



Microsoft Threat Protection

Protection Against Modern Attack Vectors

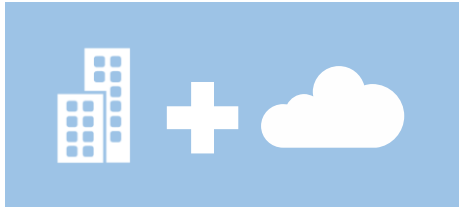
Gachay Mirzayev

Technology Solution Professional
Microsoft CIS
gachay@microsoft.com

Rasim Badalbayli

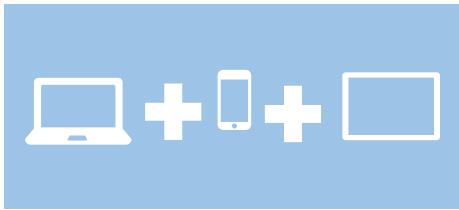
Technology Solution Professional
Microsoft CEE
rabadalb@microsoft.com

Information Security is in Transformation



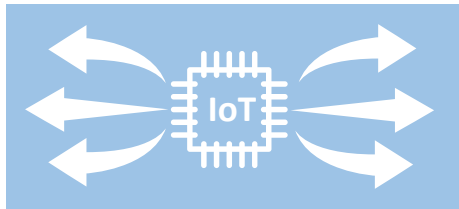
Enterprise IT is Cloud Hybrid

- Cloud adoption is inevitable (Digital Transformation + industry momentum)
- Legacy systems will take years to migrate or retire



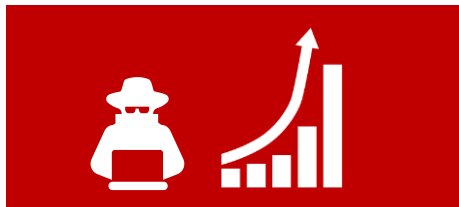
Technology Mobility and Volume is Exploding

- Increasing demand for first class experience on mobile devices
- Variance in trustworthiness of mobile devices



Pervasive Digital Transformation and IoT

- IoT adoption driving a wave of app development and cloud usage
- Enterprise PC Security strategies applying poorly to IoT devices



Increasingly Hostile Environment

- Increased attack surface with new technologies creates new blind spots
- Attacks rising in volume and sophistication to capture illicit opportunities

Note: Attackers generally invest in [technical sophistication](#) only as needed

Anomaly
detection

Endpoint
protection

Hybrid cloud
security

Data & application
security

Fraud
prevention

Data loss
prevention

Infrastructure
security

Security
management

Threat
management

150+ security controls
500+ vendors

Data center
security

Cloud Access
Security Broker

Information rights
management

Identity & access
management

Compliance
tools

Threat
detection

IoT
security

Email
security

Most Common Malware Threats in Azerbaijan

Ramnit
24 471

February 2015

Module-based malware, stealing credential information from banking websites. Configured to hide itself.

**Credential
Information
Theft/Disable
Security Defenses**

Bladabindi &
Jenxcus
22 055

June 2014

Malware using Dynamic DNS for command. It involved password and identity theft, webcam and other privacy invasions. Over 200 different types of malware impacted by the take down.

**Identity Theft /
Financial Fraud /
Privacy Invasion**

Dorkbot
7 783

December 2015

Used for cyber criminal activities such as credential harvesting for financial fraud, DDoS attacks, and the downloading of malicious payloads. Disrupted in cooperation with FBI and international law enforcement.

**Financial Fraud /
DDoS attacks /
Malicious Payloads**

HOW WE HELP OUR CUSTOMERS ?

We invest
\$1B+ on security
R&D every year



Digital Crimes Unit

Leading the fight against cybercrime

Protecting people, organizations and our cloud through **global disruptions** and **enforcement actions** against cybercriminals

Investigations, forensics, and analytics

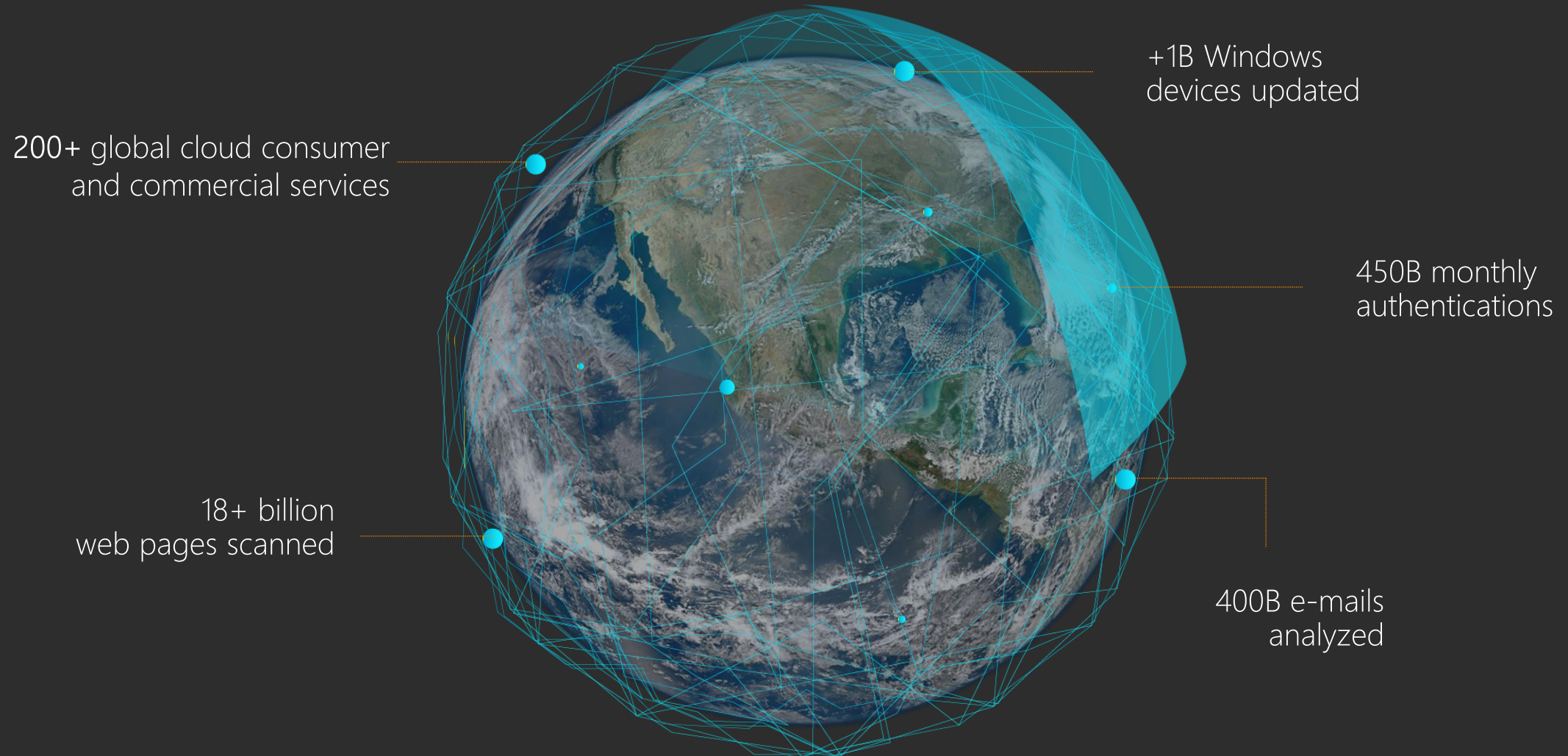
Machine learning, AI, and data visualization

