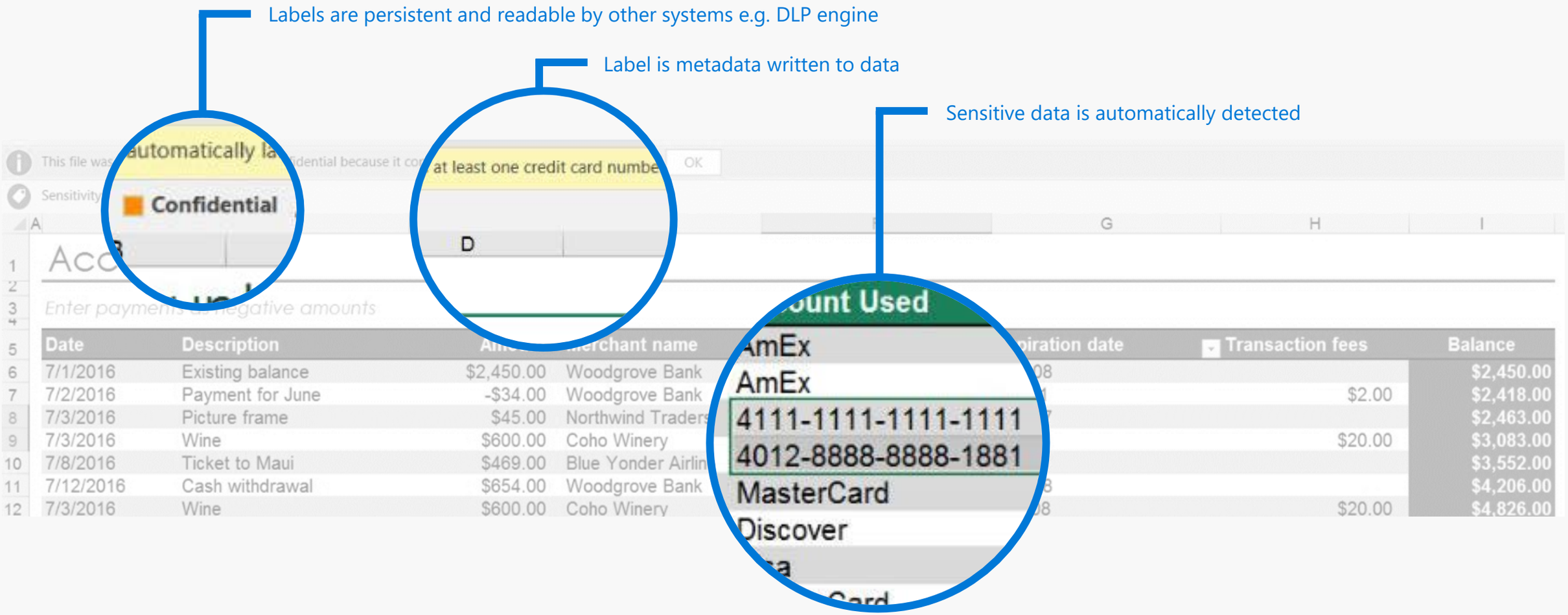
Policies targeting specific locations
Determine which locations are subject to policy, such as Exchange Online and SharePoint Online

Configure label schema and settings
Customize labels, sub-labels and settings like mandatory labeling, default label and justifications



