ICT as Tool of Compliance

Chadymae Barinan

Partner Technology Strategist – Modern Workplace

Microsoft Philippines

World’s Largest Transportation Service Owns No Car

UBER

World’s Largest Accomodation Provider Owns No Real Estate

airbnb

World’s Most Popular Media Owner Creates No Content

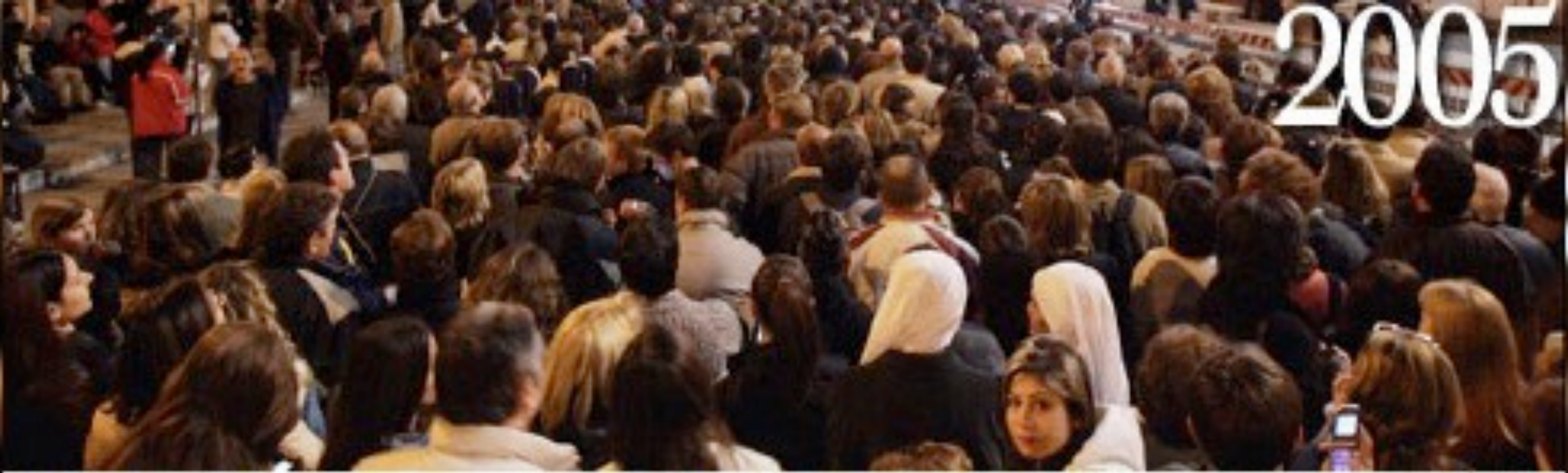
facebook

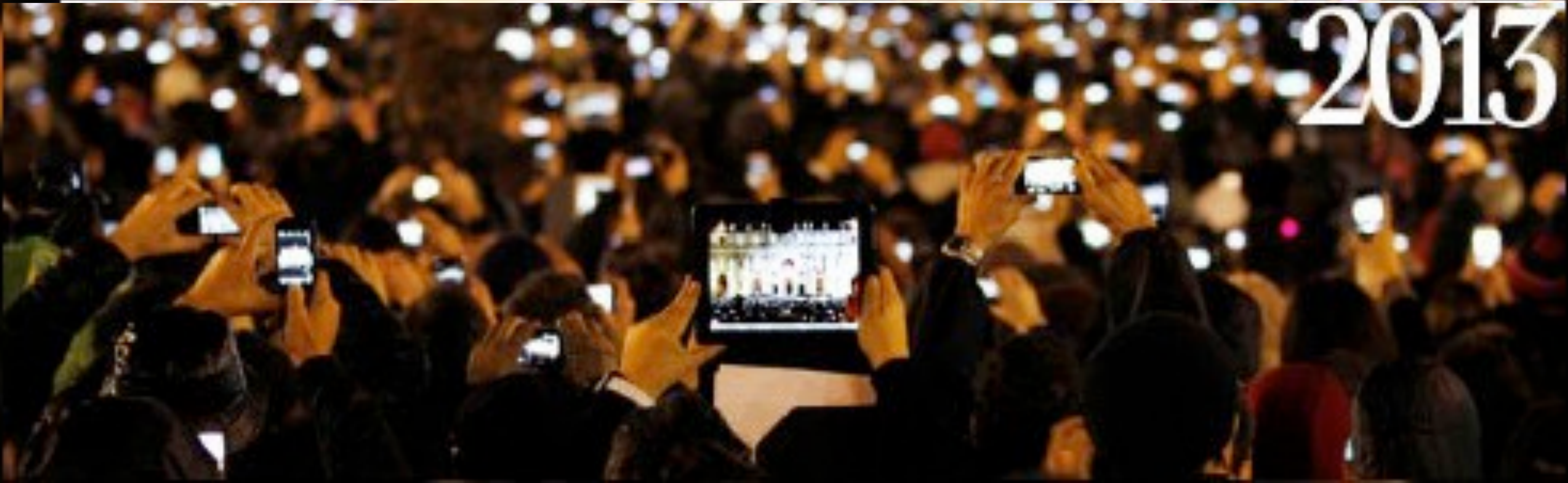
World’s Most Valuable Retailer Has No Inventory

