Microsoft Threat Protection

Protection Against Modern Attack Vectors

Microsoft

OUR COMMITMENT TO **YOU**

- SECURITY
- PRIVACY & CONTROL
- COMPLIANCE
- TRANSPARENCY
- RELIABILITY

"CYBER SECURITY IS A **CEO ISSUE.**"

-MCKINSEY

$4.0M
is the average cost of a data breach per incident.

81%
of breaches involve weak or stolen passwords.

>300K
new malware samples are created and spread every day.

87%
of senior managers have admitted to accidentally leaking business data.

CYBER THREATS ARE A **MATERIAL RISK** TO YOUR BUSINESS

Sources: McKinsey, Ponemon Institute, Verizon, Microsoft

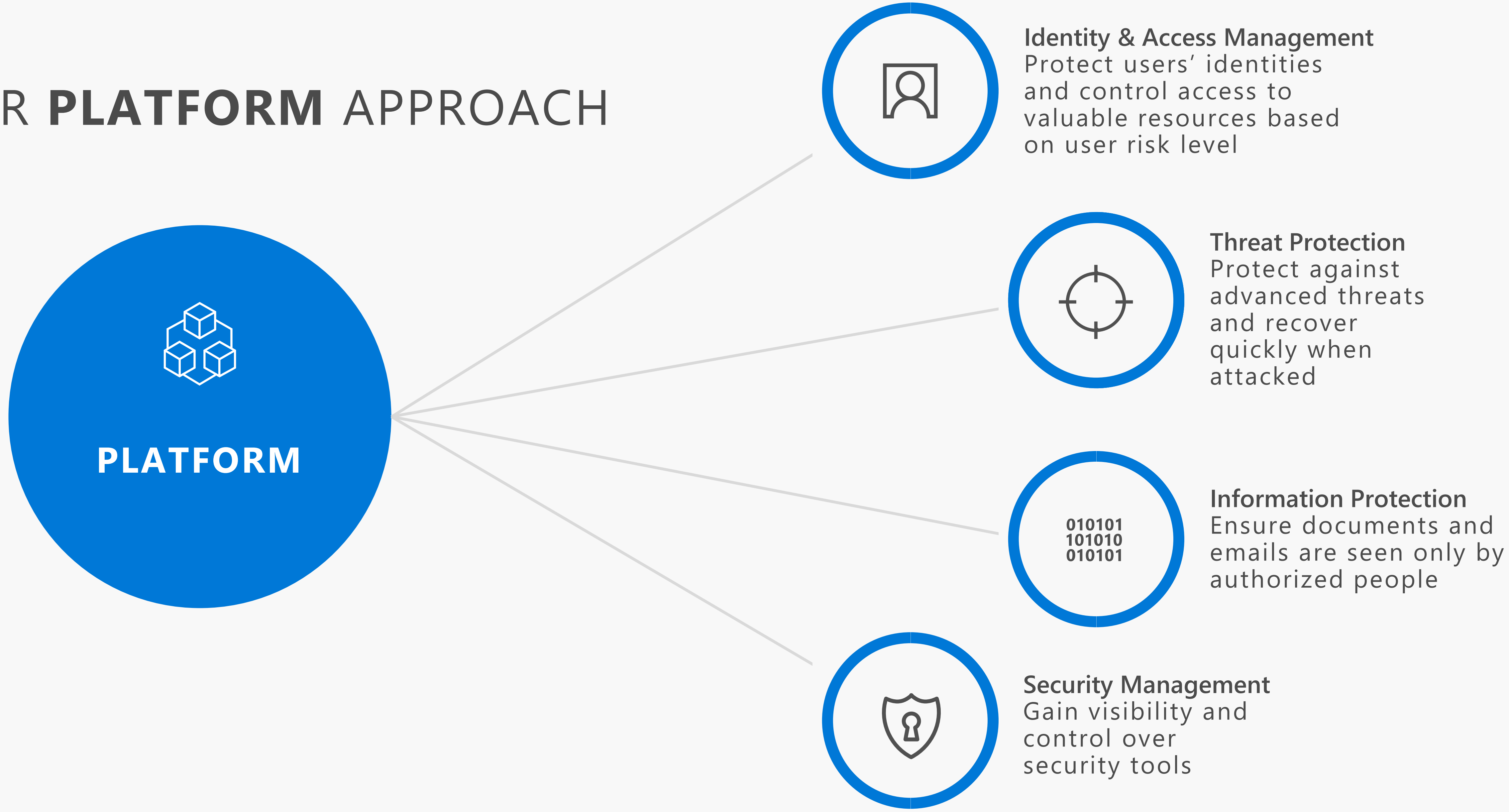
OUR **UNIQUE** APPROACH

PLATFORM

INTELLIGENCE

PARTNERS

OUR **PLATFORM** APPROACH



PLATFORM

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

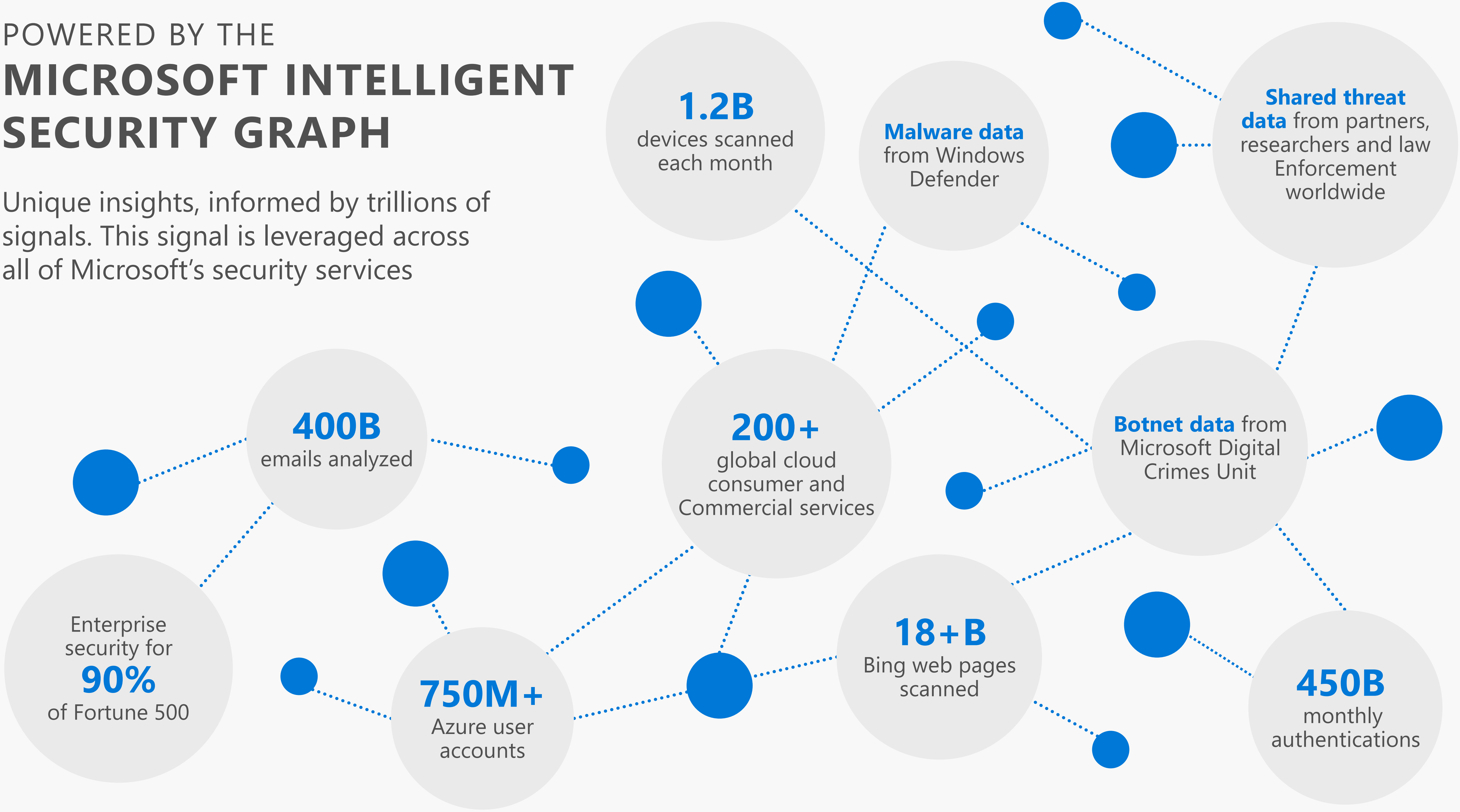
Information Protection
Ensure documents and emails are seen only by authorized people

Security Management
Gain visibility and control over security tools

POWERED BY THE

MICROSOFT INTELLIGENT SECURITY GRAPH

Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services



1.2B devices scanned each month

Malware data from Windows Defender

Shared threat data from partners, researchers and law Enforcement worldwide

400B emails analyzed

200+ global cloud consumer and Commercial services

Botnet data from Microsoft Digital Crimes Unit

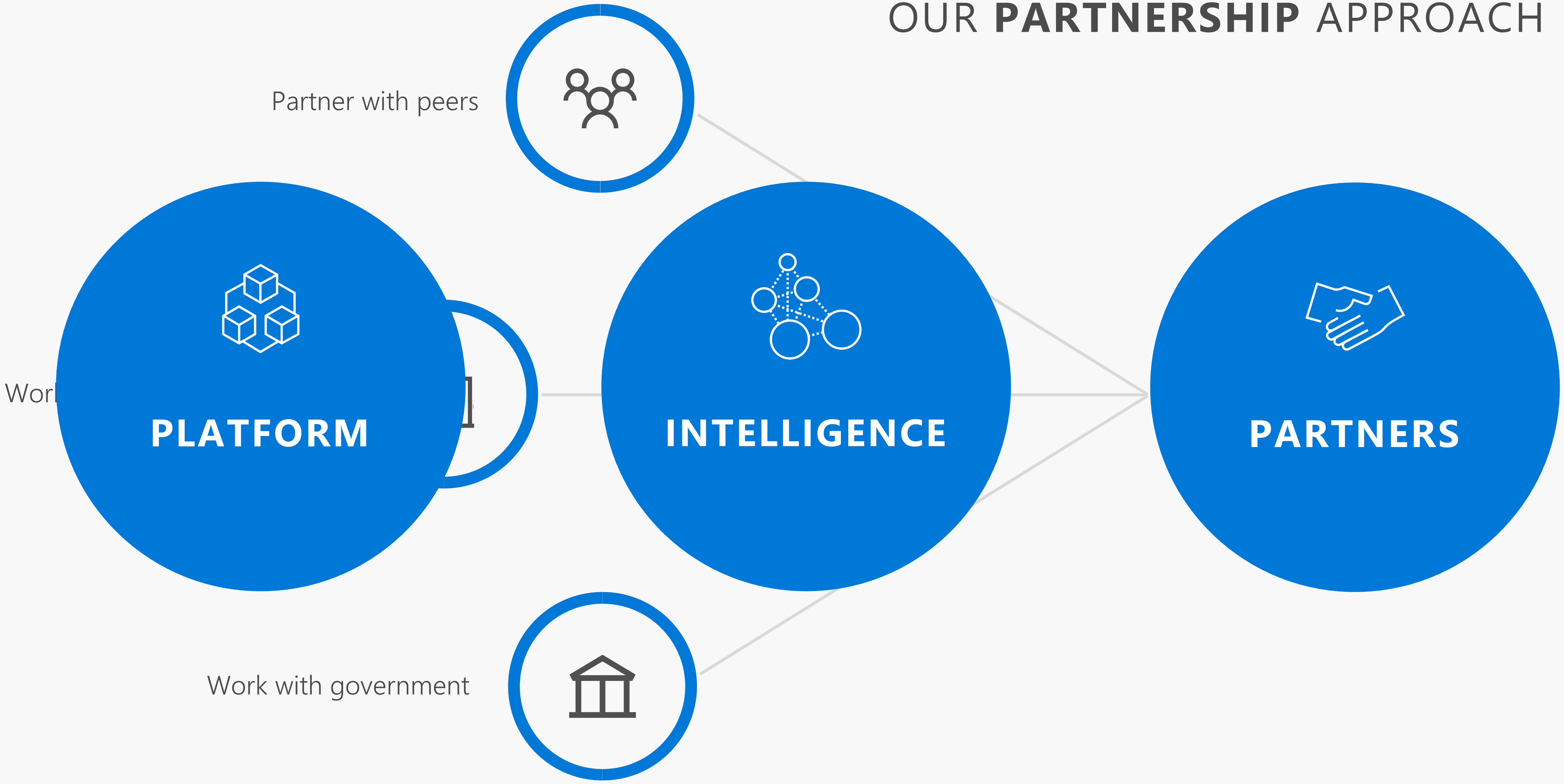
Enterprise security for **90%** of Fortune 500

