



# Security Transformation Overview

NYC CISO Forum

**James Cowling, CTO**

With the breakdown of the traditional perimeter, the ubiquity of machine learning and massive signal collection have enabled an identity-centric approach to security. The use of modern approaches to security, based on these signals and machine learning, enhances existing security approaches, transforming an organization's ability to respond to the changing attack landscape. This session will discuss how this security transformation is affecting businesses.

# Agenda

- The Security Transformation
- What is Changing
- Q&A

# Introductions



- Oxford Computer Group
  - Founded 1983
  - From 2002: focus on Identity
  - Increasing focus on Security and Governance
  - Numerous Microsoft awards for training and services in Identity, Enterprise Mobility and Security

**The  
Economist**

APRIL 8TH - 14TH 2017

The Pearl river delta: a special report

Hospitals of the future

Jacob Zuma must go

Parking, wrong on so many levels

# Why computers will never be safe



**OXFORD**  
COMPUTER GROUP

# Technical and Market Drivers

- Rise of cloud scale and machine learning
  - Increasing availability of global signal and telemetry
  - Availability of Machine Learning to act on this massive dataset
- Grey-scale, risk-based security assessment and management
- Automated attacks require automated responses
- Identity has become recognised as increasingly important – most successful attacks start with identity theft

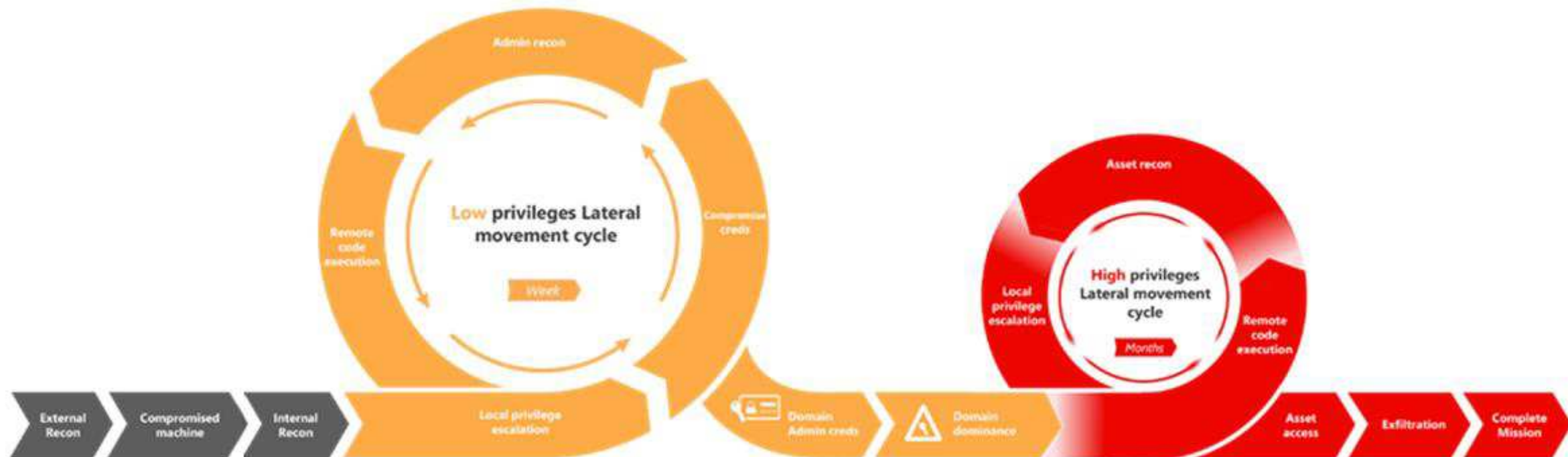
# What is the Security Transformation?



- Combination of technical and organizational developments
- Technical: Ability to perform real-time, identity-centric, risk-based security
  - Actionable intelligence across products
  - Supports the need to maintain flexibility in workload deployment
  - Massive signal collection from integrated global cloud systems
- Organizational: Ability for security to be an accelerator rather than a brake
  - Identity and risk integration across Hybrid and Cloud workloads
  - Help IT Operations to have workload flexibility
  - Accelerated speed of response to issues and requests

# Cyber Attack Cycles

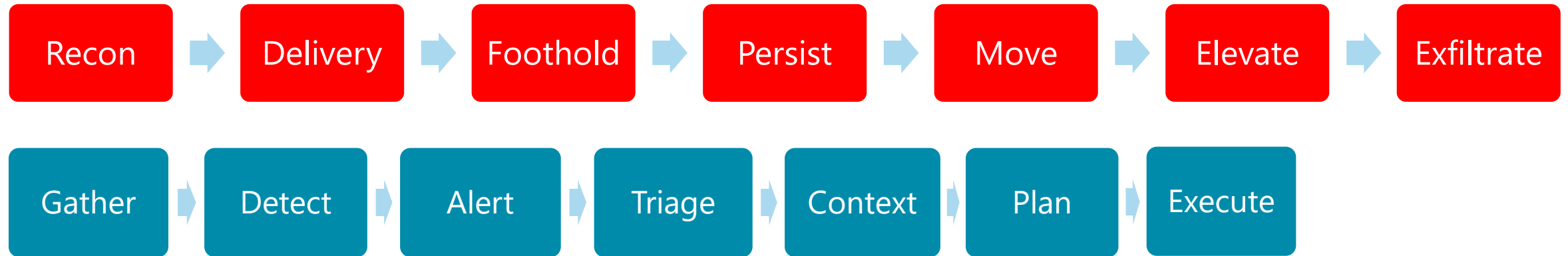
- Security investments (both prevention and detection) must be made along the whole process







# Increasing Response Speed



# Massive Data and Machine Learning



- The collection of massive data and the application of modern machine learning enables automation of response
- Automated responses allow disruption of attacks
- Enables the consolidation of events into actionable issues
- Provides visualisation for oversight and reporting

# Security Solutions



Compliance

Data  
Protection

Identity  
Governance  
and Protection

Endpoint and  
Network  
Protection

Attack  
Detection +  
Analysis

# Security Solutions



Compliance

Data  
Protection

Identity  
Governance  
and Protection

Endpoint and  
Network  
Protection

Attack  
Detection +  
Analysis

# Data Protection

- Many Cloud services are used in organizations
  - With and without approval from IT or security
  - With and without attention being paid to data protection and compliance issues
- Many security departments are unable to keep up with the speed at which business units want to adopt cloud services
  - Are the services compliant with applicable regulations?
  - Are the services secure?
- Data Leak Prevention rules and Cloud App Security offer a solution