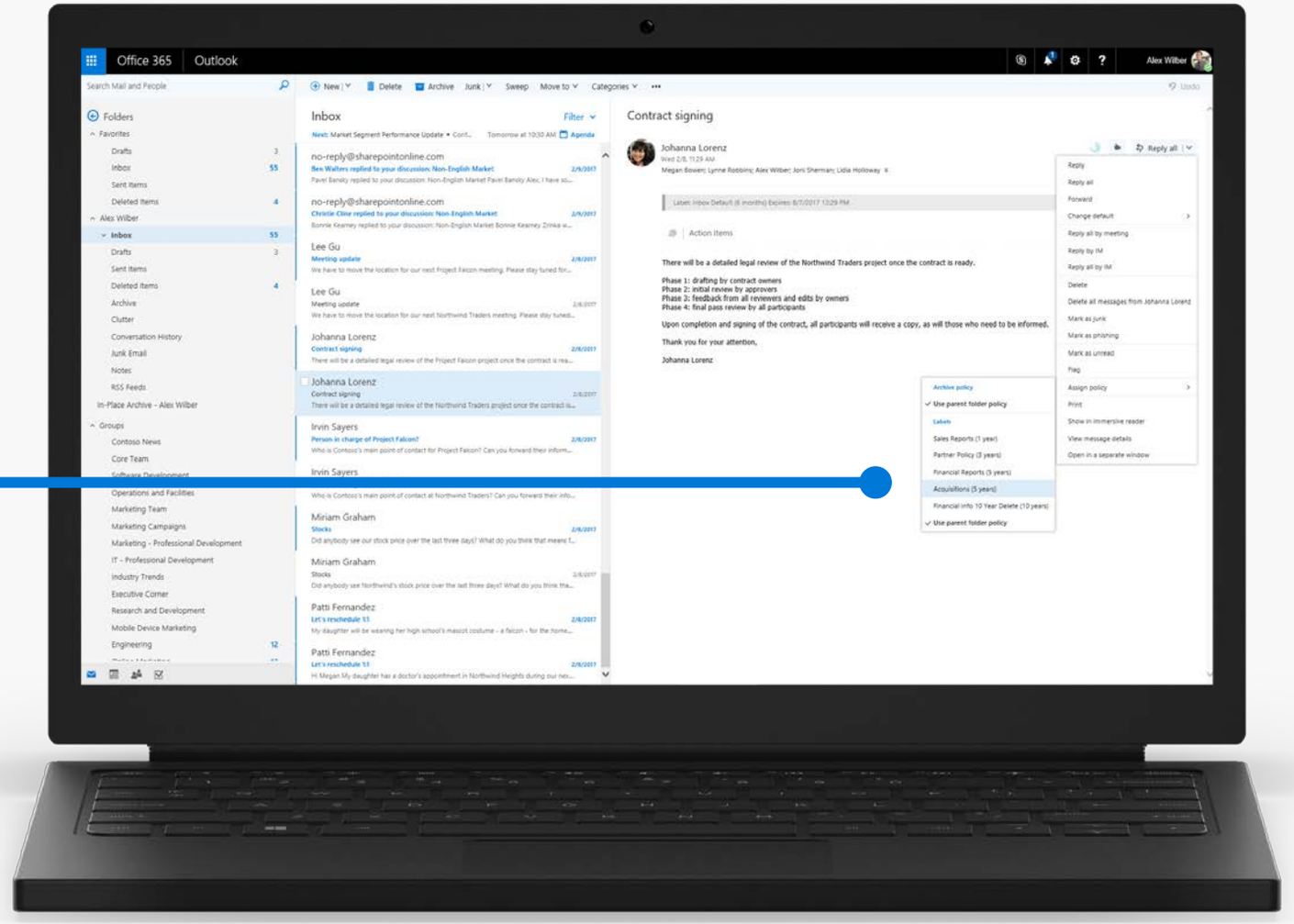
CLASSIFICATION & LABELING EXAMPLE – **SENSITIVE DATA**

Discover personal data and apply persistent labels



CLASSIFICATION & LABELING EXAMPLE – **DATA GOVERNANCE**

Labeling can be end-user driven
or automatically applied

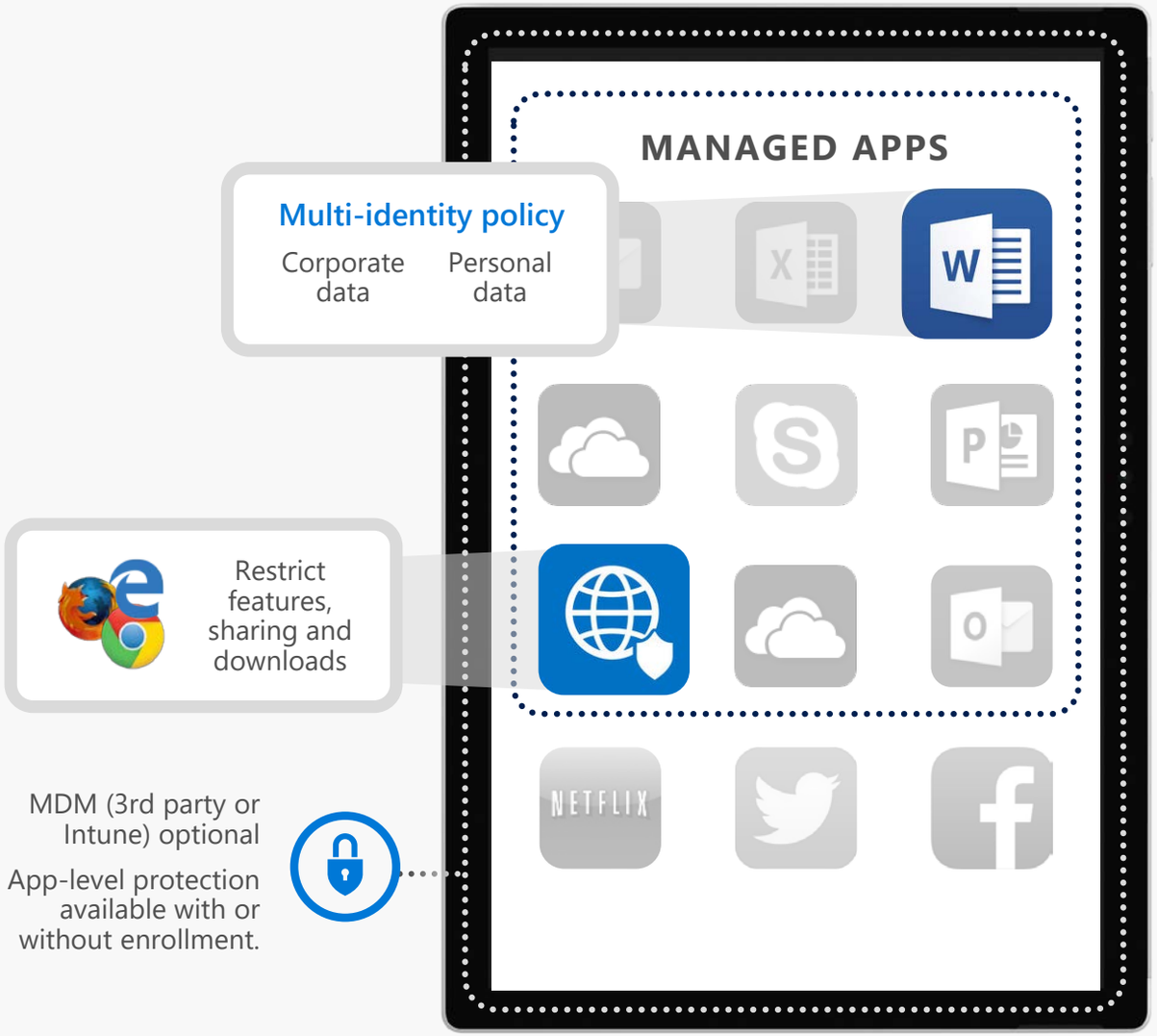


PROTECT DATA ON DEVICES AT THE APP LEVEL WITH **MOBILE APP PROTECTION POLICIES**

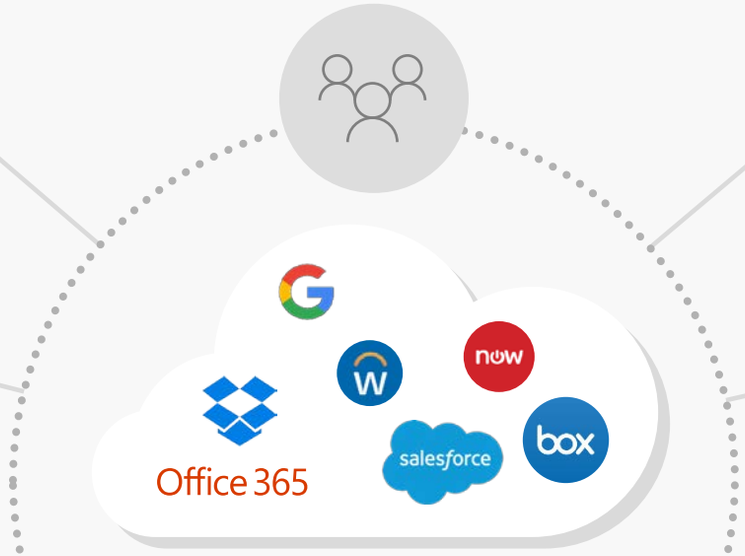
Data control
Control what happens to docs and data after they've been accessed with app protection policies

- App encryption at rest
- App access control—PIN or credentials
- Save as/copy/paste restrictions
- App-level selective wipe
- Apply policies for Windows 10 Information Protection for even greater control

Data separation
Multi-identity allows you to separate company data from personal data within an app