750M+ Azure user accounts

18+B Bing web pages scanned

450B monthly authentications

OUR **PARTNERSHIP** APPROACH



Partner with peers

Wor

PLATFORM

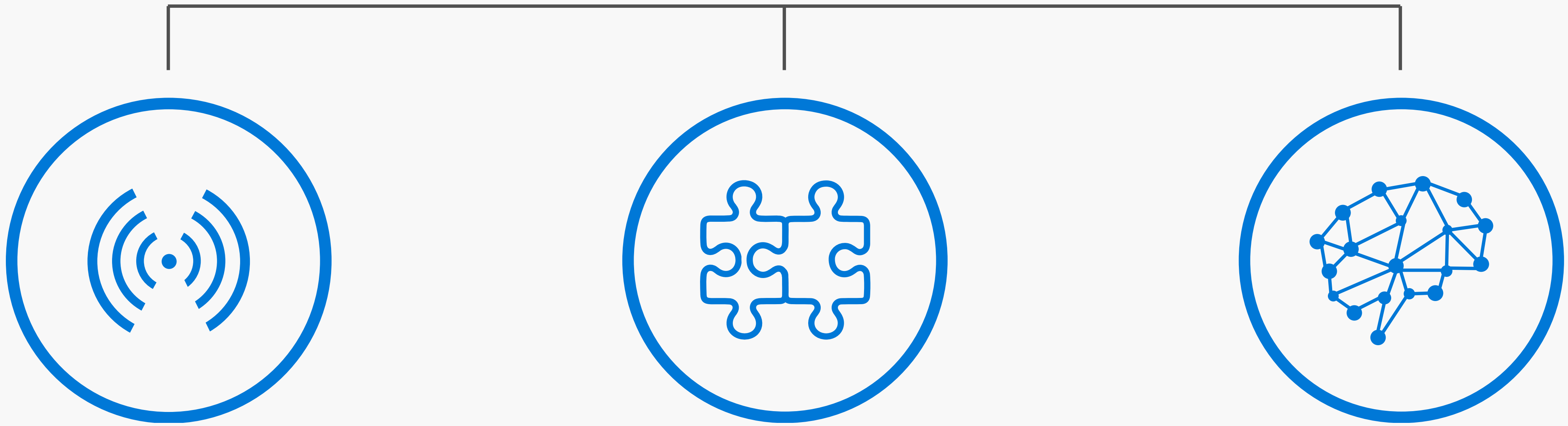
INTELLIGENCE

PARTNERS

Work with government

BUILDING ON OUR **STRENGTHS**

THE MICROSOFT INTELLIGENT SECURITY GRAPH ENABLES



Signal Breadth

Integrated Intelligence

Machine Learning/AI

TO **HELP OUR CUSTOMERS** WITH THEIR CHALLENGES

Exposure to Advanced Attacks

The escalation in the number of threats and sophistication of these threats leave many organizations more exposed to attacks.

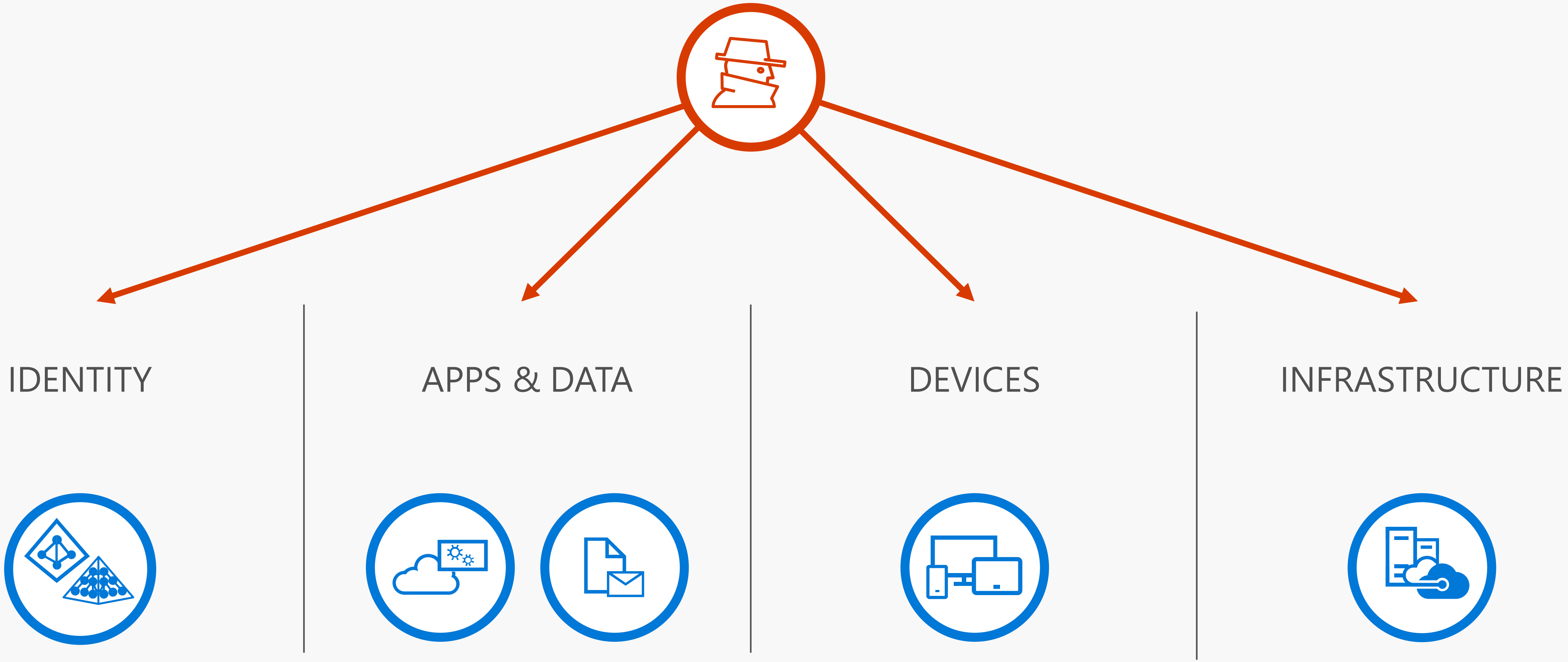
Inability to Detect Malicious Activity

With the volume of threats and enhanced capabilities of attackers, detection of malicious activity has become increasingly difficult.

Difficulty in Responding to Threats Quickly

It is often difficult to know how to respond to a threats and the length of time to respond can add to the devastating effects of a breach.

UNDERSTANDING YOUR **VULNERABILITIES**



IDENTITY

APPS & DATA

DEVICES

INFRASTRUCTURE

MICROSOFT CAN HELP **SOLVE THE CUSTOMER CHALLENGES**

PROTECT
organizations from advanced cyber attacks

DETECT
malicious activities

RESPOND
to threats quickly

PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

PROTECT Users

Identify advanced persistent threats

Detect suspicious activity

Reduce false positives

IDENTITY

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

APPS & DATA

PROTECT Your Devices

Prevent encounters

Isolate threats

Control execution

DEVICES

PROTECT workloads across hybrid infrastructure

Assess security state continuously

Remediate vulnerabilities and drive compliance

Enable security controls

INFRASTRUCTURE

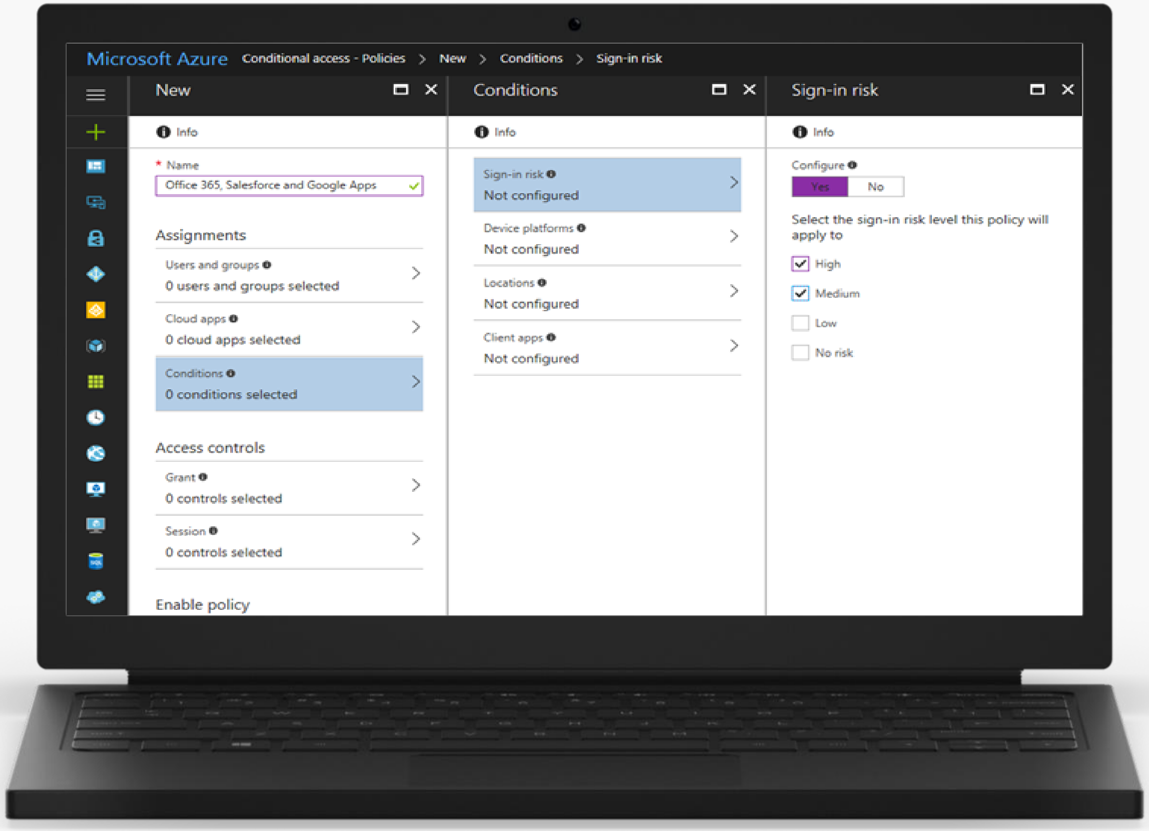
PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