Discover ▾ Investigate ▾ Control ▾

# Cloud App Security - Discovery



- Provides discovery of apps in use, as well as monitoring of activity
  - Machine-level agents, HTTP and optionally HTTPS traffic can be inspected
- Security and Compliance scoring for each app performed in advance by Microsoft

The screenshot displays the Microsoft Cloud App Security interface. The top navigation bar includes 'Cloud App Security', 'Discover', 'Investigate', 'Control', and 'Alerts' (with 16 alerts). The main content area is titled 'Cloud Discovery' and shows a list of discovered apps. On the left, there are summary cards for '552 all apps', '3 sanctioned apps', '0 unsanctioned apps', and '549 other apps'. The main table lists the following apps:

Name	Traffic	Upload	Transactions	Score	Users	IP addresses	Last seen
Microsoft OneDrive for Business Cloud storage	820 MB	179 MB	5K	10	620	537	Sep 20, 2016
Box Cloud storage	538 MB	106 MB	6K	9	393	278	Sep 20, 2016
Microsoft Skype for Business Online meetings	3.0 GB	1.3 GB	480	10	384	280	Sep 20, 2016
Microsoft Exchange Online Webmail	4.2 GB	1.1 GB	452	10	366	262	Sep 20, 2016
Office 365 Collaboration	5.5 GB	390 MB	2K	10	341	248	Sep 20, 2016
Microsoft Dynamics CRM	5.7 GB	13 MB	366	10	311	230	Sep 20, 2016

# App Security Scoring



Cloud App Security Discover Investigate Control Alerts 16 Microsoft

24 Content management	Data center	United States	Hosting company	Rackspace Hosting
22 Security	Founded	2001	Holding	Private
21 Content sharing	Domain	isnetworld.com	Domain registration	Aug 6, 1999
20 News and entertainment	Consumer popularity	8	Privacy policy	<a href="https://isnetworld.com/PrivacyPolicy.aspx">isnetworld.com/PrivacyPolicy.aspx</a>
17 Web analytics	Logon URL	<a href="https://isnetworld.com/LoginAssistance.aspx">isnetworld.com/LoginAssistance.aspx</a>	Vendor	ISN Software Corp
17 Customer support	<b>Security</b> <span>3</span>			
17 Transportation and travel	Multi-factor authentication	N/A	IP address restriction	N/A
16 Development tools	User audit trail	N/A	Admin audit trail	N/A
14 Collaboration	Data audit trail	N/A	Data classification	N/A
14 Human-resource management	Data ownership	N/A	Remember password	Yes
14 Advertising	User-roles support	N/A	Valid certificate name	Yes
12 Online meetings	Trusted certificate	Yes	Encryption protocol	TLS 1.2
11 Productivity	Heartbleed patched	Yes	HTTP security headers	Partial
10 Forums	Supports SAML	No	Enforce transport encryption	Yes
8 Webmail	Protected against DROWN	Yes		
6 CRM	<b>Compliance</b> <span>3</span>			
5 Communications	FINRA	N/A	HIPAA	N/A
5 Project management	ISAE 3402	N/A	ISO 27001	N/A
5 Business management	SOC 2	N/A	SOC 3	N/A
	SOX	N/A	SSAE 16	N/A
	Safe Harbor	Yes	PCI DSS version	N/A



# Data Leak Visibility



APP: Select apps... OWNER: Select owner (email) ACCESS LEVEL: Select access level... FILE TYPE: Select type... MATCHED POLICY: Select policy... Advanced

File name	Owner	Access Level	App	Collaborators	Last modified
Contoso Purchasing Permissions.docx	Tom Miyahira	Public (Internet) Anyone on the Internet can find and access	Microsoft OneDrive for Business	🔒	Oct 12, 2016
Sales Memo.docx	Tom Miyahira	Public Anyone with a link can access	Microsoft OneDrive for Business	🔒	Oct 12, 2016
Business Roundtable Presentation.pptx	Tom Miyahira	External Specific people outside of the organization can access	Microsoft OneDrive for Business	🔒	Oct 12, 2016
Customer Data.xlsx	Tom Miyahira	Internal Anyone in the organization can access	Microsoft OneDrive for Business	🔒	Oct 12, 2016
Investor Relations Meeting Presentation.pptx	Tom Miyahira	Private	Microsoft OneDrive for Business	🔒	Oct 12, 2016
Q2 Pricing Guidelines.docx	Tom Miyahira		Microsoft OneDrive for Business	🔒	Oct 12, 2016
Contoso Company Goals Q1 - Q4.docx	Tom Miyahira		Microsoft OneDrive for Business	🔒	Oct 12, 2016
East Region Q3 Sales.xlsx	Tom Miyahira		Microsoft OneDrive for Business	🔒	Oct 12, 2016
International Marketing Strategies.docx	Tom Miyahira		Microsoft OneDrive for Business	🔒	Oct 12, 2016

# Data Leak Analysis



## Integrated scenario with Azure Information Protection

Cloud App Security | Discover | Investigate | Control | Alerts 16 | Search | Settings | Help | Profile | Microsoft

Files | New policy from search

APP: Select apps... | OWNER: Select owner (email) | ACCESS LEVEL: Public | FILE TYPE: Select type... | MATCHED POLICY: Select policy... | Advanced

1 - 2 of 2 files

File name	Owner	App	Collaborators	Last modified
Pre-release Due Diligence.docx <small>Path: Sara Davis / Documents - <a href="#">View hierarchy</a></small>	Sara Davis	Microsoft OneDrive for Business	1 collaborator	Oct 6, 2016
<small>Type: document</small>	<small>Owner: <a href="#">sarad@emscr10.onmicrosoft.com (Sara Davis)</a></small>	<small>Created: Oct 6, 2016, 3:16:16 PM</small>	<small>Matched policies: <a href="#">Azure Information Protection Document Monitoring</a></small>	
<small>MIME type: application/vnd.openxmlformats-officedocument.wordprocessi...</small>	<small>Owner OU: —</small>	<small>Modified: Oct 6, 2016, 3:16:16 PM</small>	<small>Classification labels: <a href="#">Finance Only (external)</a>, <a href="#">Secret (external)</a></small>	
<small>File identifiers: <a href="#">View file identifiers</a></small>	<small>Collaborators: <a href="#">1 collaborator</a></small>	<small>File size: ~45 KB</small>	<small>Scan status: Completed</small>	
Account Log.xlsx	Sara Davis	Microsoft OneDrive for Business	1 collaborator	Oct 6, 2016