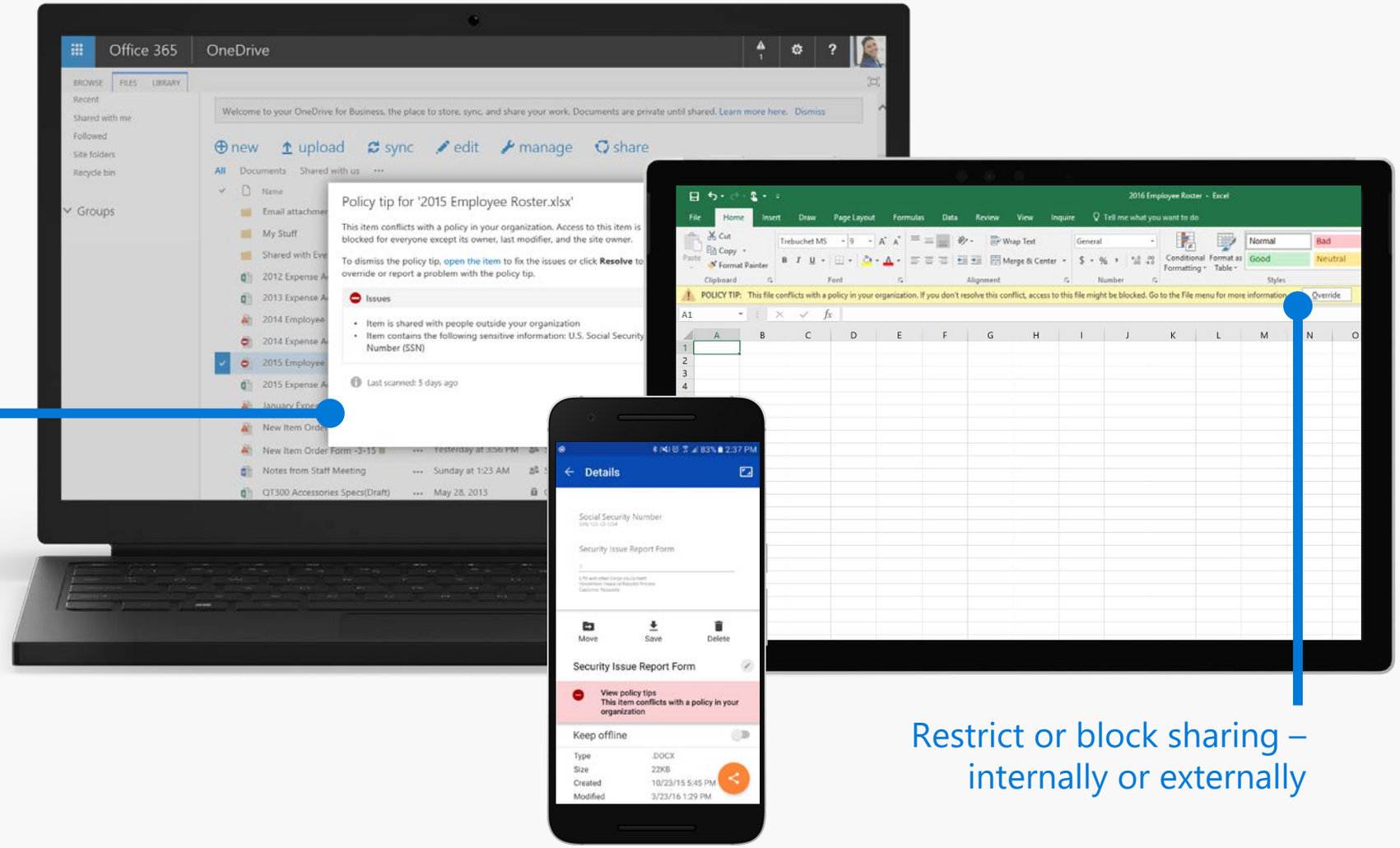
PROTECT SENSITIVE INFORMATION ACROSS CLOUD SERVICES & ON PREMISES



- Data encryption built into Azure & Office 365
- File-level encryption and permissions
- DLP actions to block sharing
- Control cloud app access & usage
- Email-level encryption and rights protection
- Retain, expire or delete documents
- Visual markings to indicate sensitive documents
- Policy tips to notify and educate end users
- Revoke app access