Protect Your Users

Protect your organization at the front door with risk-based conditional access

Detect known security vulnerabilities and risks in your organization based on world-class security research

Discover, control and protect your admin accounts with privileged identity management



Microsoft Azure Conditional access - Policies > New > Conditions > Sign-in risk

New

Info

* Name: Office 365, Salesforce and Google Apps ✓

Assignments

- Users and groups: 0 users and groups selected
- Cloud apps: 0 cloud apps selected
- Conditions: 0 conditions selected

Access controls

- Grant: 0 controls selected
- Session: 0 controls selected

Enable policy

Conditions

Info

- Sign-in risk: Not configured
- Device platforms: Not configured
- Locations: Not configured
- Client apps: Not configured

Sign-in risk

Info

Configure: [✓ Yes] No

Select the sign-in risk level this policy will apply to

☑ High

☑ Medium

☐ Low

☐ No risk

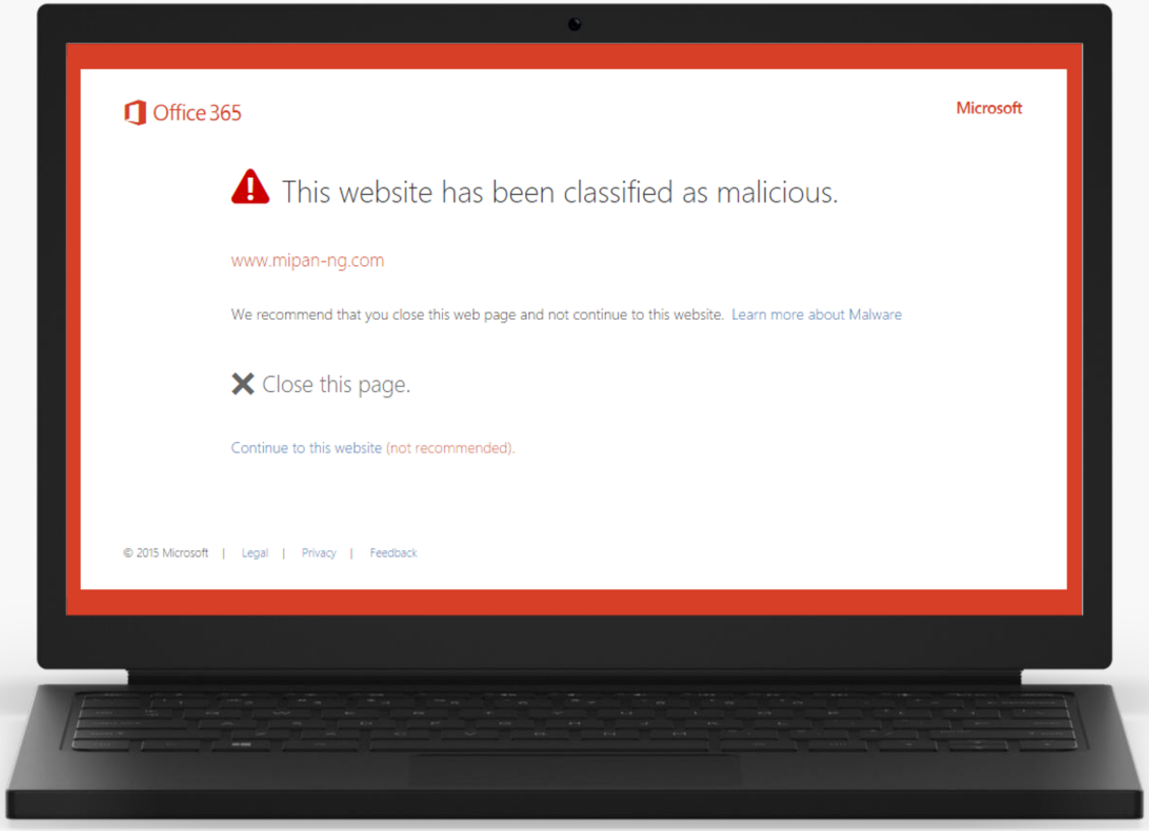
PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

Protect Your Email

Stop malicious attachments

Provide time of click protection against malicious links

Stop known email threats



Office 365 Microsoft

⚠ This website has been classified as malicious.

www.mipan-ng.com

We recommend that you close this web page and not continue to this website. Learn more about Malware

✕ Close this page.

Continue to this website (not recommended).

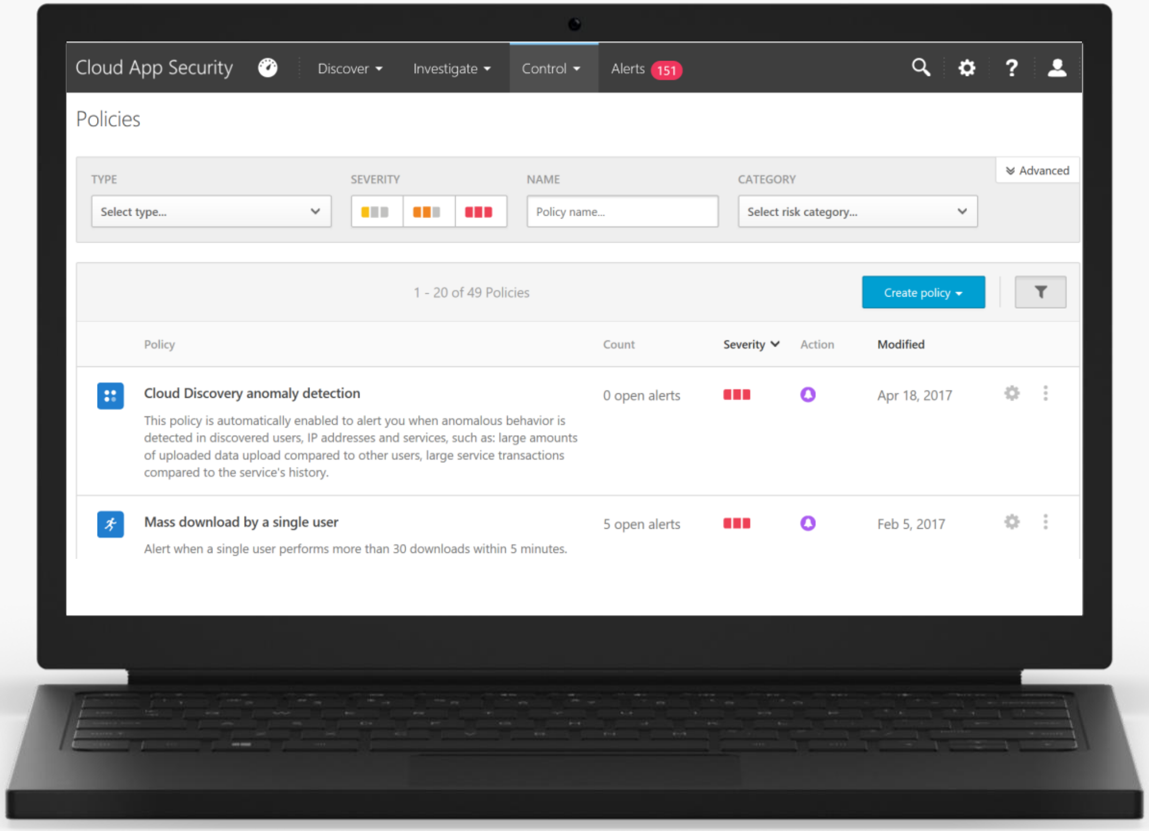
© 2015 Microsoft | Legal | Privacy | Feedback

PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

Protect Apps & Data

Control and protect data in cloud apps with granular policies & enhanced threat protection (Cloud Access security Broker)

Advanced security for all Office files as well as documents in cross-SaaS apps



Policy	Count	Severity	Action	Modified
Cloud Discovery anomaly detection This policy is automatically enabled to alert you when anomalous behavior is detected in discovered users, IP addresses and services, such as: large amounts of uploaded data upload compared to other users, large service transactions compared to the service's history.	0 open alerts	■■■	🔔	Apr 18, 2017
Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	5 open alerts	■■■	🔔	Feb 5, 2017

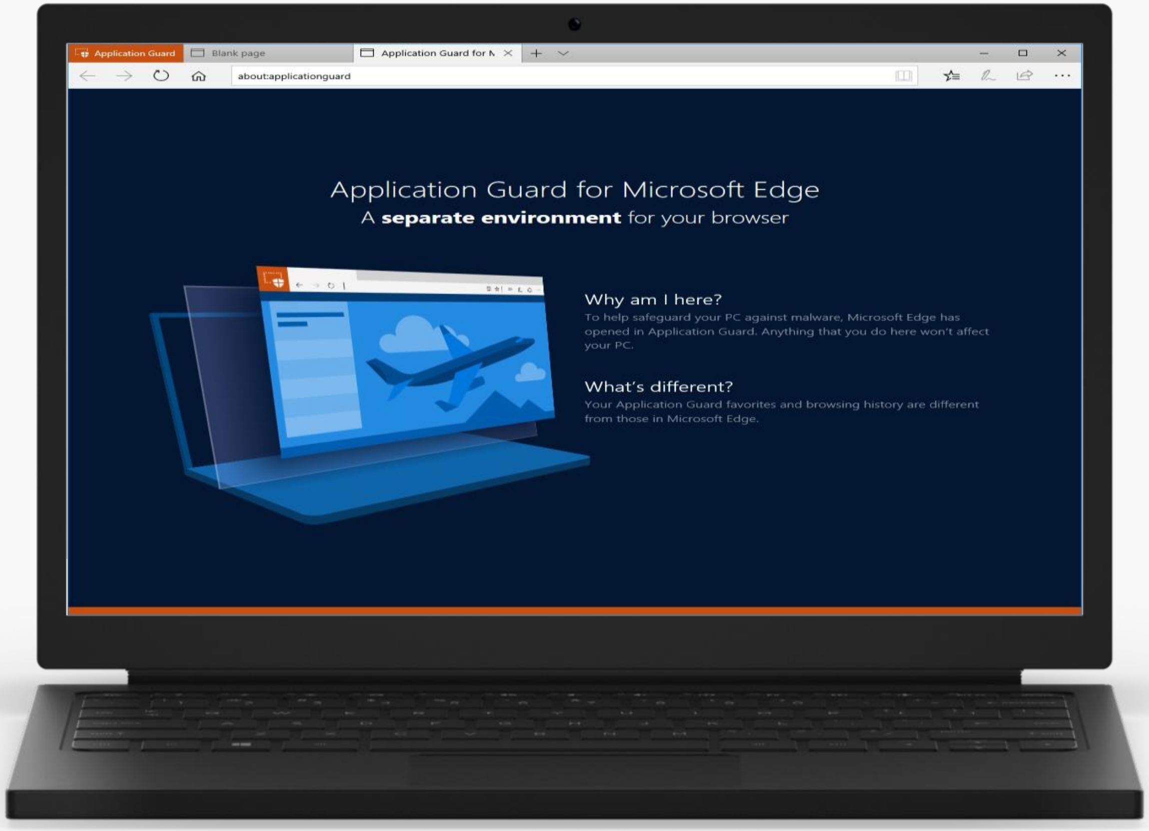
PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

Protect Your Devices

Built-in next generation threat protection technologies

Using the power of the cloud to block malicious apps and websites

Stops attackers from establishing a foothold on the local machine



Application Guard for Microsoft Edge

A **separate environment** for your browser

Why am I here?