amazon

World’s Largest Movie House Owns No Cinemas

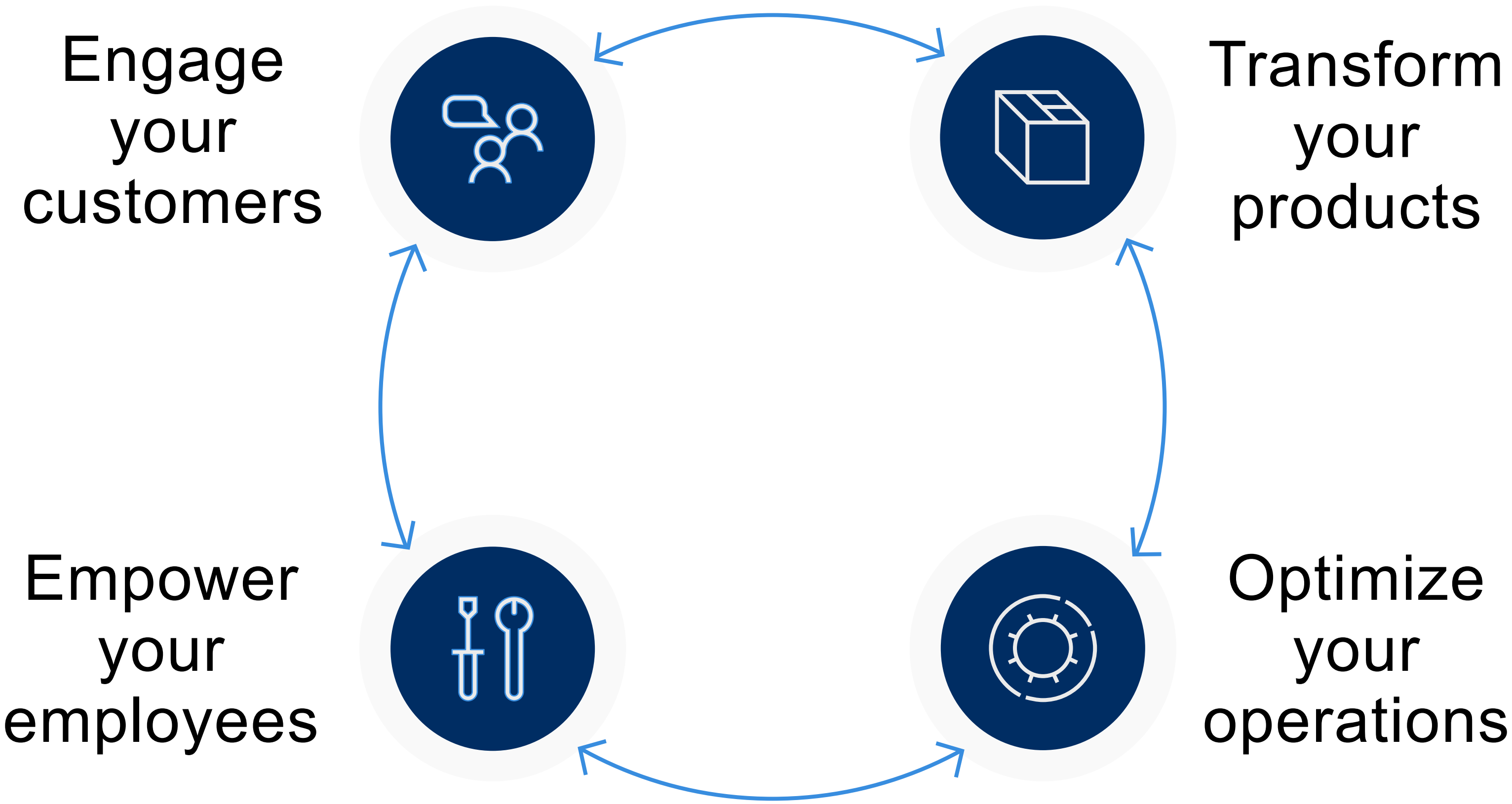
NETFLIX


2005


2013

THE WORLD HAS CHANGED

Digital Transformation



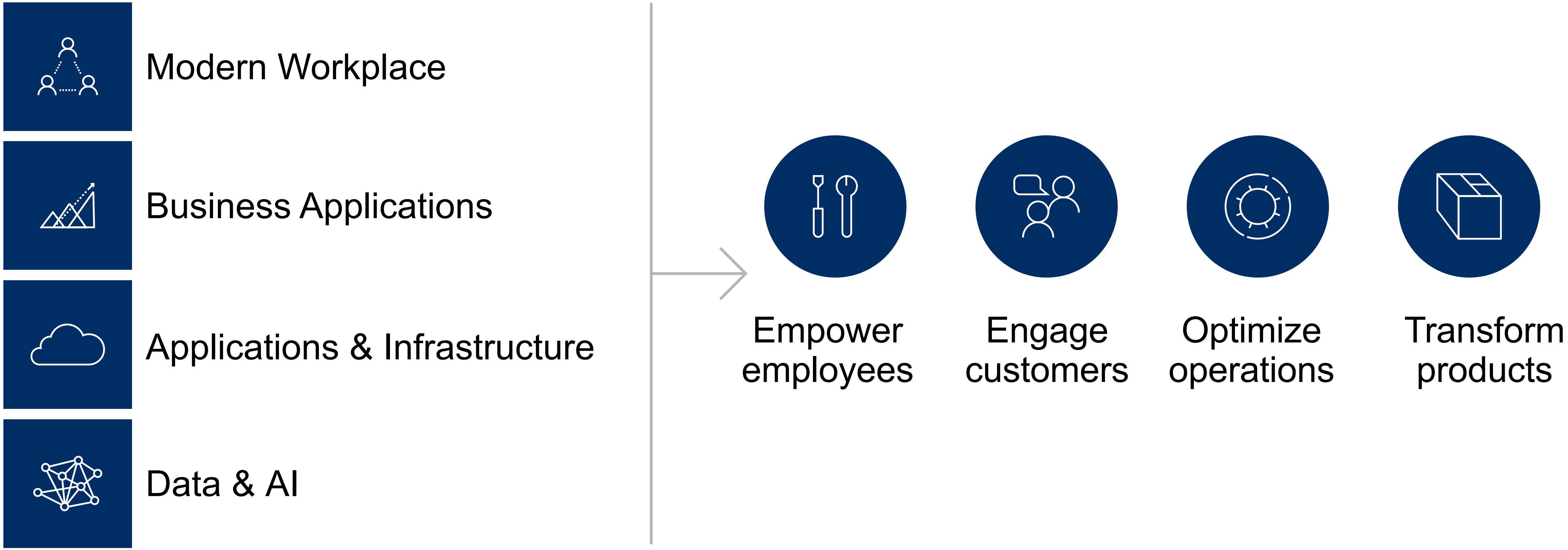
Engage your customers

Transform your products

Empower your employees

Optimize your operations

Enabling Digital Transformation



Modern Workplace

Business Applications

Applications & Infrastructure

Data & AI

Empower employees

Engage customers

Optimize operations

Transform products

Microsoft mission

Empower every person and every organization on the planet to achieve more

Microsoft

TURBULENT TIMES

2 Billion records compromised in the last year

99+ DAYS between infiltration and detection

$15 MILLION of cost/business impact per breach

Challenges to defense

Identity-based attacks
are up 300% this year

Information is your
most attractive target

96% of malware is
automated polymorphic

Most enterprises report using
more than 60 security solutions

Challenges to success

Strategies for defense

Identity-based attacks are up 300% this year	→	Adopt identity-based protection
Information is your most attractive target	→	Protect information wherever it goes
96% of malware is automated polymorphic	→	Detect attacks faster and automate response
Most enterprises report using more than 60 security solutions	→	Use tools that integrate investigation experience and provide guidance

Our commitment to you

- Security
- Privacy & control
- Compliance
- Transparency
- Reliability

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

Microsoft

OUR **UNIQUE** APPROACH

Platform

Intelligence

Partners

Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

Azure Active Directory

Conditional Access

Windows Hello

Windows Credential Guard

Threat protection

Protect against advanced threats and recover quickly when attacked

Advanced Threat Analytics

Windows Defender Advanced Threat Protection

Office 365 Advanced Threat Protection

Office 365 Threat Intelligence

Information protection

Ensure documents and emails are seen only by authorized people

Azure Information Protection

Office 365 Data Loss Prevention

Windows Information Protection

Microsoft Cloud App Security

Office 365 Advanced Security Mgmt.