Public and private partnerships

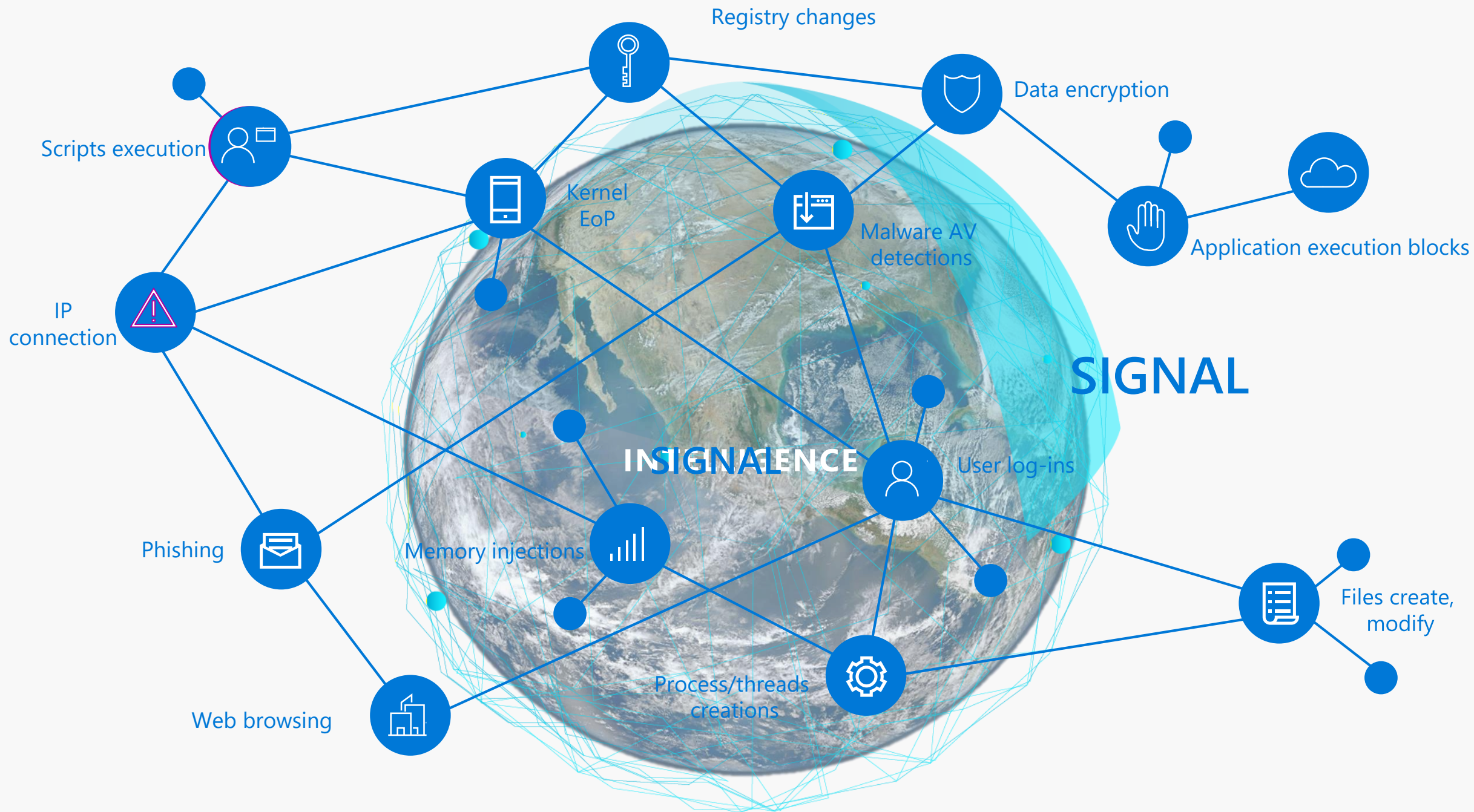
Creative legal strategies



THE MICROSOFT INTELLIGENT SECURITY GRAPH



Unparalleled cybersecurity visibility and insight



THREAT PROTECTION

Protect against advanced attacks; detect and respond quickly if breached



PROTECT

organizations from
advanced cyber attacks



DETECT

malicious activities



RESPOND

to threats quickly

PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

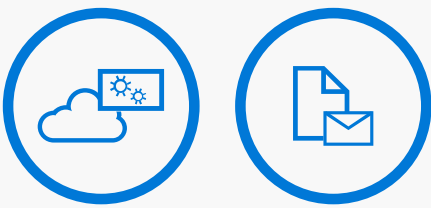
IDENTITY



PROTECT Users

- Identify advanced persistent threats
- Detect suspicious activity
- Reduce false positives

APPS & DATA



PROTECT Apps and Data

- Stop Malicious email attachments
- Avoid malicious email links
- Defend the gateway
- File inspection and remediation
- Mitigate shadow IT
- Automatically block over sharing
- Risk detection for data in cloud apps

DEVICES



PROTECT Your Devices

- Prevent encounters
- Isolate threats
- Control execution

INFRASTRUCTURE



PROTECT workloads across hybrid infrastructure

- Assess security state continuously
- Remediate vulnerabilities and drive compliance
- Enable security controls

DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

DETECT compromised
user credentials

DETECT malicious apps
and data

DETECT advanced threats
and abnormal behavior

DETECT advanced threats to
hybrid workloads

IDENTITY



APPS & DATA



DEVICES



INFRASTRUCTURE



RESPOND TO THREATS QUICKLY

RESPOND to compromised identities

RESPOND to compromised apps and data

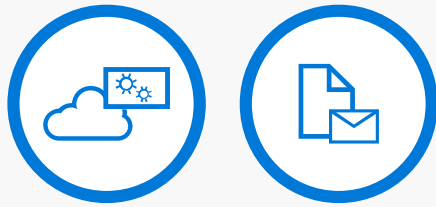
RESPOND to compromised devices

RESPOND early to compromised workloads across hybrid infrastructure

IDENTITY



APPS & DATA



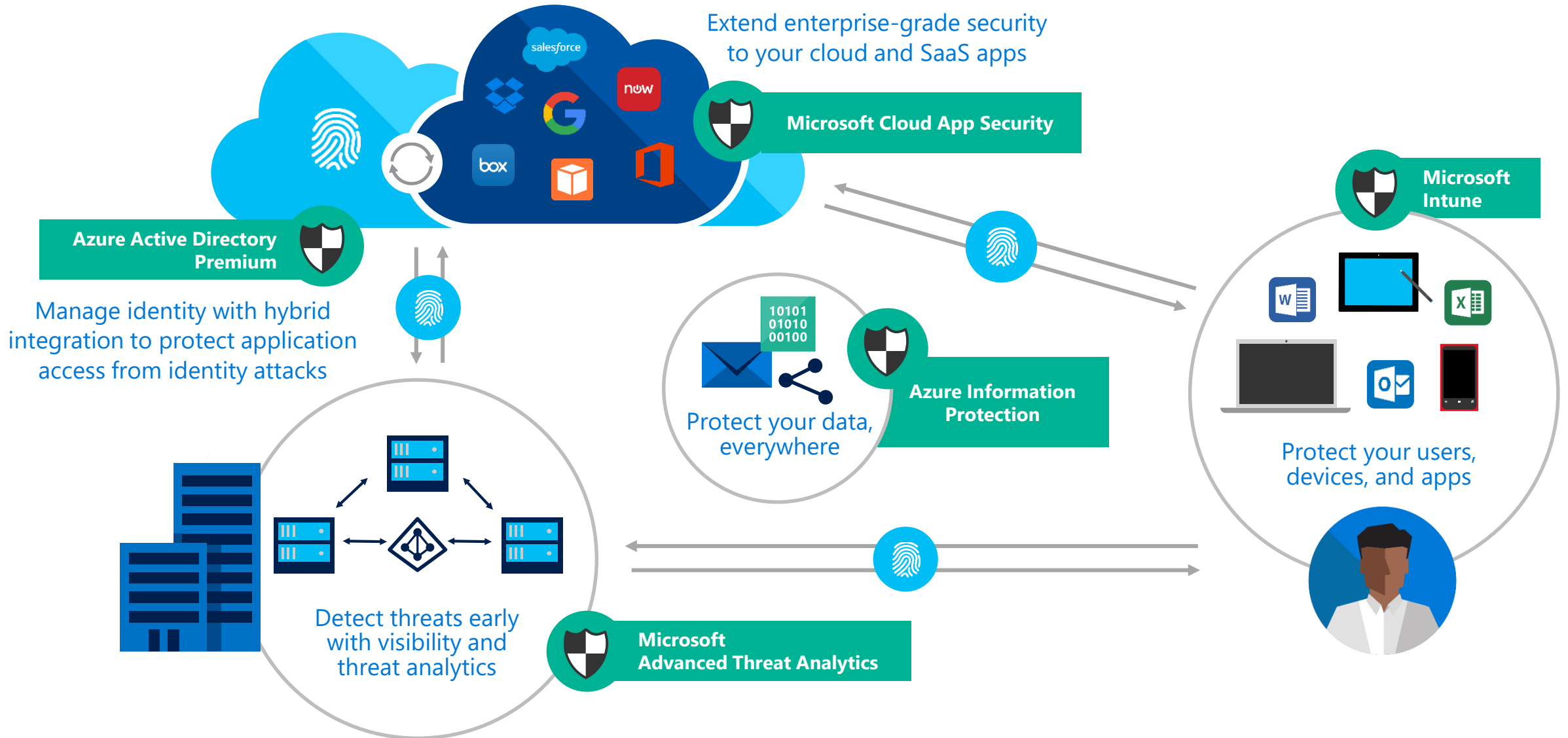
DEVICES



INFRASTRUCTURE



Enterprise Mobility + Security



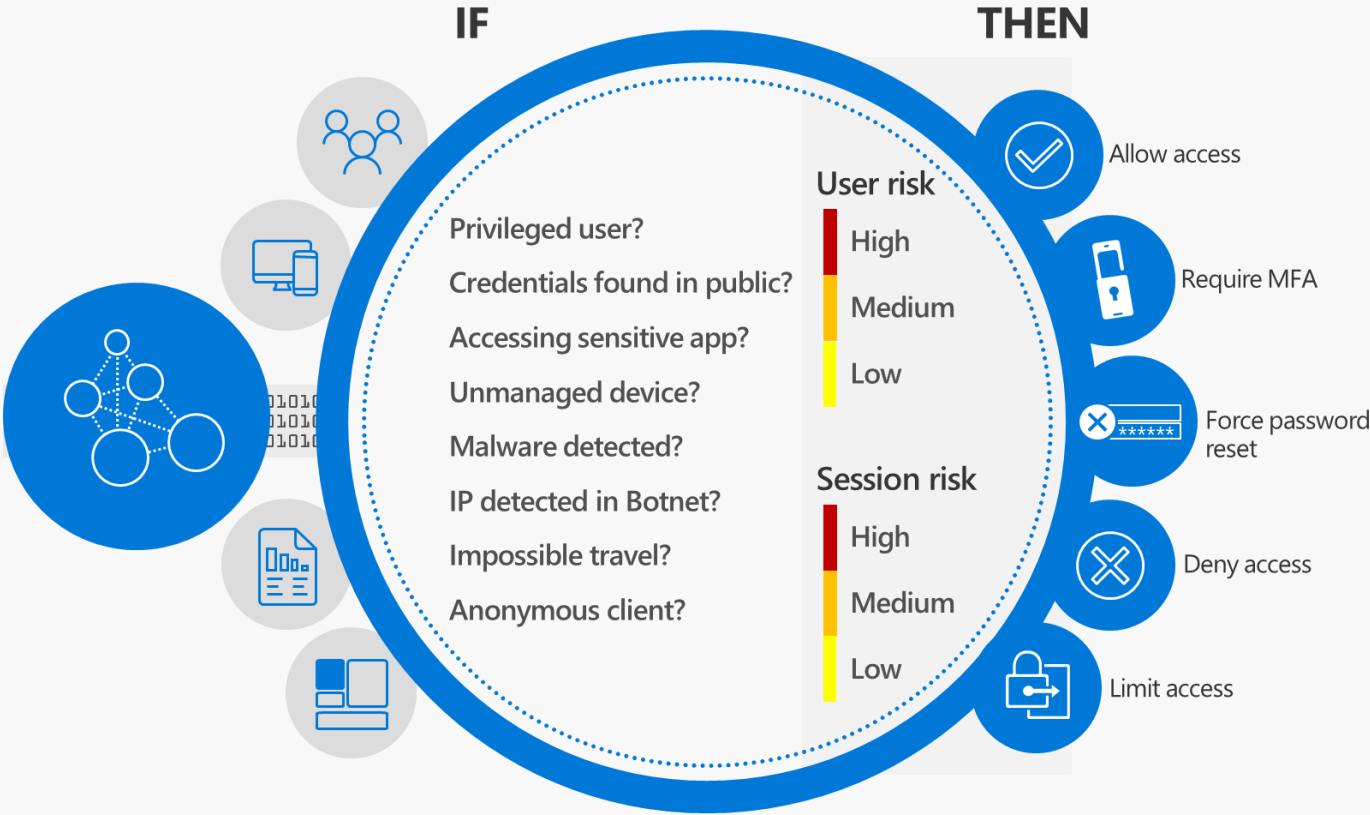
DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR USERS