To help safeguard your PC against malware, Microsoft Edge has opened in Application Guard. Anything that you do here won't affect your PC.

What's different?

Your Application Guard favorites and browsing history are different from those in Microsoft Edge.

PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

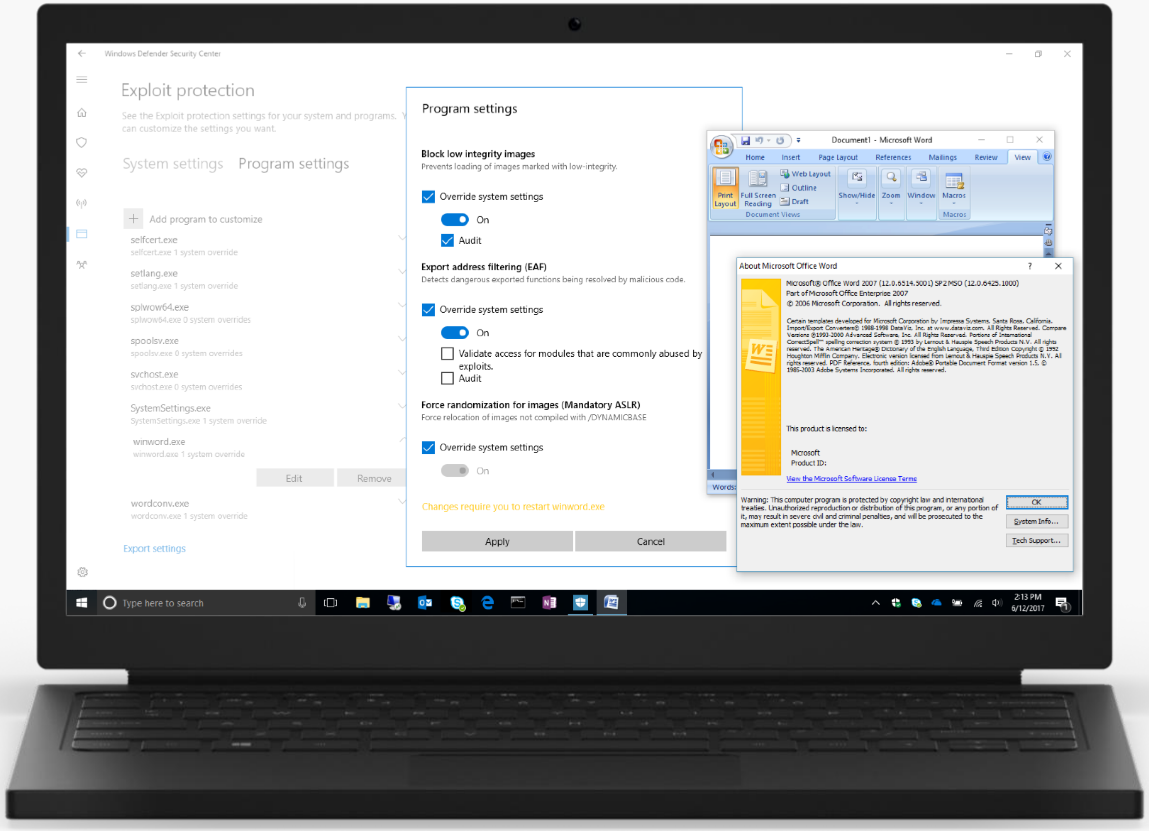
Protect Your Devices

Isolate sensitive windows components and data which

Prevent exploitation of vulnerabilities, host intrusion and files-less based attacks

Block malicious unauthorized apps using application control

Stop the execution of malicious apps and behaviors



Windows Defender Security Center

Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

System settings   Program settings

+ Add program to customize

selfcert.exe
selfcert.exe 1 system override

setlang.exe
setlang.exe 1 system override

splwow64.exe
splwow64.exe 0 system overrides

spoolsv.exe
spoolsv.exe 0 system overrides

svchost.exe
svchost.exe 0 system overrides

SystemSettings.exe
SystemSettings.exe 1 system override

winword.exe
winword.exe 1 system override

wordconv.exe
wordconv.exe 1 system override

Export settings

Program settings

Block low integrity images
Prevents loading of images marked with low-integrity.

☑ Override system settings
On
☑ Audit

Export address filtering (EAF)
Detects dangerous exported functions being resolved by malicious code.

☑ Override system settings
On
☐ Validate access for modules that are commonly abused by exploits.
☐ Audit

Force randomization for images (Mandatory ASLR)
Force relocation of images not compiled with /DYNAMICBASE

☑ Override system settings
On

Changes require you to restart winword.exe

Document1 - Microsoft Word

About Microsoft Office Word

Microsoft® Office Word 2007 (12.0.6514.5001) SP2 MSO (12.0.6425.1000)
Part of Microsoft Office Enterprise 2007
© 2006 Microsoft Corporation. All rights reserved.

Certain templates developed for Microsoft Corporation by Impressa Systems, Santa Rosa, California. Import/Export Converters© 1988-1998 DataViz, Inc. at www.dataviz.com. All Rights Reserved. Compare Versions ©1993-2000 Advanced Software, Inc. All Rights Reserved. Portions of International CorrectSpell™ spelling correction system © 1993 by Lernout & Hauspie Speech Products N.V. All rights reserved. The American Heritage® Dictionary of the English Language, Third Edition Copyright © 1992 Houghton Mifflin Company. Electronic version licensed from Lernout & Hauspie Speech Products N.V. All rights reserved. PDF Reference, fourth edition: Adobe® Portable Document Format version 1.5. © 1985-2003 Adobe Systems Incorporated. All rights reserved.

This product is licensed to:

Microsoft
Product ID:

View the Microsoft Software License Terms

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2:13 PM
6/12/2017

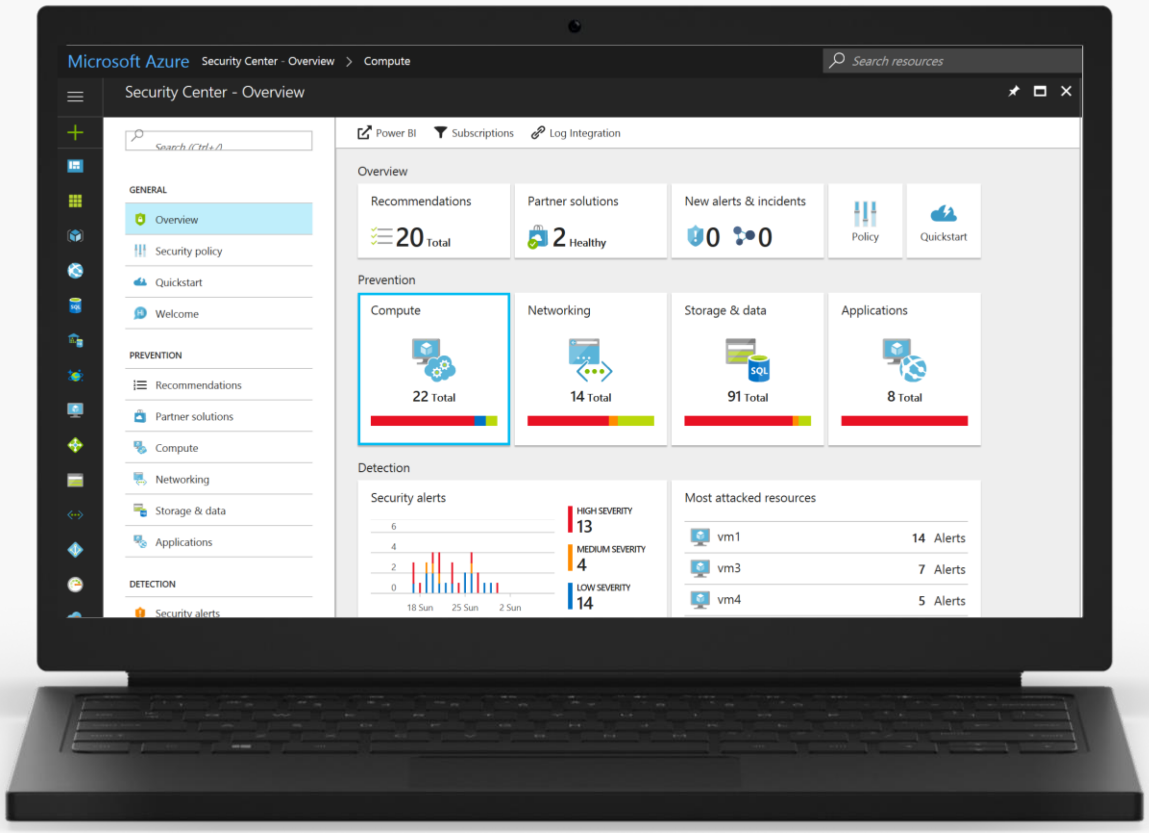
PROTECT ORGANIZATIONS FROM ADVANCED CYBER ATTACKS

Protect Workloads Across Hybrid Infrastructure

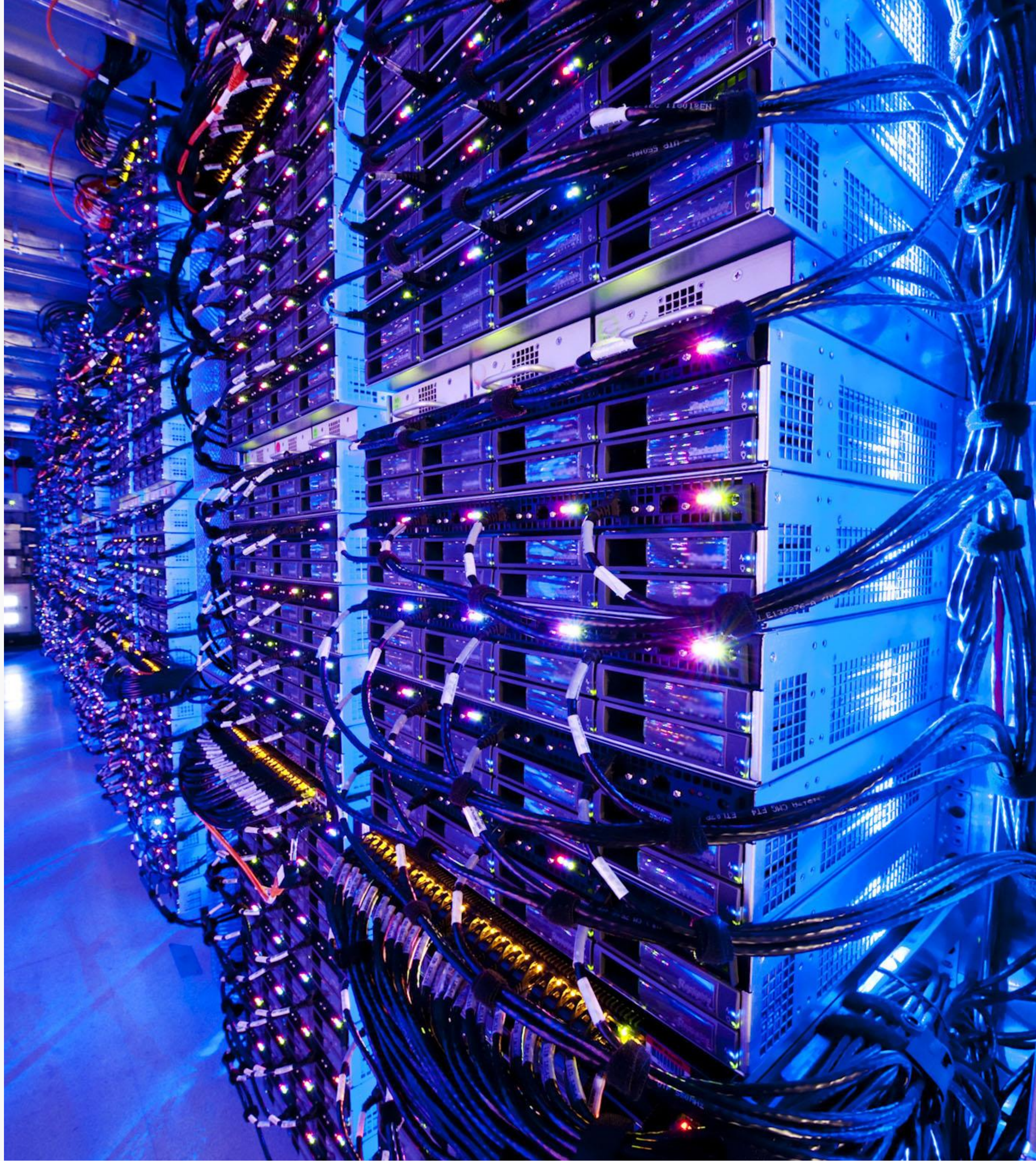
Mitigate vulnerabilities with continuous assessment and recommendations

Reduce attack surface with application whitelisting, just in time access to ports

Rapidly deploy security controls from Microsoft and partners to cloud workloads



HOWEVER WE LIVE IN A WORLD WHERE **BREACHES STILL OCCUR**



DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

DETECT compromised user credentials

IDENTITY

DETECT malicious apps and data

APPS & DATA

DETECT advanced threats and abnormal behavior

DEVICES

DETECT advanced threats to hybrid workloads

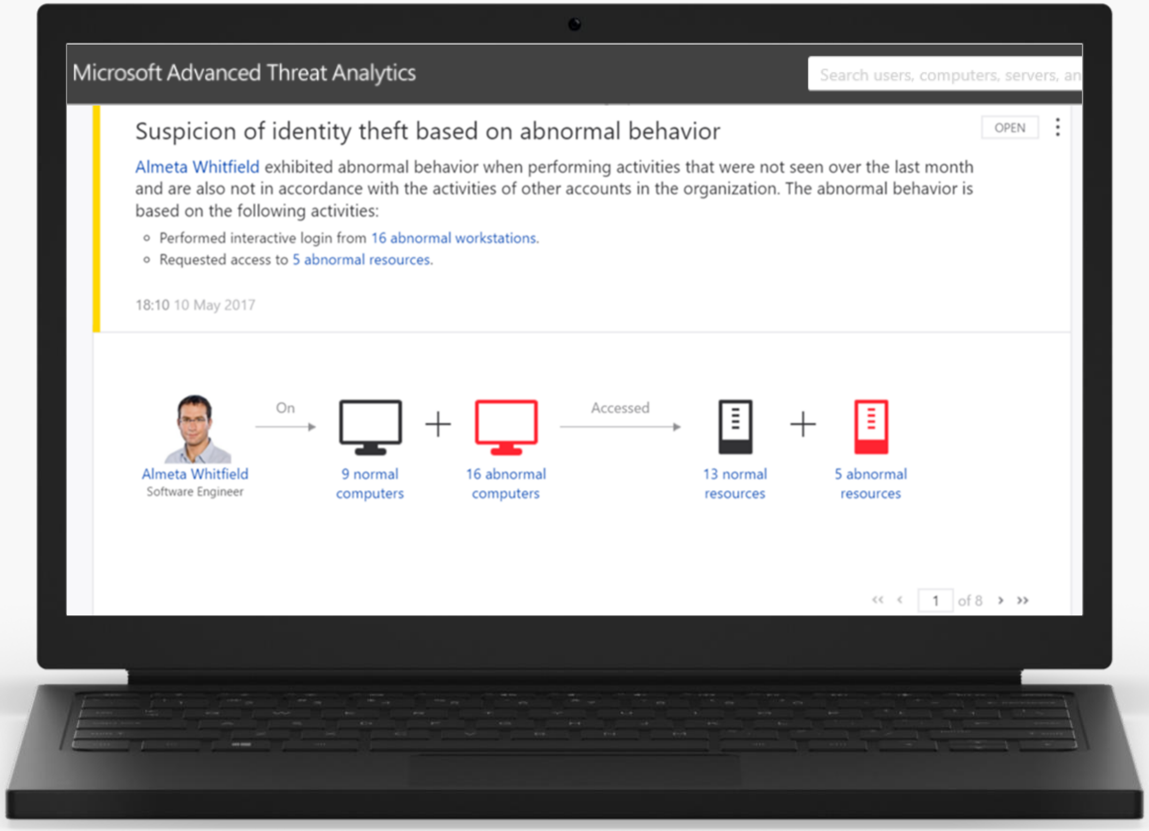
INFRASTRUCTURE

DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

Detect Abnormal Identity Behavior & Malicious Attacks On-Premises

Detect suspicious behavior and anomalies using behavioral analytics on-premises & in the cloud

Identify malicious attacks inside your network leveraging machine learning (i.e. Pass-the-Hash, Pass-the-Ticket, lateral movement)


Microsoft Advanced Threat Analytics
Search users, computers, servers, an
OPEN

Suspicion of identity theft based on abnormal behavior

Almeta Whitfield exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 16 abnormal workstations.
- Requested access to 5 abnormal resources.

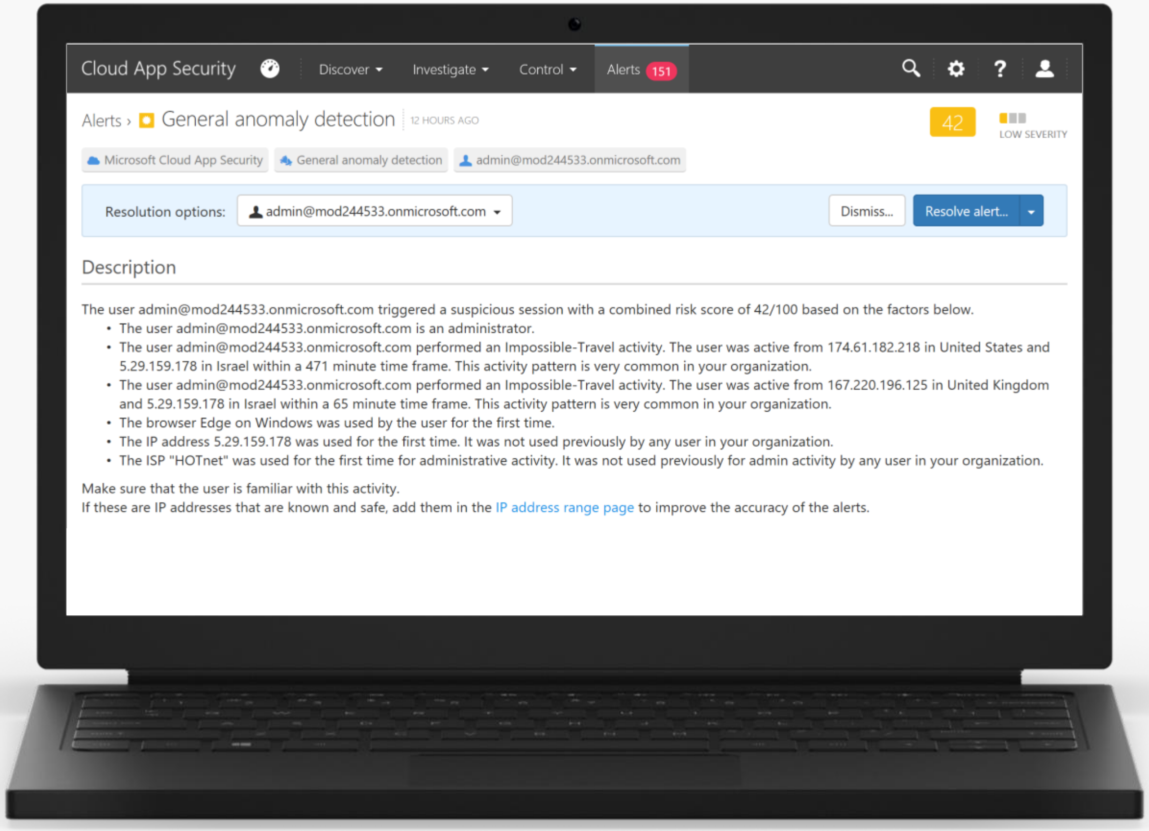
18:10 10 May 2017

DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

Detect Abnormal Behavior & Anomalies in Cloud Apps

Identify high risk usage, cloud security issues, detect abnormal user behavior in cloud apps.

Identify and stop known attack pattern activities originating from risky sources with threat prevention enhanced with vast Microsoft threat intelligence



Resolution options: admin@mod244533.onmicrosoft.com

The user admin@mod244533.onmicrosoft.com triggered a suspicious session with a combined risk score of 42/100 based on the factors below.

- The user admin@mod244533.onmicrosoft.com is an administrator.
- The user admin@mod244533.onmicrosoft.com performed an Impossible-Travel activity. The user was active from 174.61.182.218 in United States and 5.29.159.178 in Israel within a 471 minute time frame. This activity pattern is very common in your organization.
- The user admin@mod244533.onmicrosoft.com performed an Impossible-Travel activity. The user was active from 167.220.196.125 in United Kingdom and 5.29.159.178 in Israel within a 65 minute time frame. This activity pattern is very common in your organization.
- The browser Edge on Windows was used by the user for the first time.
- The IP address 5.29.159.178 was used for the first time. It was not used previously by any user in your organization.
- The ISP "HOTnet" was used for the first time for administrative activity. It was not used previously for admin activity by any user in your organization.

Make sure that the user is familiar with this activity.
If these are IP addresses that are known and safe, add them in the IP address range page to improve the accuracy of the alerts.

DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

Visibility into Malicious Emails/ Files and Activity

Access message and url trace reports

Determine email attachment detonation results

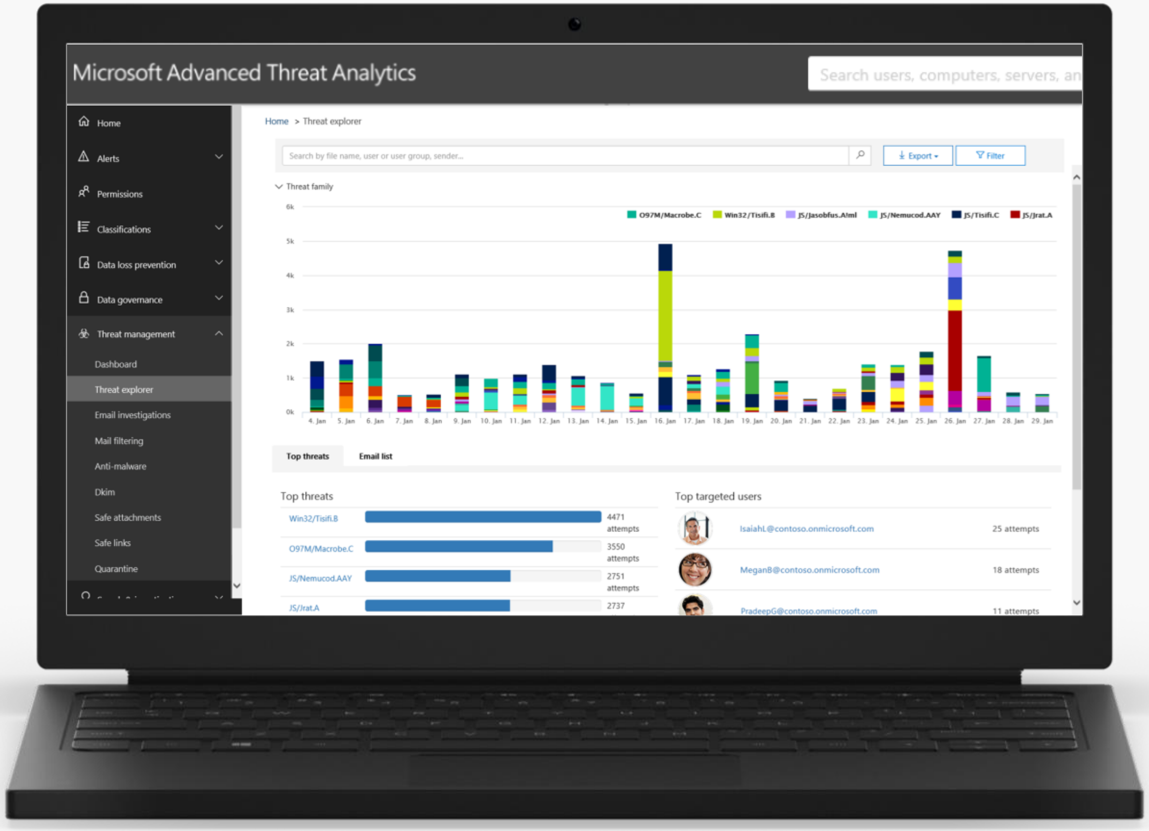
Gain visibility into the threat landscape

Determine top targeted users

Read detailed campaign reports

Monitor cloud app usage

Monitor end user behavior patterns to determine anomalous behavior



Top threats

Win32/Tisifi.B	4471 attempts
O97M/Macrobe.C	3550 attempts
JS/Nemucod.AAY	2751 attempts
JS/Jrat.A	2737

Top targeted users

IsaiahL@contoso.onmicrosoft.com	25 attempts
MeganB@contoso.onmicrosoft.com	18 attempts
PradeepG@contoso.onmicrosoft.com	11 attempts

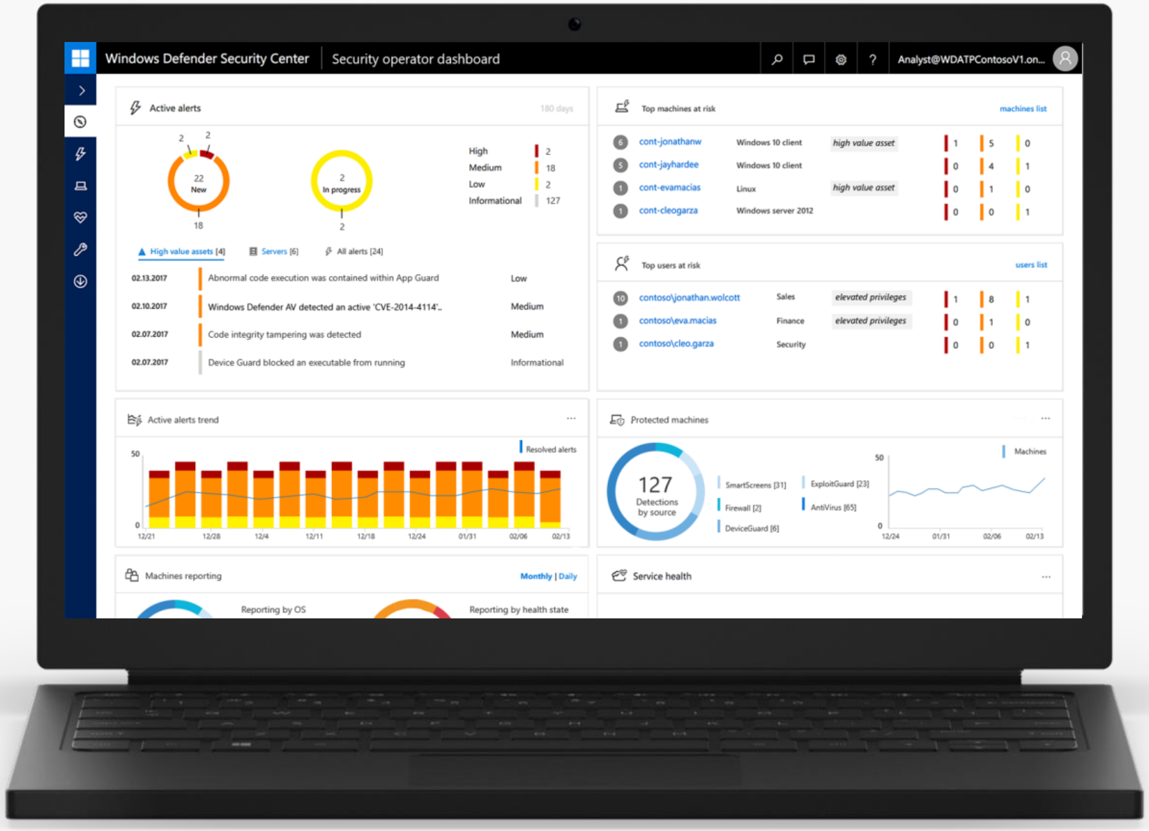
DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

Detect Abnormal Behaviors

Detect targeted advanced attacks and zero days.

Visually investigate forensic evidence across your devices to easily uncover scope of breach, assess the entire footprint of the incident, and trace it back to identify the root cause.

Search and explore 6 months of historical data across your devices


Windows Defender Security Center | Security operator dashboard

Analyst@WDATPContosoV1.on...

Active alerts — 180 days

High	🟥	2
Medium	🟧	18
Low	🟨	2
Informational	▨	127

High value assets [4] · Servers [6] · All alerts [24]

02.13.2017	Abnormal code execution was contained within App Guard	Low
02.10.2017	Windows Defender AV detected an active 'CVE-2014-4114'..	Medium
02.07.2017	Code integrity tampering was detected	Medium
02.07.2017	Device Guard blocked an executable from running	Informational

Top machines at risk — machines list

6	cont-jonathanw	Windows 10 client	high value asset	1	5	0
5	cont-jayhardee	Windows 10 client		0	4	1
1	cont-evamacias	Linux	high value asset	0	1	0
1	cont-cleogarza	Windows server 2012		0	0	1

Top users at risk — users list

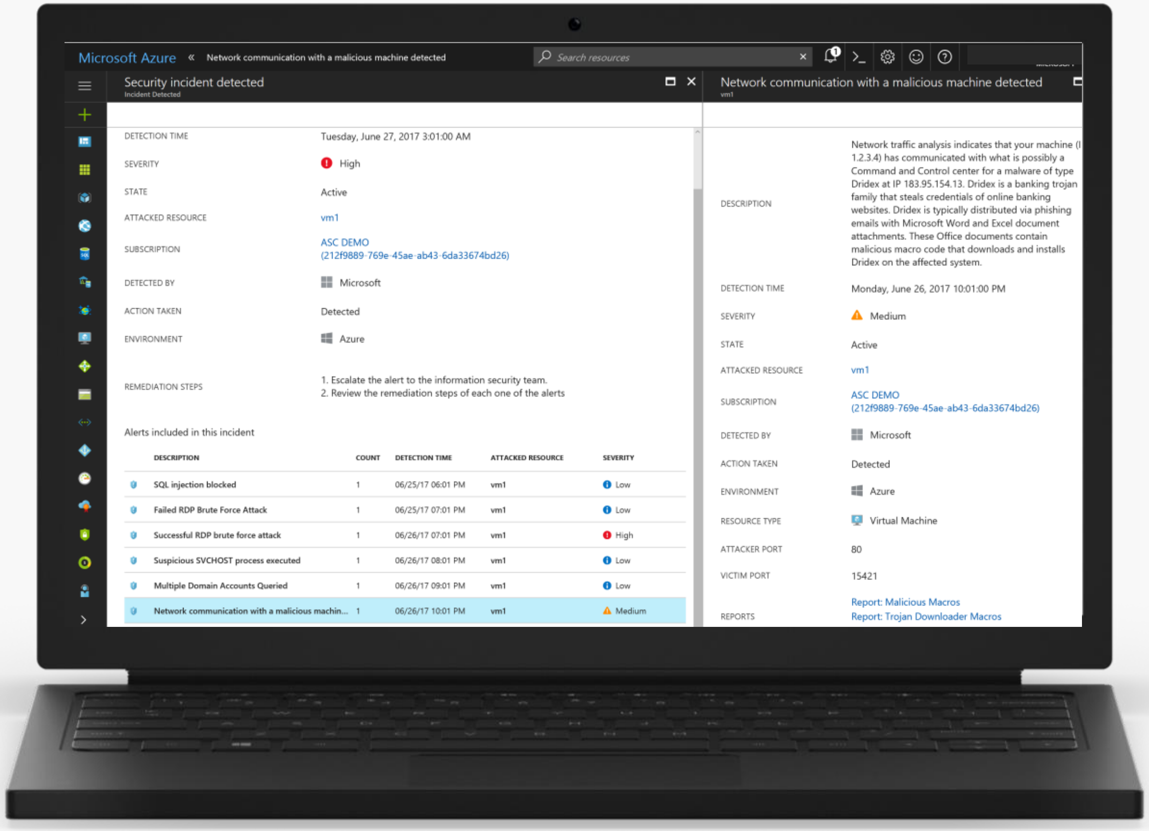
10	contoso\jonathan.wolcott	Sales	elevated privileges	1	8	1
1	contoso\eva.macias	Finance	elevated privileges	0	1	0
1	contoso\cleo.garza	Security		0	0	1

DETECT MALICIOUS ACTIVITY IN ORGANIZATIONS

Detect Advanced Threats to Hybrid Workloads

Built-in behavioral analytics and anomaly detection to identify real attacks across servers, networks, storage and apps

Arm yourself with information about an attacker's actions mapped across the kill chain, objectives, and tactics