# Policy Controls



## Policies

TYPE:  SEVERITY:       NAME:  CATEGORY:  Advanced

1 - 6 of 6 Policies Create policy

Report	Count	Severity	Category	Action	Modified
<b>New risky app</b> Alert when new apps are discovered with a risk score lower than 6, that are used by more than 50 users with a total daily use of more than 50 MB.	0 open alerts	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Cloud Discovery		Oct 6, 2016
<b>Azure Information Protection Document Monitoring</b> Monitors for any Azure Information Protection labelled file that is shared publicly.	2 matches	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	DLP		Oct 7, 2016
<b>Logon from a risky IP address</b> Alert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky IP address category contains addresses that have IP address tags of Anonymous proxy, TOR or Botnet. You can add more IP addresses to this category in the IP address ranges settings page.	5 open alerts	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Threat detection		Oct 11, 2016
<b>File containing PCI detected in the cloud (built-in DLP engine)</b> Alert when a file containing payment card information (PCI) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app.	3 matches	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	DLP		Oct 6, 2016
<b>General anomaly detection</b> The pre-configured anomaly detection policy is applied to all activity in your environment to provide protection from anomalous login, access and account activities. Additional anomaly detection policies can be created that are focused on a specific scope of activity (e.g. specific users).	0 open alerts	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Threat detection		Sep 1, 2016

# Policy Violations



Matching now History

AUTHORIZATION APP OWNER ACCESS LEVEL FILE TYPE OWNER OU Advanced

? ✓ Select apps... Select owner (email) Select access level... Select type... Select organizational units...

1 - 3 of 3 files

File name	Owner	App	Collaborators	Content matches co...	Detection date
Northwind Customer Data.xlsx	Provisioning User	Microsoft SharePoint Online	28 collaborators	35 matches	Oct 6, 2016
Path: Contoso Team Site / Shared Documents / DemoDocs - <a href="#">View hierarchy</a> URL: <a href="https://emscr10.sharepoint.com/Shared_Documents/DemoDocs/Northwind_Customer_Data.xlsx?id=w4c336218c4a048d0afbc0484a66737e9">https://emscr10.sharepoint.com/Shared_Documents/DemoDocs/Northwind_Customer_Data.xlsx?id=w4c336218c4a048d0afbc0484a66737e9</a>					
Type: spreadsheet	Owner: provisioninguser0@emscr10.onmicrosoft.com (Provisioning User)	Created: Oct 27, 2015, 4:17:14 PM	Matched policies: File containing PCI detected in the cloud (built-in DLP.en...		
MIME type: application/vnd.openxmlformats-officedocument.spreadsheet...	Owner OU: —	Modified: Oct 27, 2015, 4:17:16 PM	File tags: —		
File identifiers: <a href="#">View file identifiers</a>	Collaborators: 28 collaborators	File size: ~38 KB	Scan status: Completed		
Project Falcon Customer Data.xlsx	Provisioning User	Microsoft SharePoint Online	28 collaborators	9 matches	Oct 6, 2016
Customer US Store Purchases.xlsx	Zrinka Makovac	Microsoft SharePoint Online	28 collaborators	35 matches	Oct 6, 2016

# Security Solutions



## Compliance

Data  
Protection

Identity  
Governance  
and Protection

Endpoint and  
Network  
Protection

Attack  
Detection +  
Analysis

Cloud App  
Security

Saviynt

# Security Solutions



## Compliance

Data  
Protection

Identity  
Governance  
and Protection

Endpoint and  
Network  
Protection

Attack  
Detection +  
Analysis

Cloud App  
Security

Saviynt

# Endpoint Protection

- Identity theft from the endpoint is the entry point for many successful attacks
- Ability to execute code on an endpoint makes identity theft much easier
- Windows 10 brings significant advances to prevent both remote code execution and identity theft
  - Interplay with Azure services delivers good visualization of correlated events for analysis and action
  - CredentialGuard and DeviceGuard are new technologies at the Windows endpoint to help prevent these attacks

# Malware Protection and Analysis



- Dashboard
- Alerts Queue
- Machines View
- Service Health
- Preferences setup
- Endpoint Management

### ATP alerts 100 days

5 New

4 In progress

■ High 1  
■ Medium  
■ Low

#### Latest ATP alerts

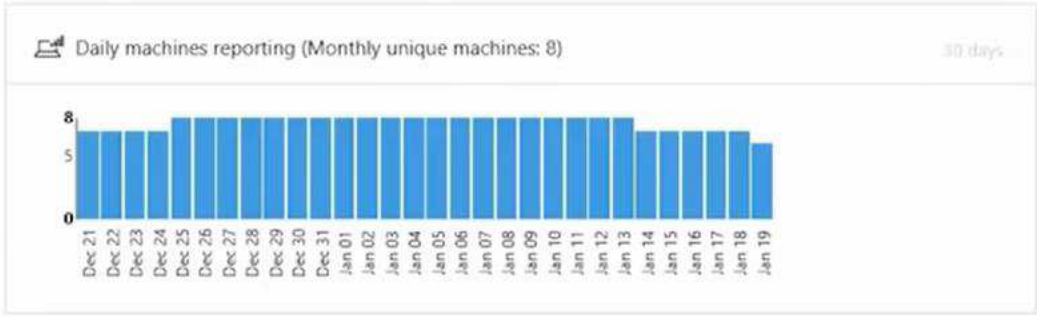
Date	Description	Severity
11.19.2016	A malicious file was detected based on FireEye iSIGHT TI	Medium
09.22.2016	A suspicious process was observed accessing the LSASS (Local Security A...	Medium
09.22.2016	A suspicious Powershell commandline was found on the machine	Medium
09.19.2016	A potential reverse shell has been detected	Medium

### Machines at risk machines view

Machine Name	High	Medium	Low
cont-lizbean	1	4	1
cont-brianeagle	0	1	0
cont-yolandawil	0	1	0
contserver2012	0	1	0

### Machines with active malware detections 180 days

No active malware detections found



### Machines health 30 days

0  
Machines

Misconfigured 0

Inactive 0

[More info on TechNet](#)