IDENTITY



USE **CONDITIONAL ACCESS** TO
PROTECT YOUR ORGANIZATION
AT THE FRONT DOOR

CONTROL AND PROTECT
PRIVILEGED IDENTITIES



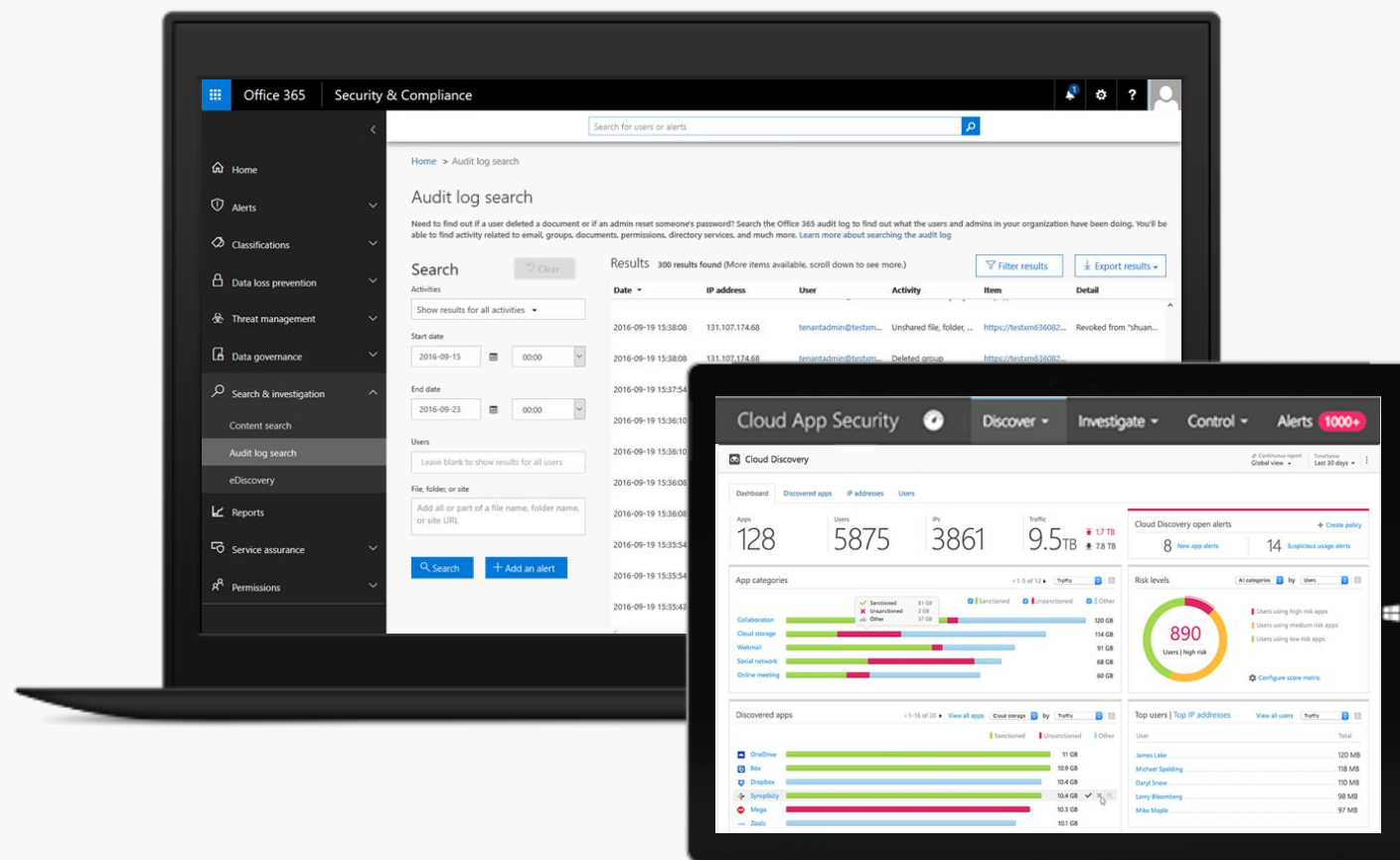
UNDERSTAND SECURITY STATE OF APPS & DATA



GAIN VISIBILITY INTO **CLOUD APPS** USED IN YOUR ENVIRONMENT & GET A **RISK ASSESSMENT**

AUDIT LOGS AND REPORTS TO HELP **DETECT ACTIVITY** WITHIN PRODUCTIVITY APPS

ALERTS TO HELP YOU **SEE ANOMALOUS ACTIVITY**





All apps

Security score
OK

View dashboard for a specific app

- ✓ Microsoft SharePoint Online
- ✓ Google Apps
- ✓ Box
- ✓ Salesforce
- ✓ Jive Software
- ✓ Office 365
- ✓ SuccessFactors
- ✓ Microsoft Cloud App Security
- ✓ Microsoft Exchange Online
- ✓ Microsoft Office 365 Portal
- ✓ Microsoft Office Online
- ✓ Microsoft OneDrive
- ✓ Microsoft Skype for Business
- ✓ Okta
- ✓ Yammer