Network communication with a malicious machine detected

Security incident detected

Incident Detected

DETECTION TIME	Tuesday, June 27, 2017 3:01:00 AM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	vm1
SUBSCRIPTION	ASC DEMO (212f9889-769e-45ae-ab43-6da33674bd26)
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
REMEDIATION STEPS	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts

Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
SQL injection blocked	1	06/25/17 06:01 PM	vm1	Low
Failed RDP Brute Force Attack	1	06/25/17 07:01 PM	vm1	Low
Successful RDP brute force attack	1	06/26/17 07:01 PM	vm1	High
Suspicious SVCHOST process executed	1	06/26/17 08:01 PM	vm1	Low
Multiple Domain Accounts Queried	1	06/26/17 09:01 PM	vm1	Low
Network communication with a malicious machin...	1	06/26/17 10:01 PM	vm1	Medium

Network communication with a malicious machine detected

vm1

DESCRIPTION	Network traffic analysis indicates that your machine (I 1.2.3.4) has communicated with what is possibly a Command and Control center for a malware of type Dridex at IP 183.95.154.13. Dridex is a banking trojan family that steals credentials of online banking websites. Dridex is typically distributed via phishing emails with Microsoft Word and Excel document attachments. These Office documents contain malicious macro code that downloads and installs Dridex on the affected system.
DETECTION TIME	Monday, June 26, 2017 10:01:00 PM
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	vm1
SUBSCRIPTION	ASC DEMO (212f9889-769e-45ae-ab43-6da33674bd26)
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
ATTACKER PORT	80
VICTIM PORT	15421
REPORTS	Report: Malicious Macros Report: Trojan Downloader Macros

RESPOND TO THREATS QUICKLY

RESPOND to compromised identities

IDENTITY

RESPOND to compromised apps and data

APPS & DATA

RESPOND to compromised devices

DEVICES

RESPOND early to compromised workloads across hybrid infrastructure

INFRASTRUCTURE

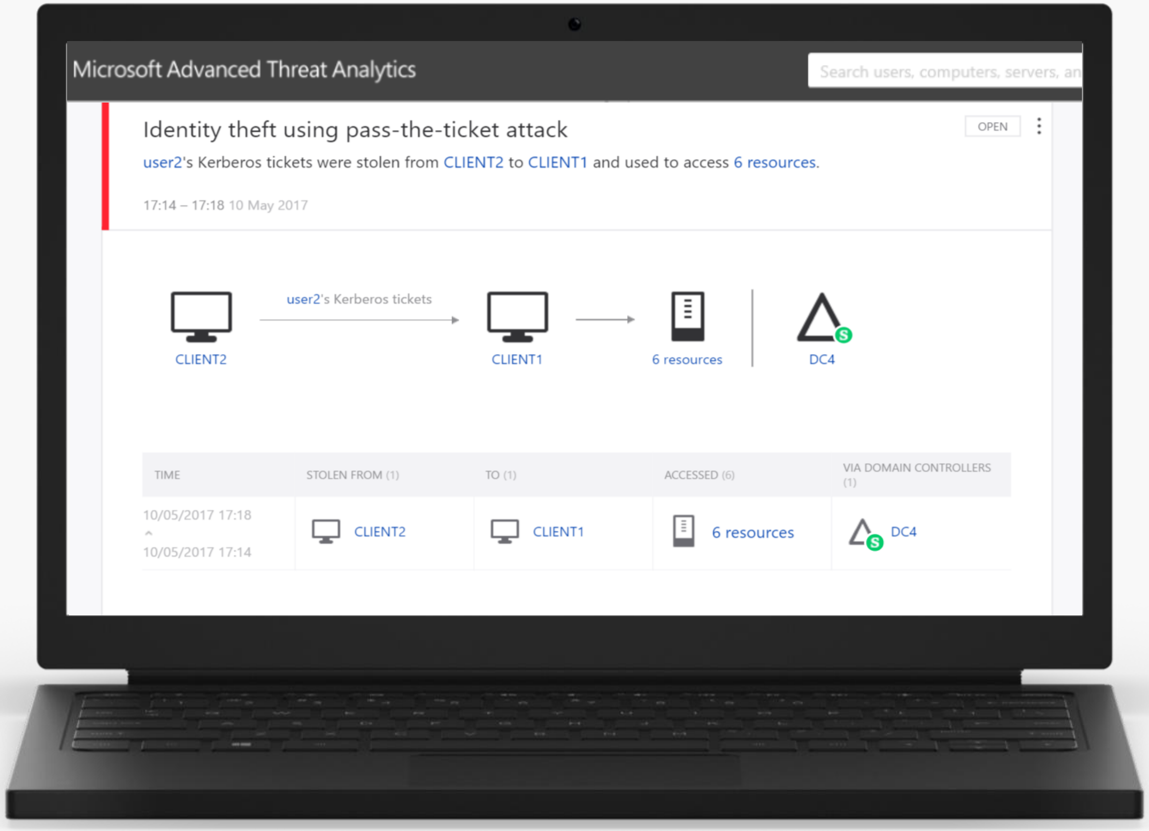
RESPOND TO THREATS QUICKLY

Respond to Compromised Identities

Get recommendations and remediation actions in case of a suspicious activity on-premises or in the cloud

Review next steps on a simple, actionable attack timeline

Identify threats before the attackers access critical data and resources


Microsoft Advanced Threat Analytics
Search users, computers, servers, an
OPEN

Identity theft using pass-the-ticket attack

user2's Kerberos tickets were stolen from CLIENT2 to CLIENT1 and used to access 6 resources.

17:14 – 17:18 10 May 2017

user2's Kerberos tickets
CLIENT2
CLIENT1
6 resources
DC4

TIME	STOLEN FROM (1)	TO (1)	ACCESSED (6)	VIA DOMAIN CONTROLLERS (1)
10/05/2017 17:18 ^ 10/05/2017 17:14	CLIENT2	CLIENT1	6 resources	DC4

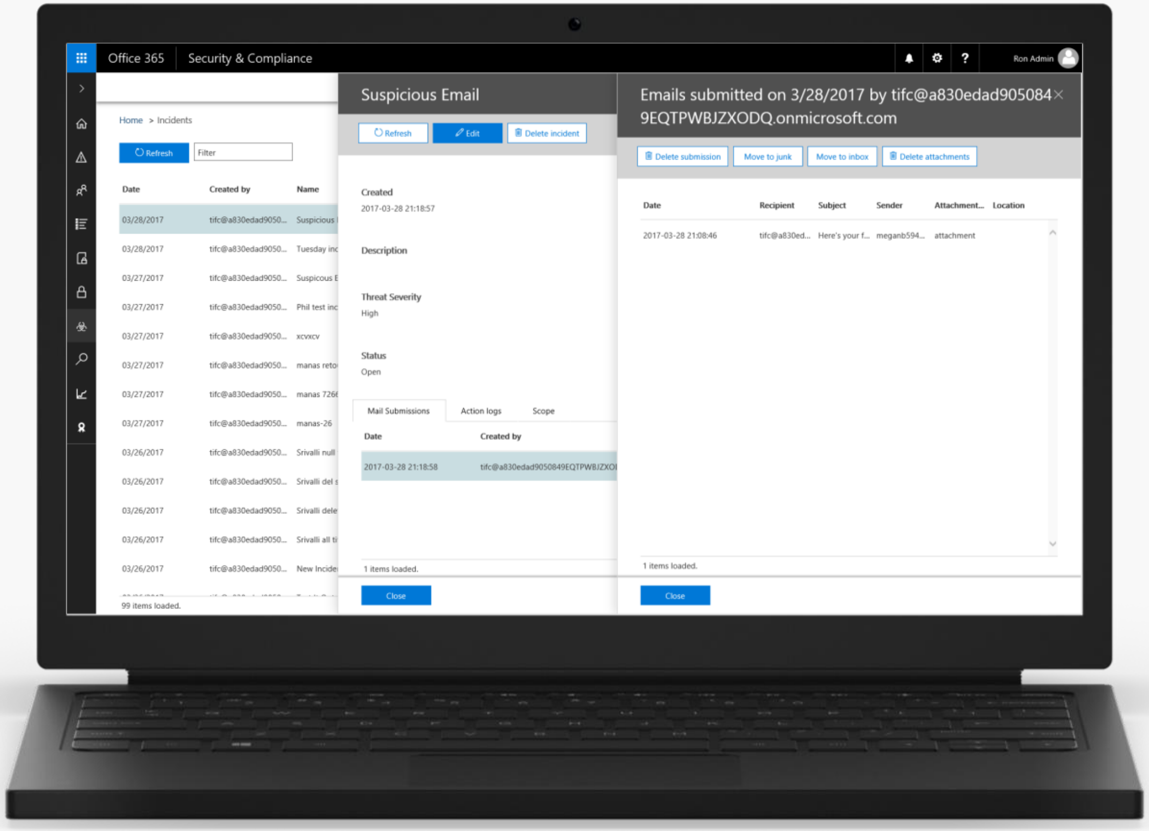
RESPOND TO THREATS QUICKLY

Respond to Malicious Email Files

Remove emails found to be malicious *after* they land in user inbox.

Intelligent filters which update based on evolving cyber threat landscape.

Ability to remediate for real-time malicious emails.



Date	Created by	Name
03/28/2017	tifc@a830edad9050...	Suspicious
03/28/2017	tifc@a830edad9050...	Tuesday inc
03/27/2017	tifc@a830edad9050...	Suspicous E
03/27/2017	tifc@a830edad9050...	Phil test inc
03/27/2017	tifc@a830edad9050...	xcvxcv
03/27/2017	tifc@a830edad9050...	manas reto
03/27/2017	tifc@a830edad9050...	manas 726
03/27/2017	tifc@a830edad9050...	manas-26
03/26/2017	tifc@a830edad9050...	Srivalli null
03/26/2017	tifc@a830edad9050...	Srivalli del s
03/26/2017	tifc@a830edad9050...	Srivalli dele
03/26/2017	tifc@a830edad9050...	Srivalli all ti
03/26/2017	tifc@a830edad9050...	New Incide

99 items loaded.

Created
2017-03-28 21:18:57

Description

Threat Severity
High

Status
Open

Date	Created by
2017-03-28 21:18:58	tifc@a830edad9050849EQTPWBJZXOI

1 items loaded.