### Service health

Service is operating normally



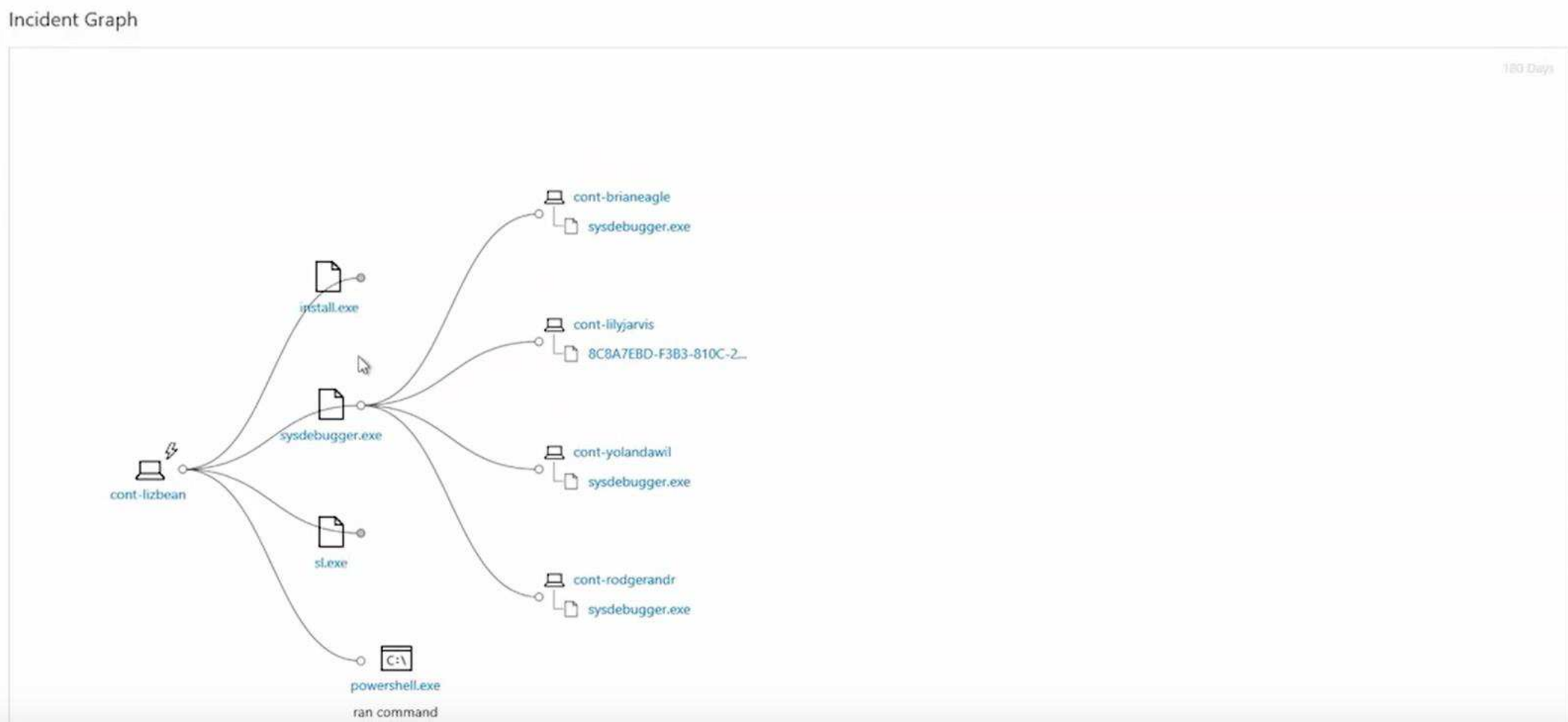
# Incident Analysis

- Dashboard
- Alerts Queue
- New
- In Progress
- Resolved
- Assigned to me

- Machines View
- Service Health
- Preferences setup
- Endpoint Management

Alert Process Tree

Alert process tree is not available for this alert



# Malware Deep Analysis



- Dashboard
- Alerts Queue
- New
- In Progress
- Resolved
- Assigned to me
- Machines View
- Service Health
- Preferences setup
- Endpoint Management

Actions ▾

Sha1: 66c2bf9b5271f63e8c05e9f0c96df5a0d01e3fb0

MDS: 33efa186e2e5bc597655251d2af1549d

Sha256: 880bf6b103a12c46646b224eec246958bd3ea2c95a49888cd8f9fe5015258a20

Size: 4.5 KB

Signer: unsigned

Issuer: unsigned

No matches for this file in Virus Total

---

**Windows Defender AV:**  
No detections found

5

First seen: 4 months ago  
Last seen: a month ago

## Deep analysis

Deep analysis request ✓ Results available [Resubmit](#)

Deep analysis summary (latest available result: a month ago)

### Behaviors

#### Communication

- ✓ A process which does not typically perform HTTP traffic, performs an HTTP operation ⓘ
- ✓ A system file communicates with an external IP address
- ✓ Communicates over the network using an encrypted channel
- ✓ Communicates with an external IP address
- ✓ Performs an HTTP GET operation
- ✓ Performs an HTTP request to a PHP page

#### Environment Awareness

- ✓ Checks for domain information
- ✓ Checks for hardware information ⓘ
- ✓ Checks for host information ⓘ
- ✓ Checks Internet Cache properties
- ✓ Checks whether Windows Error Reporting is enabled ⓘ
- ✓ Queries the BIOS version
- ✓ Reads or changes the default browser

#### Installation and persistency

- ✓ Adds a file to be loaded by Windows the next time it starts (ASERP)

# Global Signals, used Globally



- When a threat is detected by one Azure-connected service, its correlated information is made available to all other Azure services
- This is achieved by building a graph of correlated events – the Azure Security Graph
- Tenants and services who are not currently under attack therefore gain advance notice and the ability to defend pre-emptively against emerging threats

# Correlation as Data Graph

- Activity is correlated with other related activities into a data graph
- For example: malware activity