[View all apps...](#)

Dashboard

3.5M
activities monitored203
files monitored3.2K
users monitored0
activities blocked1.4K
governance actions taken0
user notifications sent24 Open alerts
New over the last month ▾

RECENT ALERTS

**Suspicious Activity**
miah@acme.com
Google Apps

21 days ago

**Salesforce zombie account**
kenton@acme.com
Salesforce

21 days ago

**New admin location**
rolando@acme.com
Office 365

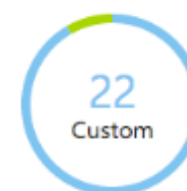
21 days ago

[View all alerts...](#)

BY SEVERITY



BY ALERT TYPE



Top 3 alert types

- 1 Suspicious activity alert
- 1 Suspicious activity alert
- 1 Inactive account

0 Activity violations
New over the last month ▾0 Content violations
New over the last month ▾

The evolution of Information Protection

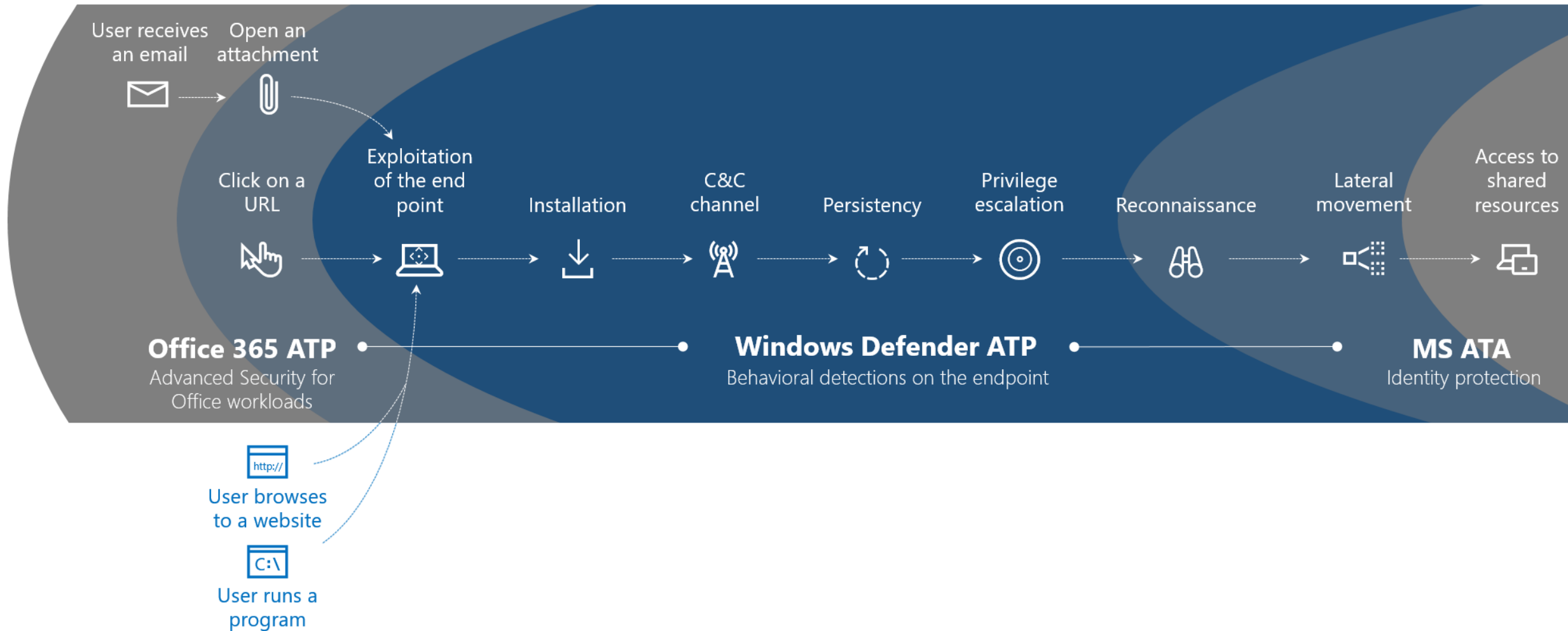


Classification
& labeling

Protect

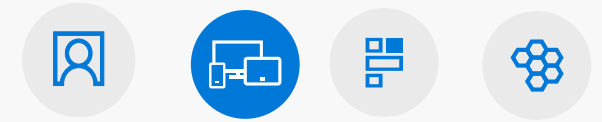
Monitor &
respond

MAXIMIZE DETECTION COVERAGE THROUGHOUT THE ATTACK STAGES



UNDERSTAND SECURITY STATE OF DEVICES

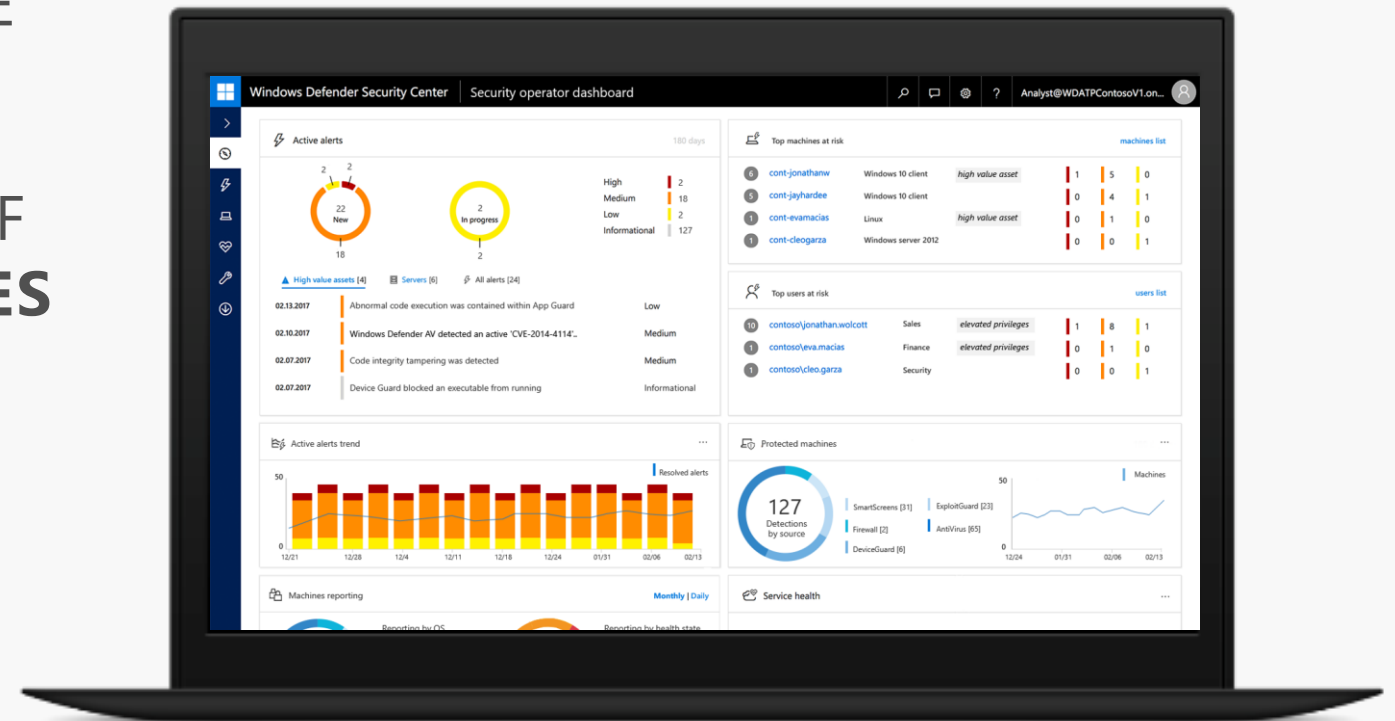
DEVICES



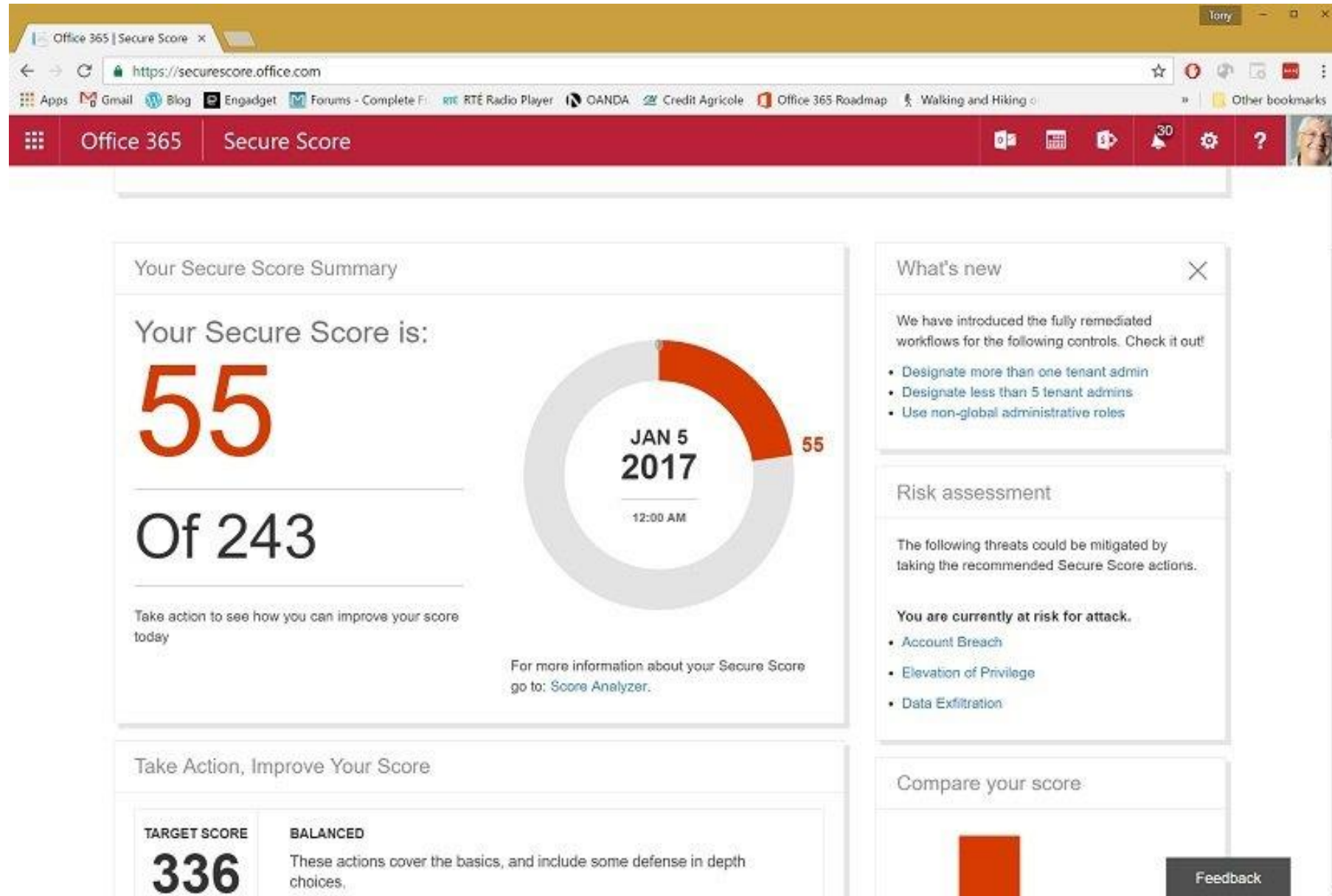
COMPLETE VISIBILITY INTO THE