PROTECTION EXAMPLE:
DLP POLICY TO **LIMIT DOCUMENT SHARING**

Across Office client applications – mobile, desktop & tablets

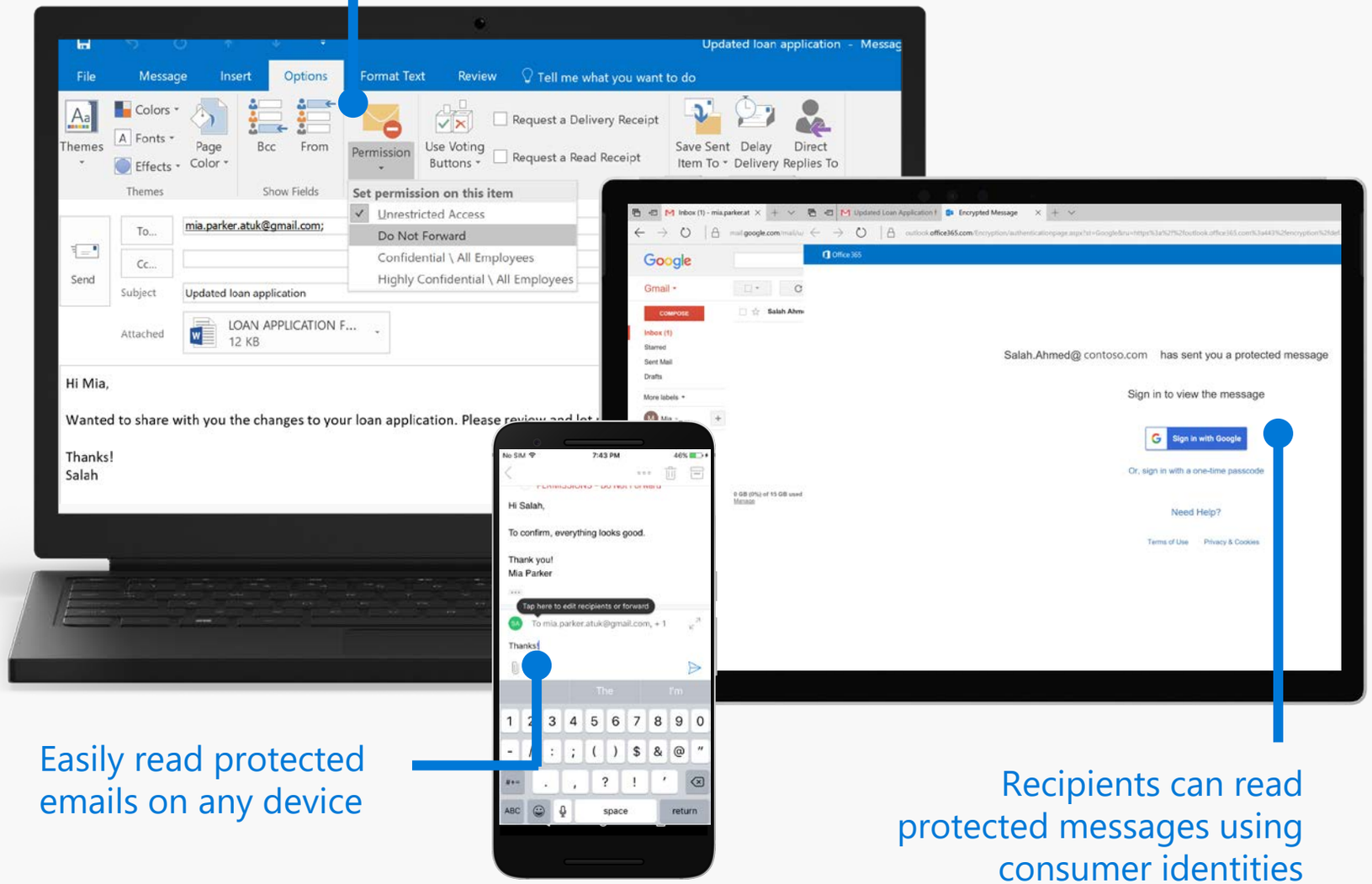


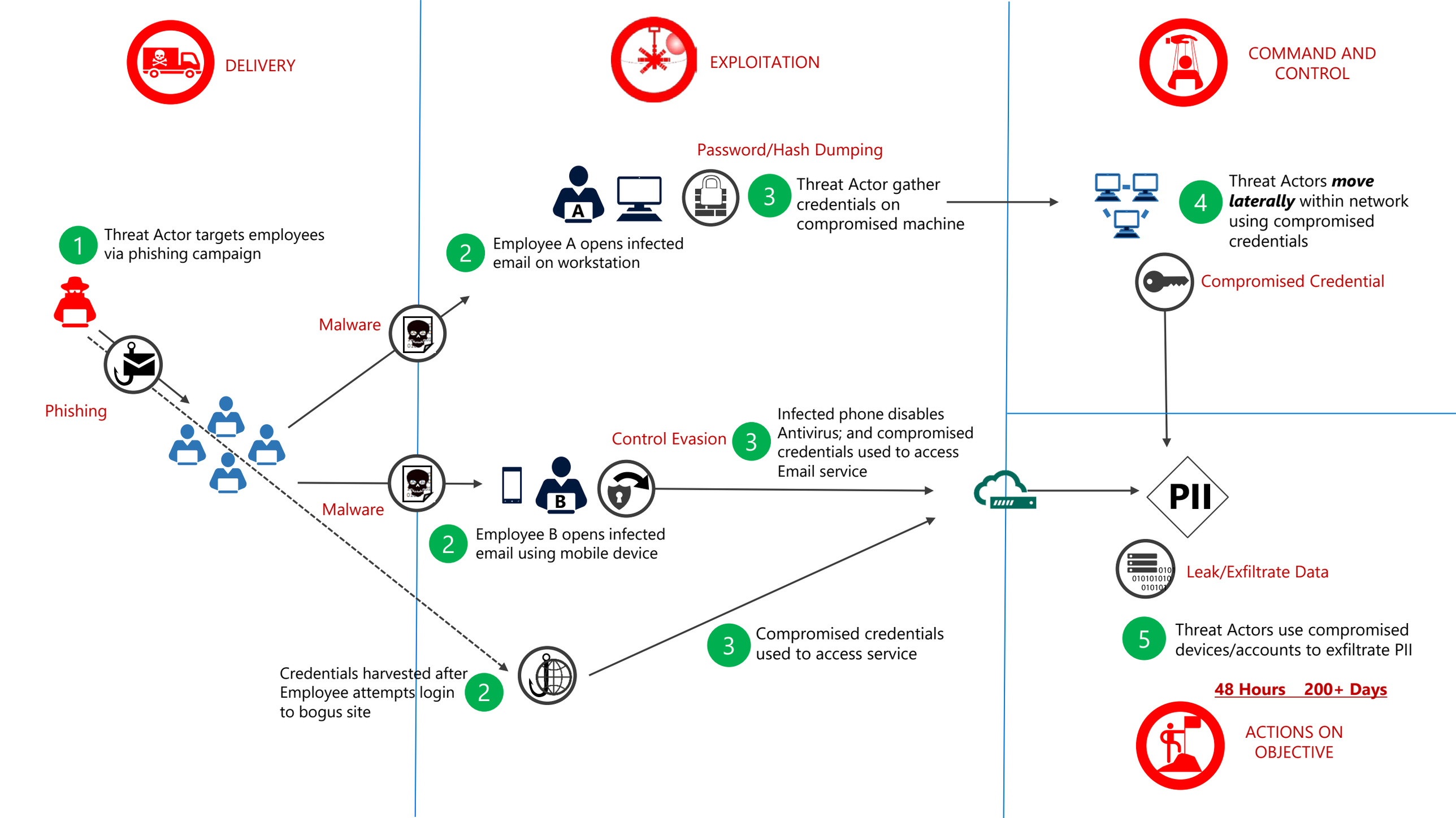
EMAIL ENCRYPTION AND RIGHTS PROTECTION

Protect
Mitigates risk of unintended disclosure through encryption and rights protection

Control
Leverage automatic policies or ad hoc end-user controls, for emails shared inside or outside the organization

Compliance
Meet compliance obligations that require encrypting data or encryption key control




DELIVERY
EXPLOITATION
COMMAND AND CONTROL
Password/Hash Dumping
A
3
Threat Actor gather credentials on compromised machine
4
Threat Actors ***move laterally*** within network using compromised credentials
1
Threat Actor targets employees via phishing campaign
2
Employee A opens infected email on workstation
Compromised Credential
Malware
Phishing