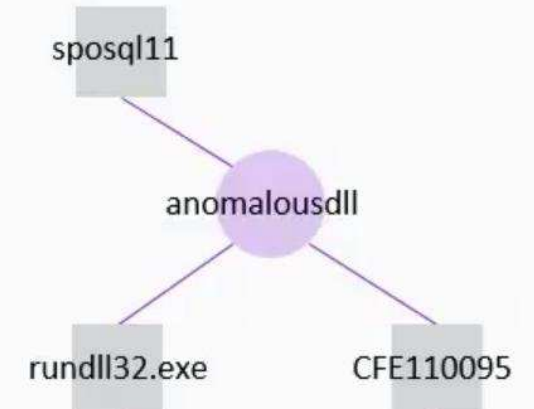
**Anomalous DLL:** rundll32.exe launched as sposql11 on CFE110095

*alert type*

*process*

*user*

*host*



# Azure Security Graph

- A central service in Azure (aka the Intelligent Security Graph)
- Digital representation of security events from across Azure services and infrastructure
- Machine learning algorithms analyse the collected data to detect and prioritise suspicious events
- Other services can contribute and read from the graph to enrich the data and respond to detected events
- Example: Malware from attached document detected by Windows Defender is blocked by Office365
- Example: Detection of emerging botnet activity

# Malware Machine Activity



Windows Defender Security Center | Machine | Analyst@WDATPContoso.onmicrosoft.com

Alert Status: New (1), In progress (0), Resolved (0)

Assigned to: Analyst@WDATPContoso.onmicrosoft.com

Related activity on machine: First activity: 09.19.2016 | 09:38:05, Last activity: 09.19.2016 | 14:35:48

Comments and history: Comment: Add your comment, + Add comment

01.03.2017 | 09:35:20: Alert assigned to Analyst@WDATPContoso.onmicrosoft.com

09.19.2016 | 09:38:05: Alert generated.

Suppression rules: Go to alert page

Time	Process	Action	Target	Process	Process	Process
14:35:48	WINWORD.EXE	ran a file from Users Folder		OUTLOOK.EXE	WINWORD.EXE	process
14:35:48	WINWORD.EXE	created process	install.exe	OUTLOOK.EXE	WINWORD.EXE	installexe
14:35:48	WINWORD.EXE	created	install.exe	OUTLOOK.EXE	WINWORD.EXE	installexe
14:34:36	WINWORD.EXE	communicated with	10.0.0.9	OUTLOOK.EXE	WINWORD.EXE	10.0.0.9
14:34:35	WINWORD.EXE	ran an Office application		OUTLOOK.EXE	WINWORD.EXE	process
14:34:33	OUTLOOK.EXE	ran an Office application		explorer.exe	OUTLOOK.EXE	process
14:34:33	OUTLOOK.EXE	saved an attachment to disk				More details on this email in O365
14:33:21	SppExtComObj.Exe	communicated with	2 IPs	svchost.exe	SppExtComObj.Exe	2 IPs

userinit.exe

explorer.exe  
ID: ea964d893c735ea8879ba68ec94620c865a644a4  
Path: C:\Windows\explorer.exe  
Process: Explorer.EXE

OUTLOOK.EXE  
ID: 0d532fc72de4ebc2c00186c5341185d80c3389cb  
Path: C:\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE  
Action: "OUTLOOK.EXE" /f "C:\Users\liz.bean\Desktop\New Customer Opportunity.msg"

files

Displaying unique files (Filename & Sha1)

- New Customer Opportunity (2).doc
- New Customer Opportunity (3).doc

Sender: Brian.Eagle@Contoso.org  
Subject: New Customer Opportunity  
Recipients: Liz.Bean@contoso.org  
Received: 09.19.2016 | 13:19:33

# O365 Threat Protection



- Home
- Alerts
- Permissions
- Threat management
- Data governance
- Search & investigation
- Dashboard
- Threat explorer
- Content search
- Audit log search
- eDiscovery
- Quarantine
- Productivity app discovery
- Reports
- Service assurance

Home > Threat explorer

## Threat explorer

Search by file name, user or user group, sender, header pattern...

Export

Filter

Threat family



Top threats

Email list

Date	Recipients	Machines	Subject	Sender	Sender IP	Status
10/24/2016 1:39PM	Yolanda.Wilder@WDATPConto...	cont-yolandawil	New Customer Opportunity	Contoso.org	75.146.176.238	Blocked
10/24/2016 1:25PM	Liz.Bean@WDATPContoso.on...	cont-lizbean	New Customer Opportunity	Contoso.org	75.146.176.238	Delivered
10/24/2016 1:30PM	Rodger.Andre@WDATPContos...	cont-rodgerandr	New Customer Opportunity	Contoso.org	75.146.176.238	Blocked

# Machine Activity Details

- Dashboard
- Alerts Queue
- Machines View
- Service Health
- Preferences setup
- Endpoint Management

Alerts related to this machine

No active alerts found.

Machine timeline


Information level: All Account: All Export to CSV



Date	Event	Details	User
<b>09.19.2016</b>			
23:50:18	svchost.exe ran backgroundtaskhost.exe	services.exe > svchost.exe > process	SYSTEM
21:00:27	svchost.exe communicated with 131.253.61.84	services.exe > svchost.exe > 131.253.61.84	SYSTEM
21:00:27	svchost.exe changed 2 registry values	services.exe > svchost.exe > 2 registry values	SYSTEM
21:00:27	svchost.exe changed 2 registry values	services.exe > svchost.exe > 2 registry values	SYSTEM
20:30:03	cleanmgr.exe ran a file from Users Folder	svchost.exe > cleanmgr.exe > process	liz.bean
20:29:58	cleanmgr.exe created 64 PE files under Users folder	svchost.exe > cleanmgr.exe > 64 files	liz.bean
20:29:58	cleanmgr.exe created 128 files	svchost.exe > cleanmgr.exe > 128 files	liz.bean
20:29:45	MsMpEng.exe created a PE file under ProgramData folder	services.exe > MsMpEng.exe > file	SYSTEM
20:29:45	MsMpEng.exe created mpengine.dll	services.exe > MsMpEng.exe > mpengine.dll	SYSTEM
20:29:42	services.exe changed 1 registry value	winit.exe > services.exe	SYSTEM
20:29:41	CompatTelRunner.exe communicated with 191.239.50.77	CompatTelRunner.exe > CompatTelRunner.exe > 191.239.50.77	SYSTEM



# Real-Time Threat Analysis



**Liz Bean**  
Sales Account Manager  
contoso-us.org  
Created on Aug 26, 2015  
(555) 123-0661 | liz.bean@contoso.org

[View in Windows Defender ATP](#)