Microsoft Intune

Security management

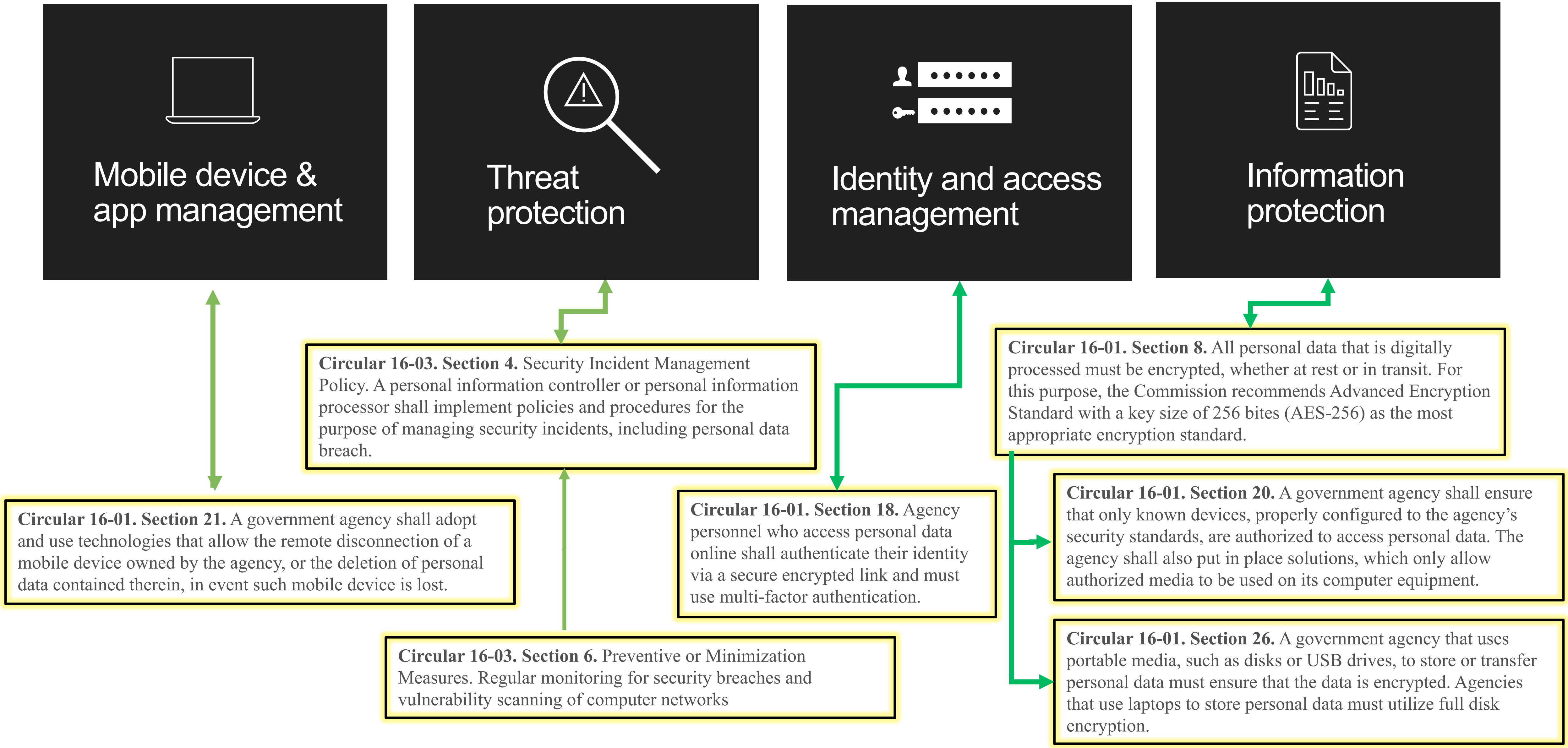
Gain visibility and control over security tools

Azure Security Center

Office 365 Security Center

Windows Defender Security Center

DPA Alignment



Mobile device & app management

Threat protection

Identity and access management

Information protection

Circular 16-01. Section 21. A government agency shall adopt and use technologies that allow the remote disconnection of a mobile device owned by the agency, or the deletion of personal data contained therein, in event such mobile device is lost.

Circular 16-03. Section 4. Security Incident Management Policy. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach.

Circular 16-03. Section 6. Preventive or Minimization Measures. Regular monitoring for security breaches and vulnerability scanning of computer networks

Circular 16-01. Section 18. Agency personnel who access personal data online shall authenticate their identity via a secure encrypted link and must use multi-factor authentication.

Circular 16-01. Section 8. All personal data that is digitally processed must be encrypted, whether at rest or in transit. For this purpose, the Commission recommends Advanced Encryption Standard with a key size of 256 bites (AES-256) as the most appropriate encryption standard.

Circular 16-01. Section 20. A government agency shall ensure that only known devices, properly configured to the agency's security standards, are authorized to access personal data. The agency shall also put in place solutions, which only allow authorized media to be used on its computer equipment.

Circular 16-01. Section 26. A government agency that uses portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is encrypted. Agencies that use laptops to store personal data must utilize full disk encryption.