Control Evasion
3
Infected phone disables Antivirus; and compromised credentials used to access Email service
B
Malware
PII
2
Employee B opens infected email using mobile device
Leak/Exfiltrate Data
3
Compromised credentials used to access service
Credentials harvested after Employee attempts login to bogus site
2
5
Threat Actors use compromised devices/accounts to exfiltrate PII
48 Hours
200+ Days
ACTIONS ON OBJECTIVE

DELIVERY

Windows 10 E3/E5
Device Guard
AppLocker

Windows 10 E5
Advanced Threat Protection

EXPLOITATION

Windows 10 E3/E5
Credential Guard

COMMAND AND CONTROL

EMS E3
Advanced Threat Analytics

Microsoft Services
- Active Directory Security Assessment
- Sec Admin & Privilege Access (ESAE & PAW)
- Restrict Lateral Movement (LAPS & POP-SLAM)
- Hunting and Incident Response (PADS & IRR)

Operations Management Suite (OMS) & Azure Security Center

1 Threat Actor targets employees via phishing campaign

Office 365 E5
Advanced Threat Protection

EMS E3
Intune conditional access

Defense in Depth reduces risk & extent of Compromise

EMS E5
Cloud App Security

Office 365 E5
Advanced Security Management

Azure
Multi-Factor Authentication

EMS E5
Azure Information Protection

Office 365 E3/E5
Azure Information Protection
Data Loss Prevention

Windows 10 E3/E5
Windows Information Protection

Azure
Key Vault

Windows 10 E3/E5
SmartScreen checks URL and App reputation

Detect

Scan & detect sensitive data based on policy

Classify

Classify data and apply labels based on sensitivity

Protect

Apply protection actions, including encryption, access restrictions

Monitor

Reporting, alerts, remediation

MONITOR INFORMATION PROTECTION EVENTS FOR GREATER CONTROL

Visibility

- Policy violations
- Document access & sharing
- App usage
- Anomalous activity
- End-user overrides
- False positives