2 suspicious activities 1 High 1 Low

[About](#) [Account Info](#) [Suspicious activities](#) [Directory Changes](#)

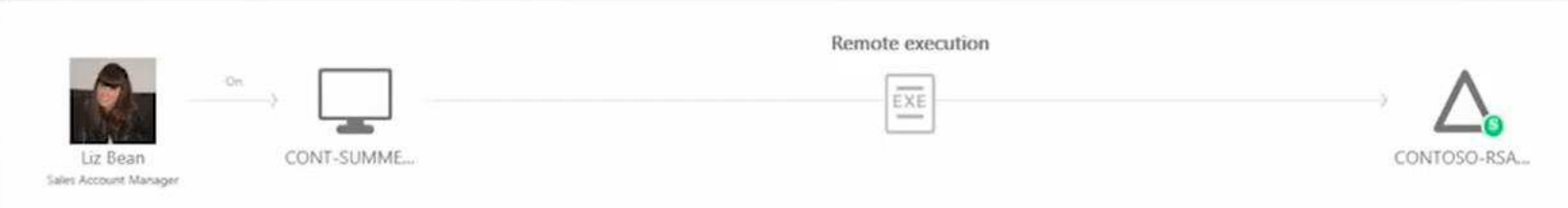
No notifications

5:13 AM  
Monday, September 19, 2016

**Remote execution attempt detected**  
The following remote execution attempts were performed on CONTOSO-RSA-ORG from CONT-SUMMERFROS:

- Successful remote creation of PSEXESVC by Liz Bean.

[Note](#) [Share](#) [Export to Excel](#) [Details](#) [Input](#) [Open](#)

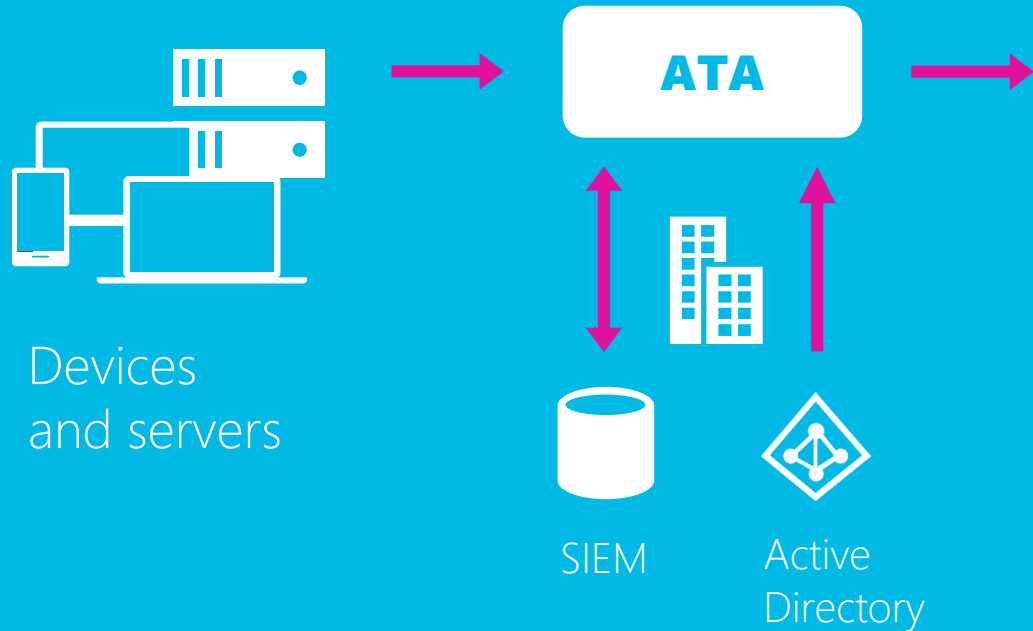


```
graph LR; LizBean[Liz Bean] -- On --> CONTSUMME[CONT-SUMME...]; CONTSUMME -- Remote execution --> EXE[EXE]; EXE --> CONTOSORSA[CONTOSO-RSA...]
```

- Recommendations
- Disconnect CONT-SUMMERFROS from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
  - Investigate the root cause on CONT-SUMMERFROS
  - Review CONTOSO-RSA-ORG for abnormal services or scheduled tasks
  - Review and delete the list of suspicious files and folders on CONTOSO-RSA-ORG

# Microsoft Advanced Threat Analytics

Security Information and Event Management (SIEM)



Behavioral analytics



Profile normal entity behavior (normal versus abnormal)