ENDPOINT SECURITY

QUICKLY ASSESS THE SCOPE OF
INCIDENTS AND ROOT CAUSES

RICH TOOLSET FOR
**INVESTIGATION AND
REMEDIATION ACTIONS**



Credit Score vs. Secure Score



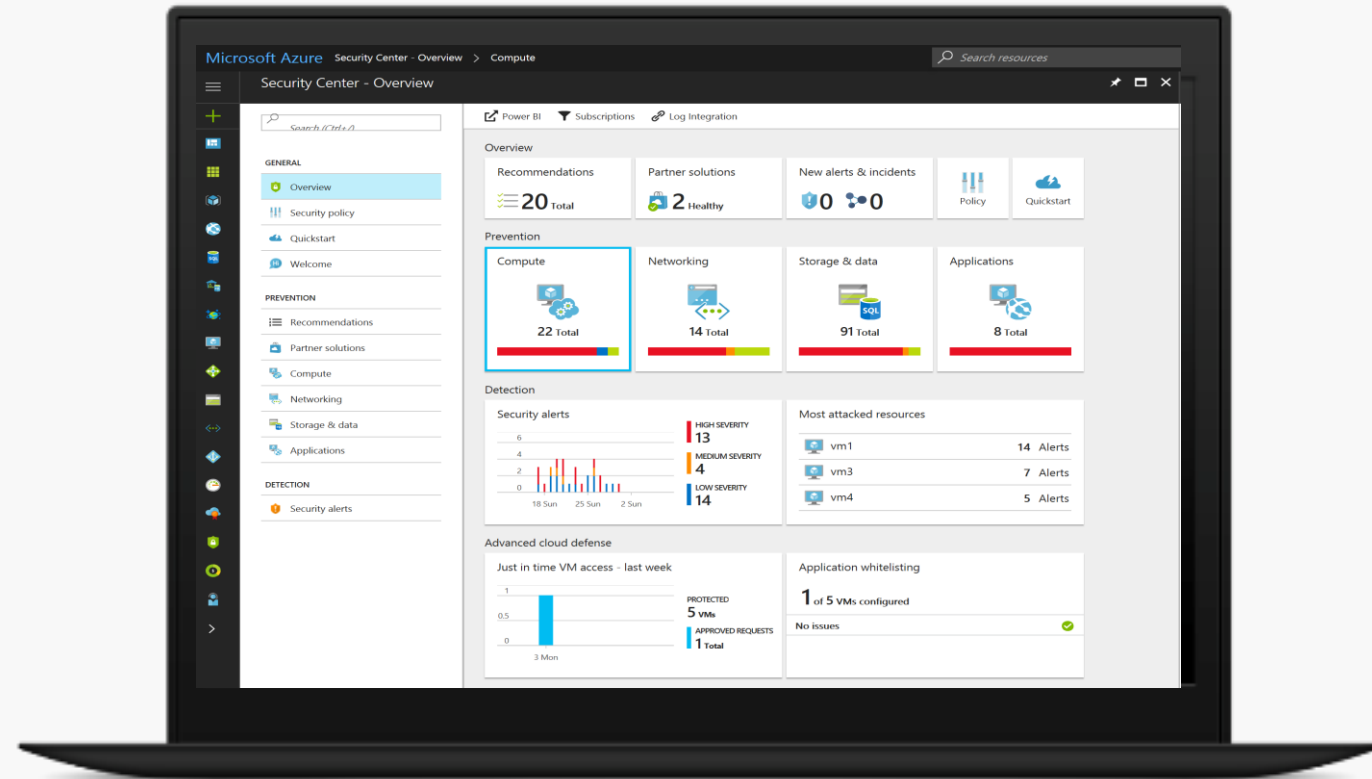
UNDERSTAND SECURITY STATE OF WORKLOADS ACROSS HYBRID INFRASTRUCTURE




MONITOR SECURITY STATE OF
RESOURCES ACROSS **CLOUD AND
ON-PREMISES**

IDENTIFY VULNERABILITIES
WITH CONTINUOUS ASSESSMENT

INVESTIGATE WITH **ADVANCED
LOG ANALYTICS AND SIEM
INTEGRATION**



Overview


Log Search



My Dashboard



Solutions Gallery


1.8GB
Usage

AD Assessment

3 Servers Assessed on Tue Jul 14 2015

3  High Priority Recommendations

2  Low Priority Recommendations

93  Passed Checks

Alert Management

1 Active critical alerts in the last 24 hours

15 Active warning alerts in the last 24 hours







Malware Assessment

25% NEEDS ATTENTION

0 Servers with Active Threats

25 Servers with Inadequate Protection





Automation

OMSAutomationdemo

3 Runbooks

3 Jobs in the last 7 days




Backup

OPI-Backup-EastAsia

1 Servers backed up

147.8MB Backup data

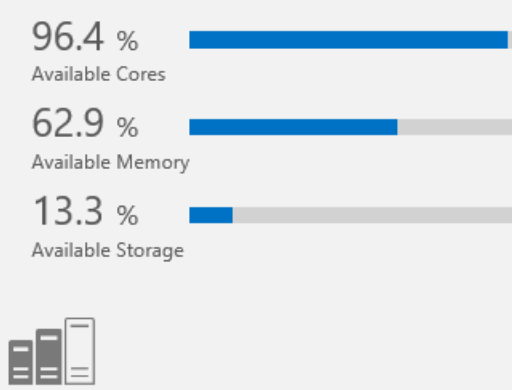


Capacity Planning