Take Action

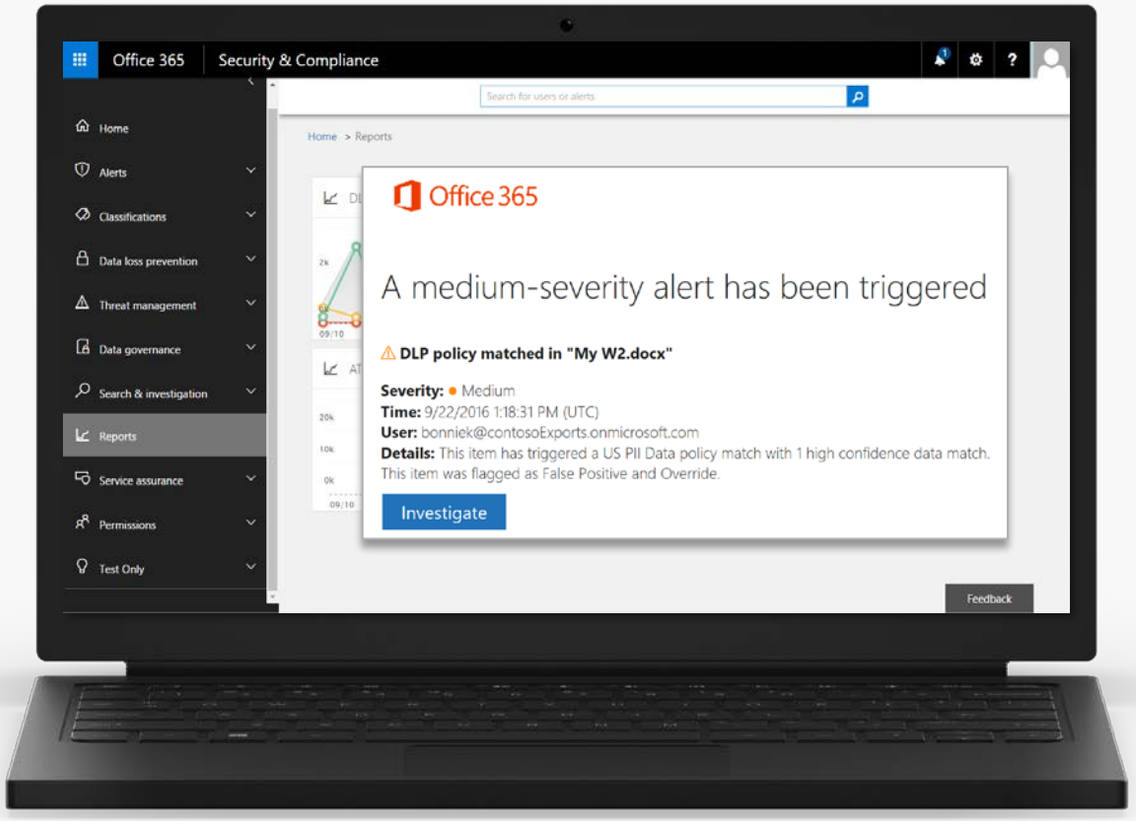
- Tune & revise policies
- Revoke access
- Quarantine file
- Quarantine user
- Integrate into workflows & SIEM

MONITOR **DLP** AND **DATA GOVERNANCE EVENTS**

Know when policy is violated
Incident report emails alert you in real time when content violates policy

See the effectiveness of your policies
Built in reports help you see historical information and tune policies

Integrates with other systems
Leverage the Activity Management API to pull information into SIEM and workflow tools



MONITOR DOCUMENT **SHARING & ACCESS**

Distribution visibility
Analyze the flow of personal and sensitive data and detect risky behaviors.

Access logging
Track who is accessing documents and from where.

Access revocation
Prevent data leakage or misuse by changing or revoking document access remotely.