Forensics for known attacks and issues



Search for known security attacks and issues

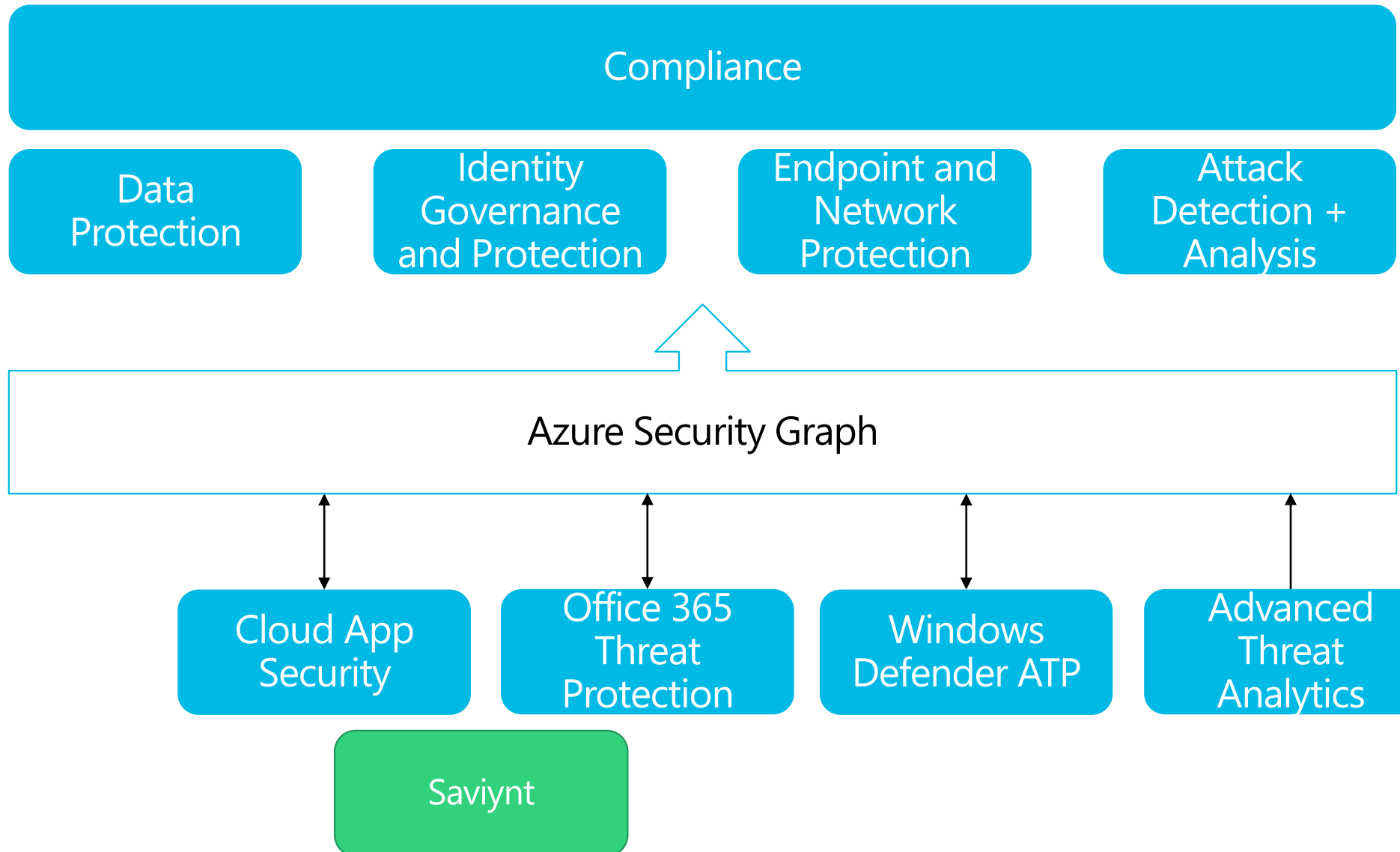
Advanced Threat Analytics



Detect suspicious user activities, known attacks, and issues



# Security Solutions



# Azure AD Identity protection



## Anomaly detection

- Heuristic and machine learning



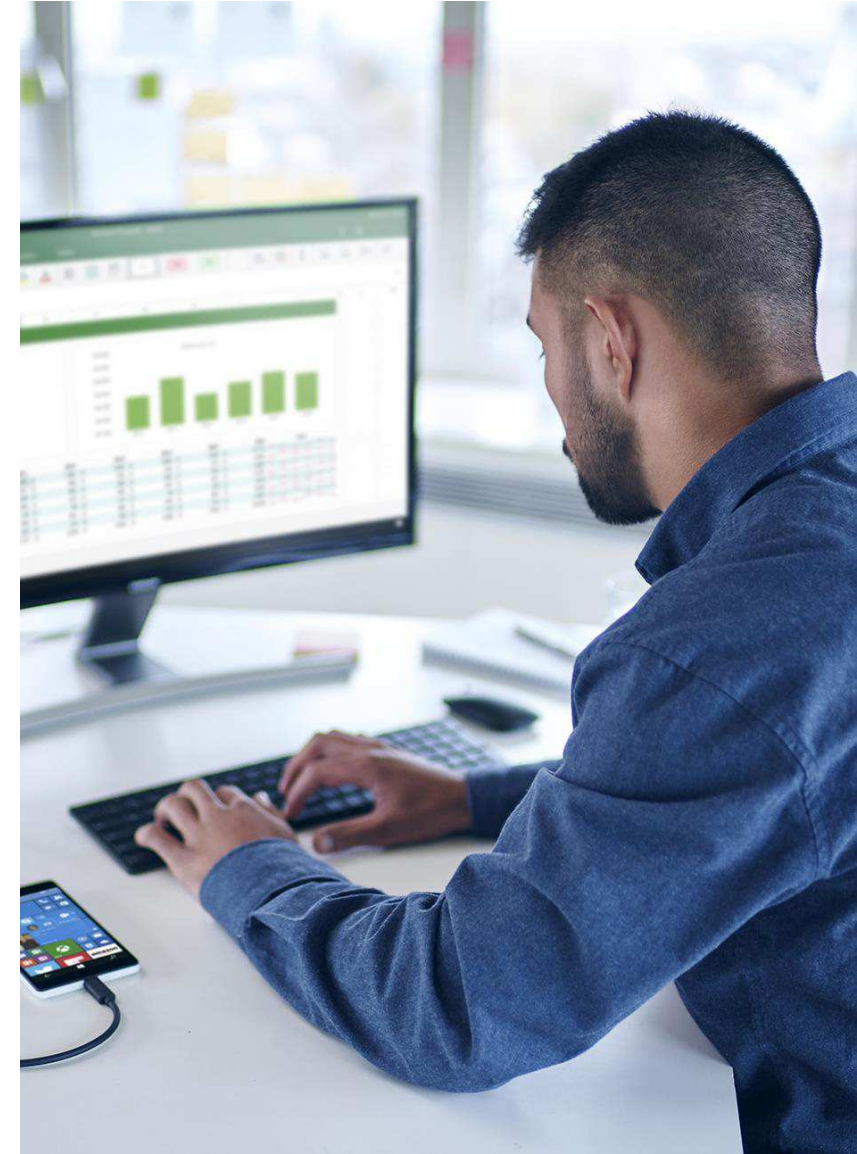
## Risk event detection

- Per user risk level

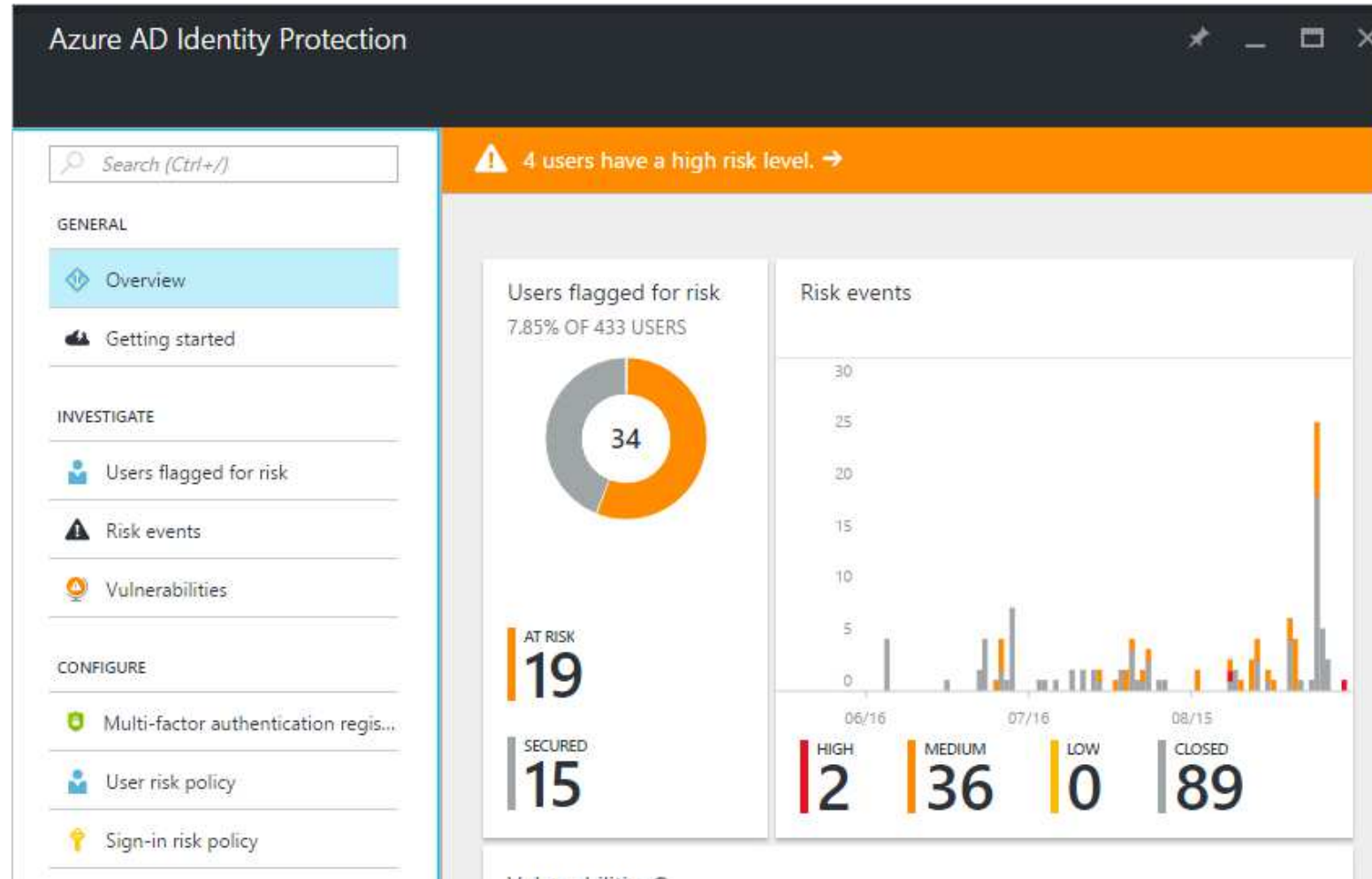


## Risk based policies

- Require MFA for risky accounts



# Azure AD Identity Protection - Dashboard



# Azure AD Identity Protection – Risk Events



Azure AD Identity Protection - Risk events

AZURE AD IDENTITY PROTECTION

Last 90 days Download

Search (Ctrl+/)