EU General Data Protection Regulation (GDPR)

Enhanced personal privacy rights

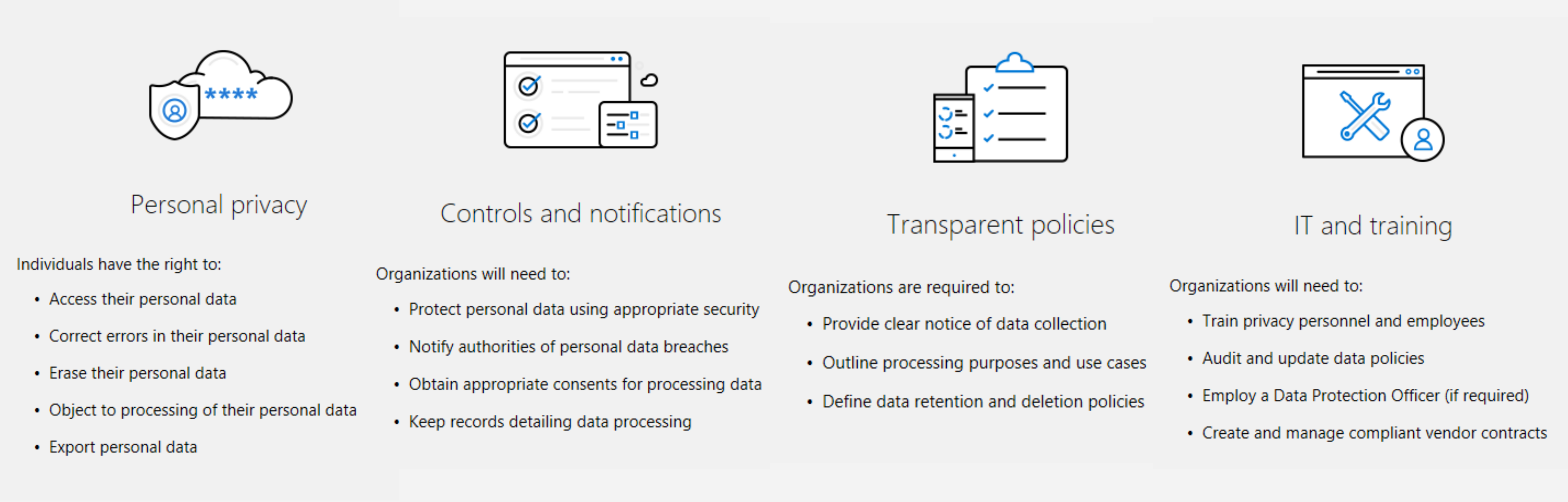
Increased duty for protecting data

Mandatory breach reporting

Significant penalties for non-compliance

www.microsoft.com/GDPR

Key changes under GDPR



Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations are required to:

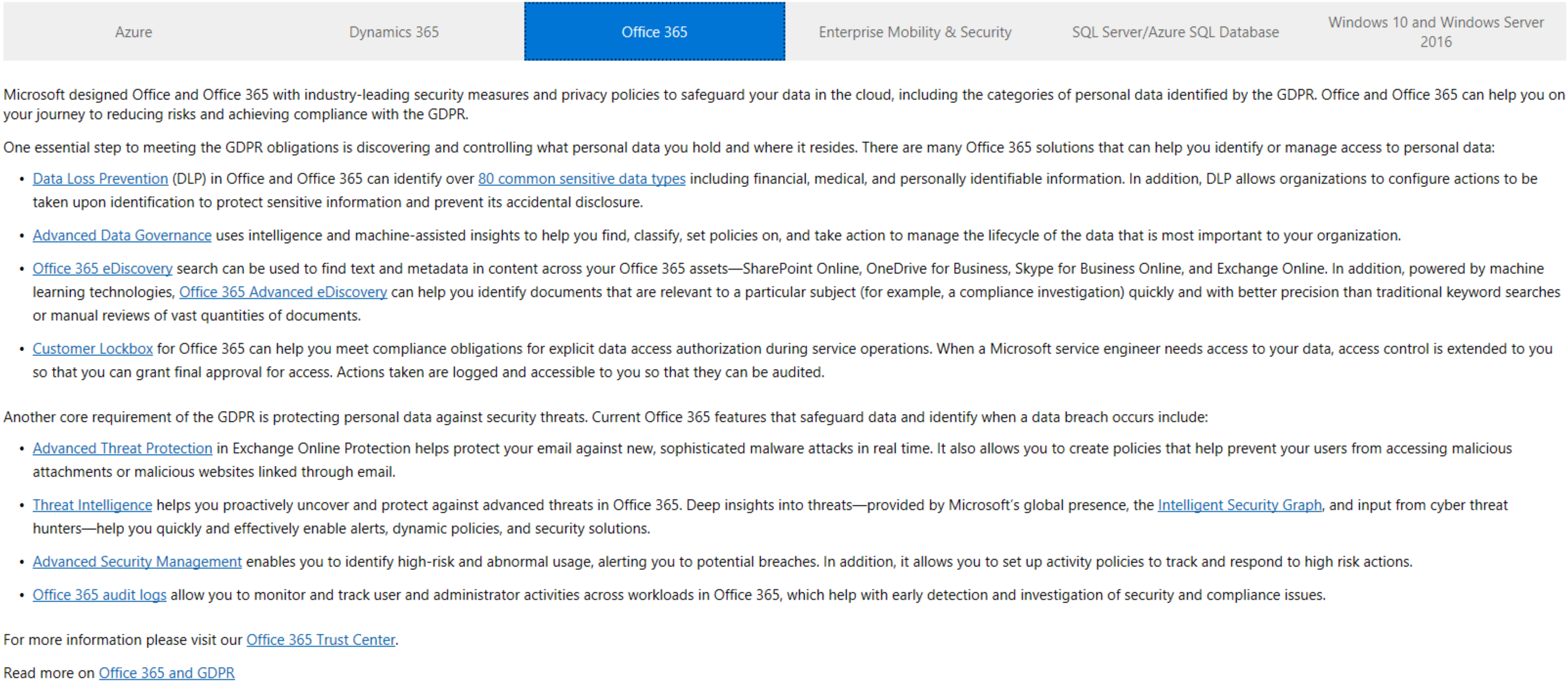
- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organizations will need to:

- Train privacy personnel and employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create and manage compliant vendor contracts

How our products help with GDPR Compliance



Azure
Dynamics 365
Office 365
Enterprise Mobility & Security
SQL Server/Azure SQL Database
Windows 10 and Windows Server 2016

Microsoft designed Office and Office 365 with industry-leading security measures and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by the GDPR. Office and Office 365 can help you on your journey to reducing risks and achieving compliance with the GDPR.

One essential step to meeting the GDPR obligations is discovering and controlling what personal data you hold and where it resides. There are many Office 365 solutions that can help you identify or manage access to personal data:

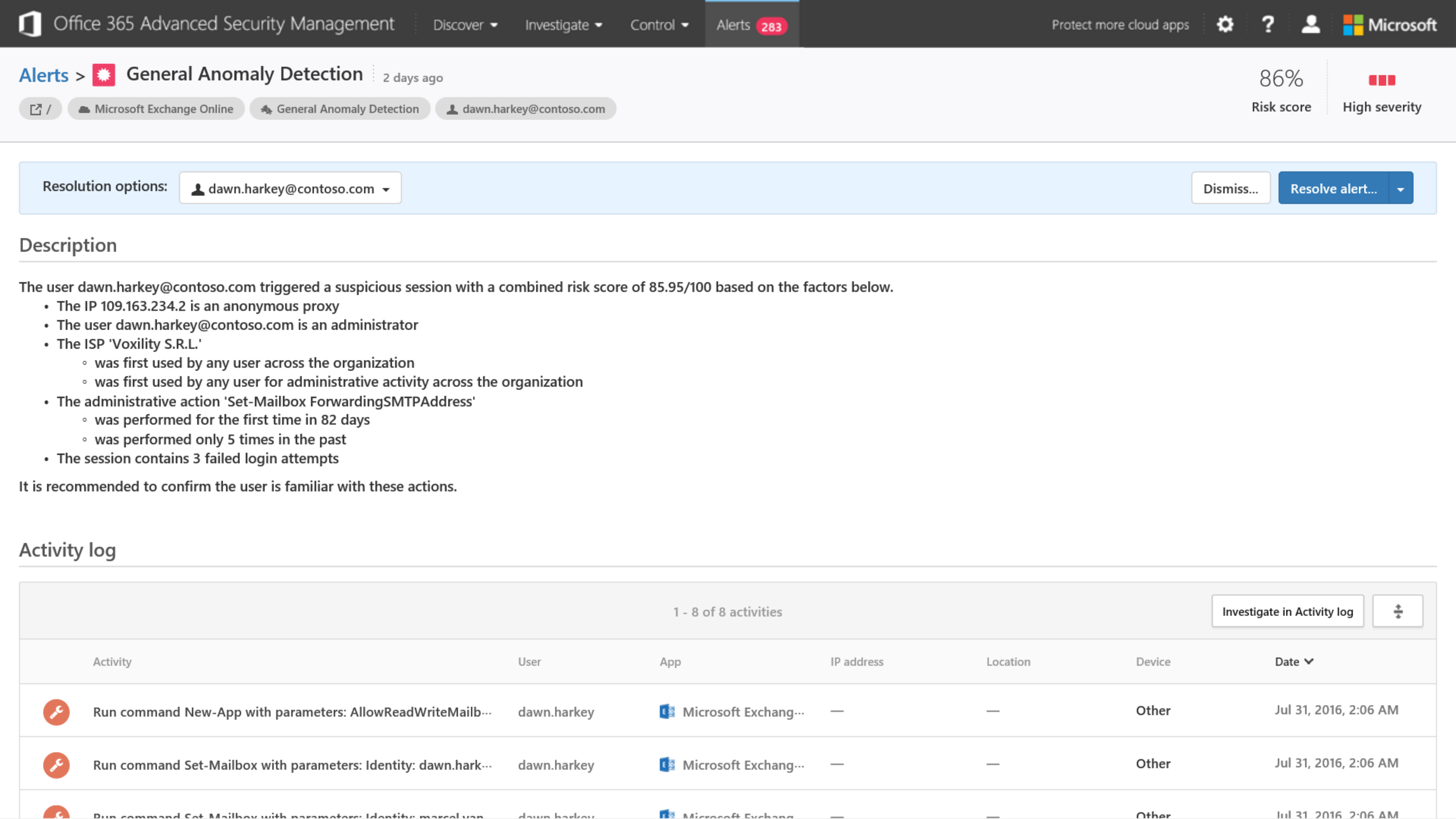
- Data Loss Prevention (DLP) in Office and Office 365 can identify over 80 common sensitive data types including financial, medical, and personally identifiable information. In addition, DLP allows organizations to configure actions to be taken upon identification to protect sensitive information and prevent its accidental disclosure.
- Advanced Data Governance uses intelligence and machine-assisted insights to help you find, classify, set policies on, and take action to manage the lifecycle of the data that is most important to your organization.
- Office 365 eDiscovery search can be used to find text and metadata in content across your Office 365 assets—SharePoint Online, OneDrive for Business, Skype for Business Online, and Exchange Online. In addition, powered by machine learning technologies, Office 365 Advanced eDiscovery can help you identify documents that are relevant to a particular subject (for example, a compliance investigation) quickly and with better precision than traditional keyword searches or manual reviews of vast quantities of documents.
- Customer Lockbox for Office 365 can help you meet compliance obligations for explicit data access authorization during service operations. When a Microsoft service engineer needs access to your data, access control is extended to you so that you can grant final approval for access. Actions taken are logged and accessible to you so that they can be audited.