96.4 % Available Cores

62.9 % Available Memory

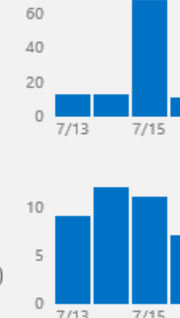
13.3 % Available Storage




Change Tracking


15 Software changes in the last 24 hours


10 Windows service changes in the last 24 hours (excludes Status)






Configuration Assessment

8  Servers with Alerts based on 364 rules

9  Servers with Recommendations based on 14.4K KB articles

112 Server Analyze




Overview ▶ Security And Audit

SECURITY POSTURE


94 ↓ 1

Active Computers



49 ↓ 3

Accounts Authenticated



30 ↓ 27

Activities in the System

210 ↓ 44

Processes Executed

0

User Accounts Changed

0

Policies Changed


4

Distinct IP Addresses Accessed

NOTABLE ISSUES

14 ↓ 1

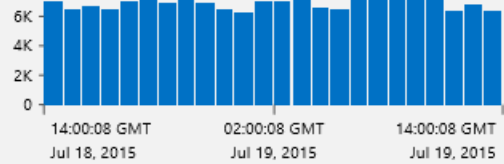
Notable issues



NAME	COUNT	CHANGE
Failed logons	14	↑ 5
Suspicious Executables	0	↓ 3
Change or Reset Passwords Attempts	0	↓ 1
Members Added to Security-Enabled Gro...	0	↓ 1
Security Groups Created or Modified	0	↓ 1
Computers with Cleaned Event Logs	0	0
Computers with System Audit Policy Chan...	0	0
Domain Security Policy Changes	0	0
Locked-out Accounts	0	0
Remote Procedure Call (RPC) attempts	0	0