Emails submitted on 3/28/2017 by tifc@a830edad905084 9EQTPWBJZXODQ.onmicrosoft.com

Date	Recipient	Subject	Sender	Attachment...	Location
2017-03-28 21:08:46	tifc@a830ed...	Here's your f...	meganb594...	attachment	

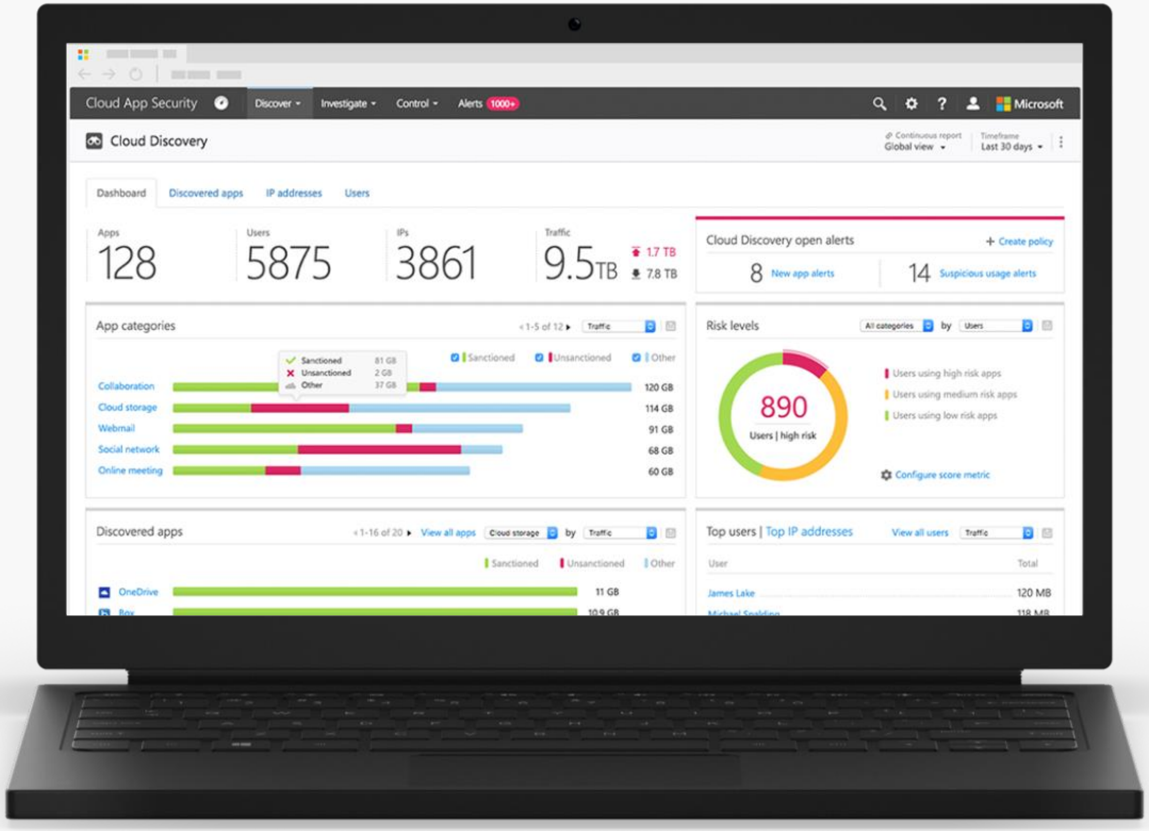
1 items loaded.

RESPOND TO THREATS QUICKLY

Respond to Compromised Data

Identify high-risk and anomalous usage in cross cloud apps - including office 365

Get recommendations and remediation actions for next steps



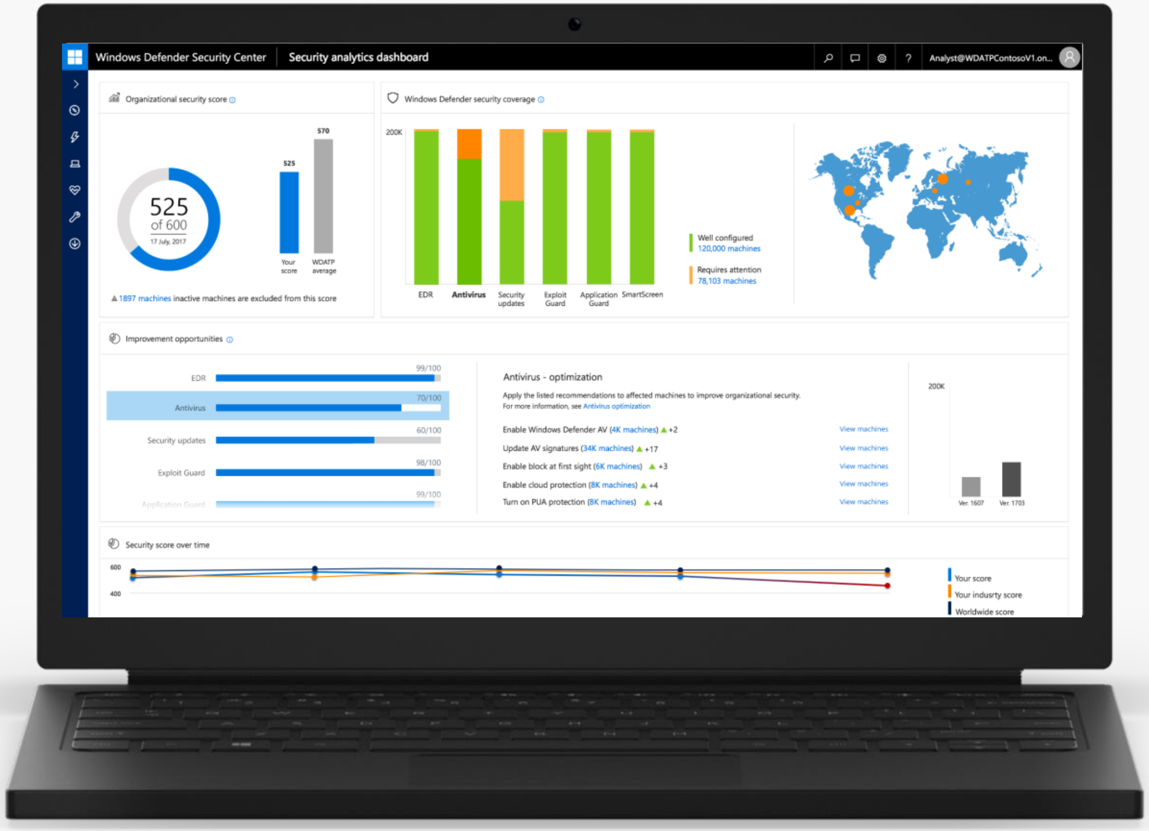
RESPOND TO THREATS QUICKLY

Respond to Compromised Devices

Remediate potential threats and prevent reoccurrence using built in technologies.

Receive mitigation guidance for remediation for threats and future risks

Assess organizational security score including trends over time



▲ 1897 machines inactive machines are excluded from this score

Antivirus - optimization

Apply the listed recommendations to affected machines to improve organizational security.
For more information, see Antivirus optimization

Enable Windows Defender AV (4K machines) ▲ +2 View machines
Update AV signatures (34K machines) ▲ +17 View machines
Enable block at first sight (6K machines) ▲ +3 View machines
Enable cloud protection (8K machines) ▲ +4 View machines
Turn on PUA protection (8K machines) ▲ +4 View machines

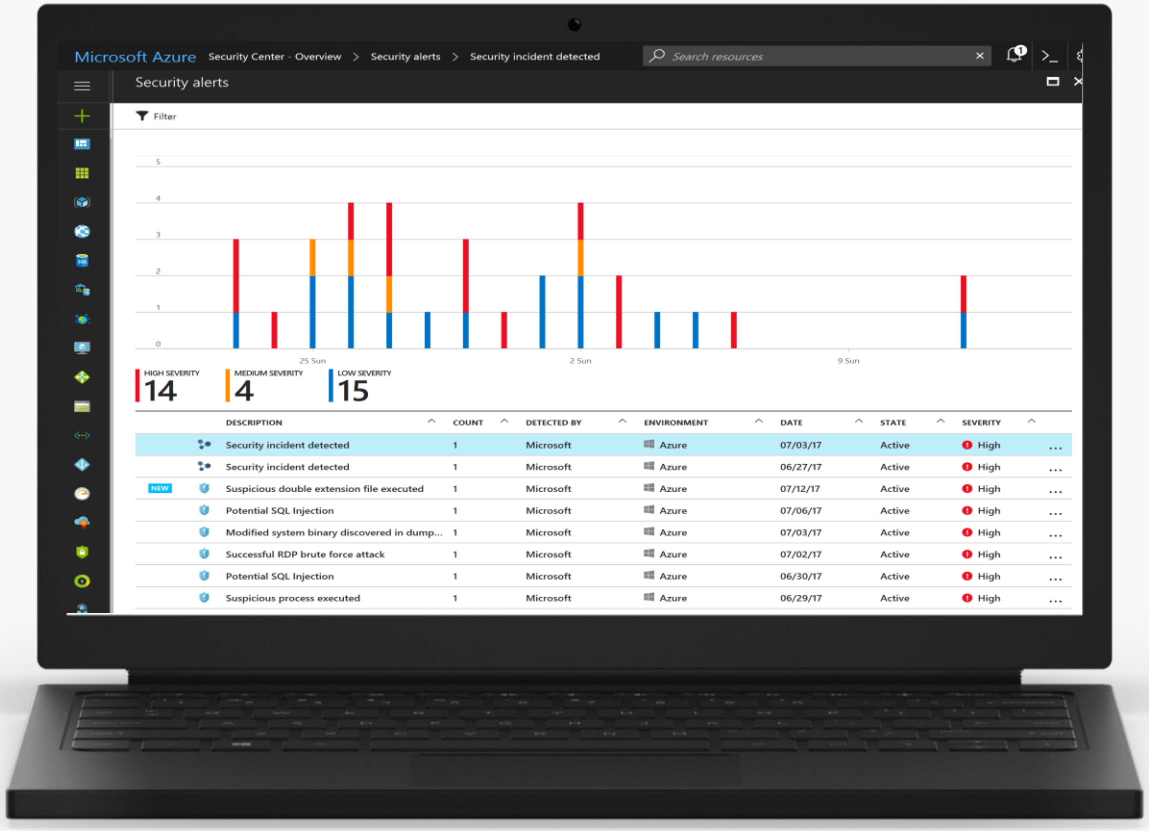
RESPOND TO THREATS QUICKLY

Respond to Compromised Workloads Across Hybrid Infrastructure

Prioritized security alerts that help you respond quickly with azure security center

Recommendations to mitigate threats and vulnerabilities

Threat intelligence reports for deeper insights into attack


Microsoft Azure
Security Center - Overview > Security alerts > Security incident detected
Search resources
Filter
5
4
3
2
1
0
25 Sun
2 Sun
9 Sun

Security alerts

HIGH SEVERITY 14
MEDIUM SEVERITY 4
LOW SEVERITY 15

	DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY	
	Security incident detected	1	Microsoft	Azure	07/03/17	Active	High	...
	Security incident detected	1	Microsoft	Azure	06/27/17	Active	High	...
NEW	Suspicious double extension file executed	1	Microsoft	Azure	07/12/17	Active	High	...
	Potential SQL Injection	1	Microsoft	Azure	07/06/17	Active	High	...
	Modified system binary discovered in dump...	1	Microsoft	Azure	07/03/17	Active	High	...
	Successful RDP brute force attack	1	Microsoft	Azure	07/02/17	Active	High	...
	Potential SQL Injection	1	Microsoft	Azure	06/30/17	Active	High	...
	Suspicious process executed	1	Microsoft	Azure	06/29/17	Active	High	...

MICROSOFT THREAT PROTECTION
INTELLIGENT & INTEGRATED

IDENTITY	APPS & DATA	DEVICES	INFRASTRUCTURE
MICROSOFT ADVANCED THREAT ANALYTICS	EXCHANGE ONLINE PROTECTION	WINDOWS DEFENDER ADVANCED THREAT PROTECTION	AZURE SECURITY CENTER
AZURE SECURITY CENTER	OFFICE 365 ADVANCED THREAT PROTECTION		
AZURE ACTIVE DIRECTORY	OFFICE 365 THREAT INTELLIGENCE		
MICROSOFT CLOUD APP SECURITY			

Microsoft