Another core requirement of the GDPR is protecting personal data against security threats. Current Office 365 features that safeguard data and identify when a data breach occurs include:

- Advanced Threat Protection in Exchange Online Protection helps protect your email against new, sophisticated malware attacks in real time. It also allows you to create policies that help prevent your users from accessing malicious attachments or malicious websites linked through email.
- Threat Intelligence helps you proactively uncover and protect against advanced threats in Office 365. Deep insights into threats—provided by Microsoft's global presence, the Intelligent Security Graph, and input from cyber threat hunters—help you quickly and effectively enable alerts, dynamic policies, and security solutions.
- Advanced Security Management enables you to identify high-risk and abnormal usage, alerting you to potential breaches. In addition, it allows you to set up activity policies to track and respond to high risk actions.
- Office 365 audit logs allow you to monitor and track user and administrator activities across workloads in Office 365, which help with early detection and investigation of security and compliance issues.

For more information please visit our Office 365 Trust Center.

Read more on Office 365 and GDPR



Alerts > General Anomaly Detection | 2 days ago

86%
Risk score

High severity

Resolution options: dawn.harkey@contoso.com

Description

The user dawn.harkey@contoso.com triggered a suspicious session with a combined risk score of 85.95/100 based on the factors below.

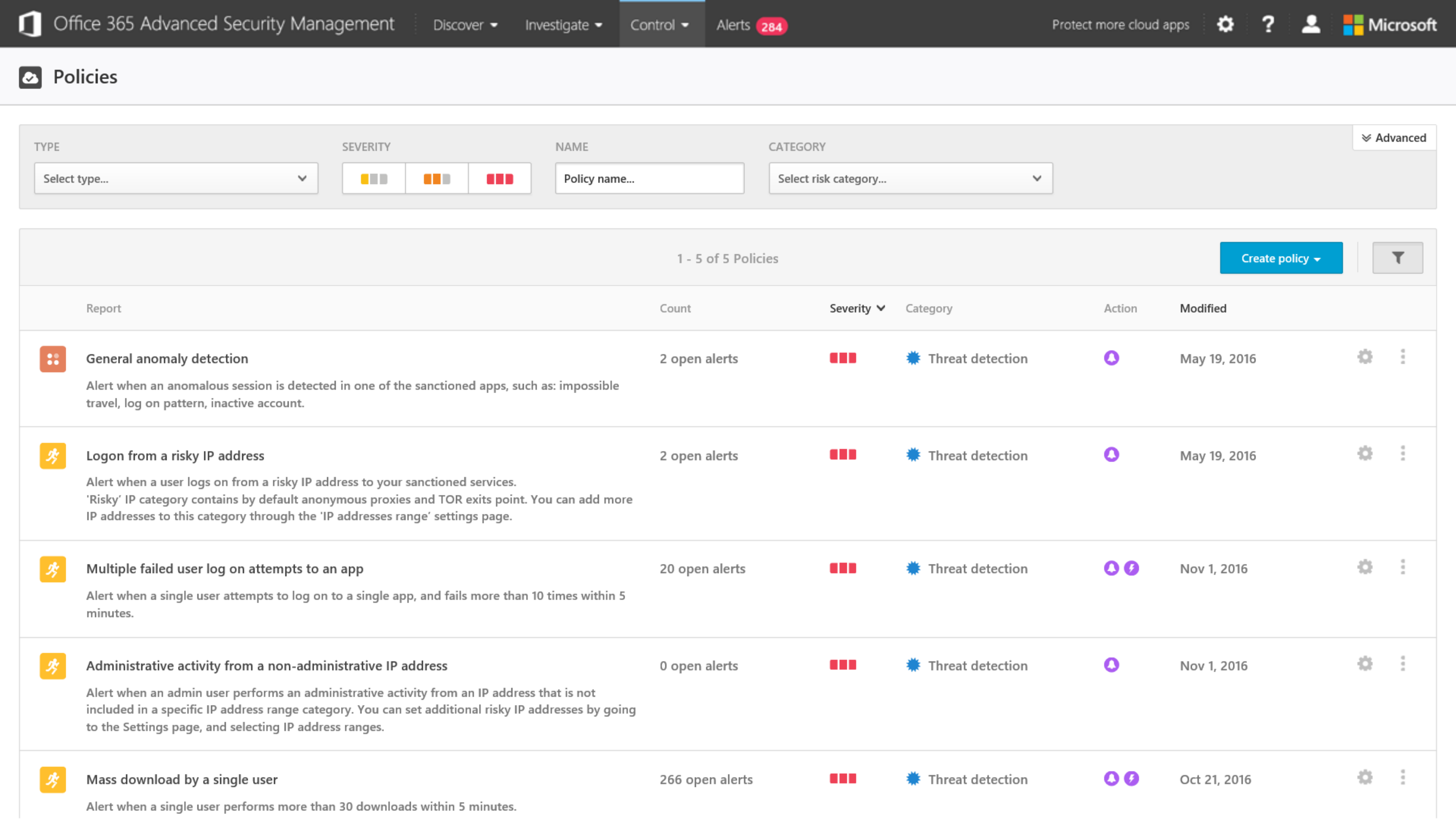
- The IP 109.163.234.2 is an anonymous proxy
- The user dawn.harkey@contoso.com is an administrator
- The ISP 'Voxility S.R.L.'
  - was first used by any user across the organization
  - was first used by any user for administrative activity across the organization
- The administrative action 'Set-Mailbox ForwardingSMTPAddress'
  - was performed for the first time in 82 days
  - was performed only 5 times in the past