CONTEXT

Log Records over time




0

Servers with active threats




24

Servers with inadequate protection




94

Servers missing security updates




80

Servers missing critical updates




15

Software changes




10

Windows service changes (excludes Status)




0

Active critical alerts



0

Active warning alerts



COMMON SECURITY QUERIES

All Security Activities
[Type=SecurityEvent | Select TimeGenerated,AccountName](#)

Security Activities on the computer "computer01.contoso.com"
[Type=SecurityEvent Computer="computer01.contoso.com"](#)

Security Activities on the computer "computer01.contoso.com" (excluding account names)
[Type=SecurityEvent Computer="computer01.contoso.com" | Where-Object { \\$_.AccountName -ne 'NT AUTHORITY\SYSTEM' }](#)

Logon Activity by Computer
[Type=SecurityEvent EventID=4624 | Measure-Object -Name Count -ForEach \\$Computer](#)

Accounts who terminated Microsoft antimalware
[Type=SecurityEvent EventID=4689 "MsMpEng.exe" | Measure-Object -Name Count -ForEach \\$Account](#)

Computers where the Microsoft antimalware was terminated
[Type=SecurityEvent EventID=4689 "MsMpEng.exe" | Measure-Object -Name Count -ForEach \\$Computer](#)

Computers where "hash.exe" was executed (regardless of user)
[Type=SecurityEvent EventID=4688 "hash.exe" | Measure-Object -Name Count -ForEach \\$Computer](#)

All Process names that were executed
[Type=SecurityEvent EventID=4688 | Measure-Object -Name Count -ForEach \\$ProcessName](#)

Logon Activity by Account
[Type=SecurityEvent EventID=4624 | Measure-Object -Name Count -ForEach \\$Account](#)

Accounts who remotely logged on the computer "computer01.contoso.com"
[Type=SecurityEvent EventID=4624 AND \(LogonType=3 OR LogonType=10\) Computer="computer01.contoso.com" | Measure-Object -Name Count -ForEach \\$Account](#)

Feedback

?

1



OUR COMMITMENT TO **YOU**



TRANSPARENCY



PRIVACY & CONTROL



COMPLIANCE



SECURITY



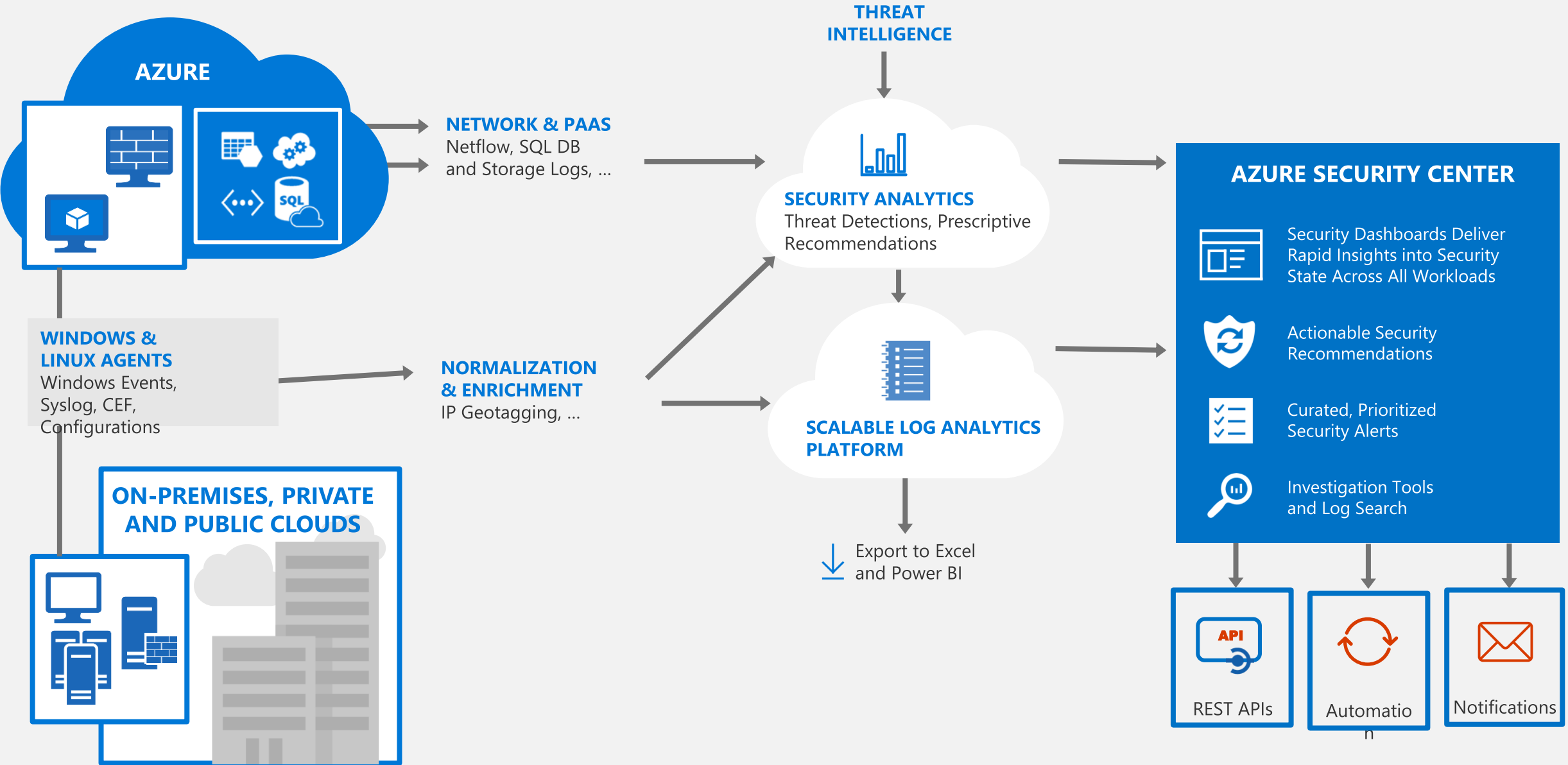
Thank you



Security threats

Threats	Motives/Goals	Methods
Non malicious Ignorance Accidents Neglect Malicious Organized crime Terrorist organizations Cyber criminals Governments Hackers Crackers Natural disasters Riots and wars	Deny services Steal information Alter information Damage information Delete information Make a joke Show off	DDOS Social engineering Phishing Spoofing Watering hole Viruses Trojan horses Worms Malware Ransomware And many more....

Architecture



Building an Integrated Security Experience