- The session contains 3 failed login attempts

It is recommended to confirm the user is familiar with these actions.

Activity log

1 - 8 of 8 activities

Activity	User	App	IP address	Location	Device	Date
Run command New-App with parameters: AllowReadWriteMailb...	dawn.harkey	Microsoft Exchang...	—	—	Other	Jul 31, 2016, 2:06 AM
Run command Set-Mailbox with parameters: Identity: dawn.hark...	dawn.harkey	Microsoft Exchang...	—	—	Other	Jul 31, 2016, 2:06 AM
Run command Set-Mailbox with parameters: Identity: marcel.van	dawn.harkey	Microsoft Exchang	—	—	Other	Jul 31, 2016, 2:06 AM



Report	Count	Severity	Category	Action	Modified
General anomaly detection Alert when an anomalous session is detected in one of the sanctioned apps, such as: impossible travel, log on pattern, inactive account.	2 open alerts	■■■	Threat detection	🔔	May 19, 2016
Logon from a risky IP address Alert when a user logs on from a risky IP address to your sanctioned services. 'Risky' IP category contains by default anonymous proxies and TOR exits point. You can add more IP addresses to this category through the 'IP addresses range' settings page.	2 open alerts	■■■	Threat detection	🔔	May 19, 2016
Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.	20 open alerts	■■■	Threat detection	🔔 ⚡	Nov 1, 2016
Administrative activity from a non-administrative IP address Alert when an admin user performs an administrative activity from an IP address that is not included in a specific IP address range category. You can set additional risky IP addresses by going to the Settings page, and selecting IP address ranges.	0 open alerts	■■■	Threat detection	🔔	Nov 1, 2016
Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	266 open alerts	■■■	Threat detection	🔔 ⚡	Oct 21, 2016

Industry Certifications

https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

Information Security Management System
ISO
27001
Certified

HIPAA
COMPLIANT

U.S. • EU
SAFE
HARBOR

PCI DSS CERTIFIED
SERVICE LEVEL 1

FISMA
COMPLIANCE

SAS 70
and
SSAE 16

EU Model Clauses
2016 Microsoft Agreement

GDPR

Philippine Data Privacy Act of 2012
RA - 10173