GENERAL

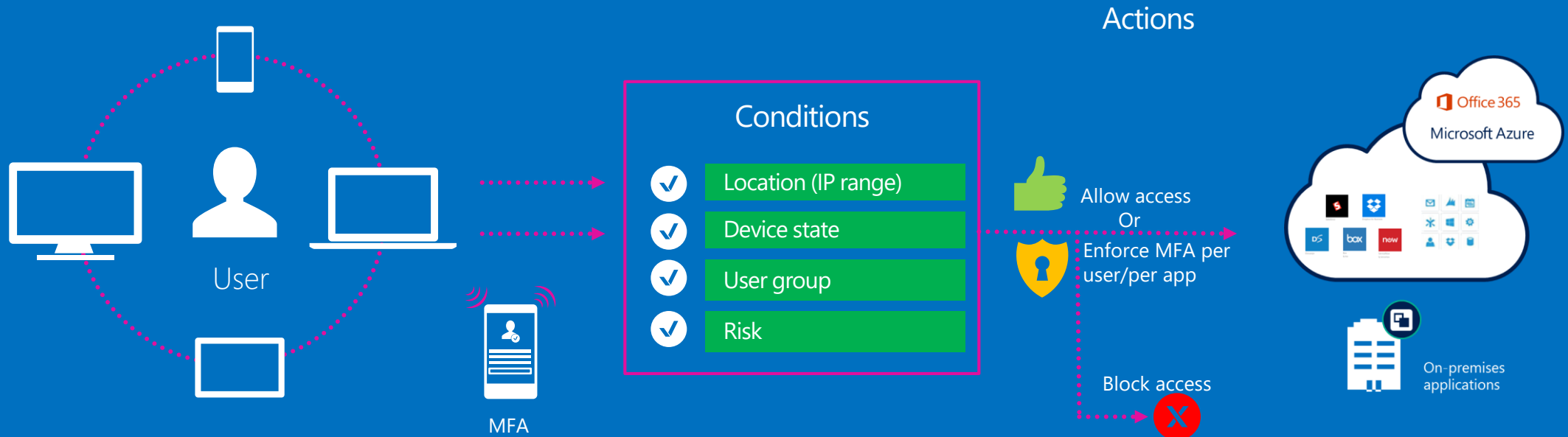
- Overview
- Getting started

INVESTIGATE

- Users flagged for risk
- Risk events**
- Vulnerabilities

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials ⓘ	0 of 2	9/12/2016, 11:36 PM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	37 of 50	9/9/2016, 5:58 PM
Medium	Offline	Impossible travels to atypical locations ⓘ	5 of 12	9/7/2016, 6:49 PM
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ	47 of 63	9/9/2016, 5:58 PM

# Identity-Driven Security



IDENTITY PROTECTION

NOTIFICATIONS, ANALYSIS, REMEDIATION, RISK-BASED POLICIES



CLOUD APP DISCOVERY



PRIVILEGED IDENTITY MANAGEMENT



# Operations Management Suite



## Collect Security Data

- From almost every source



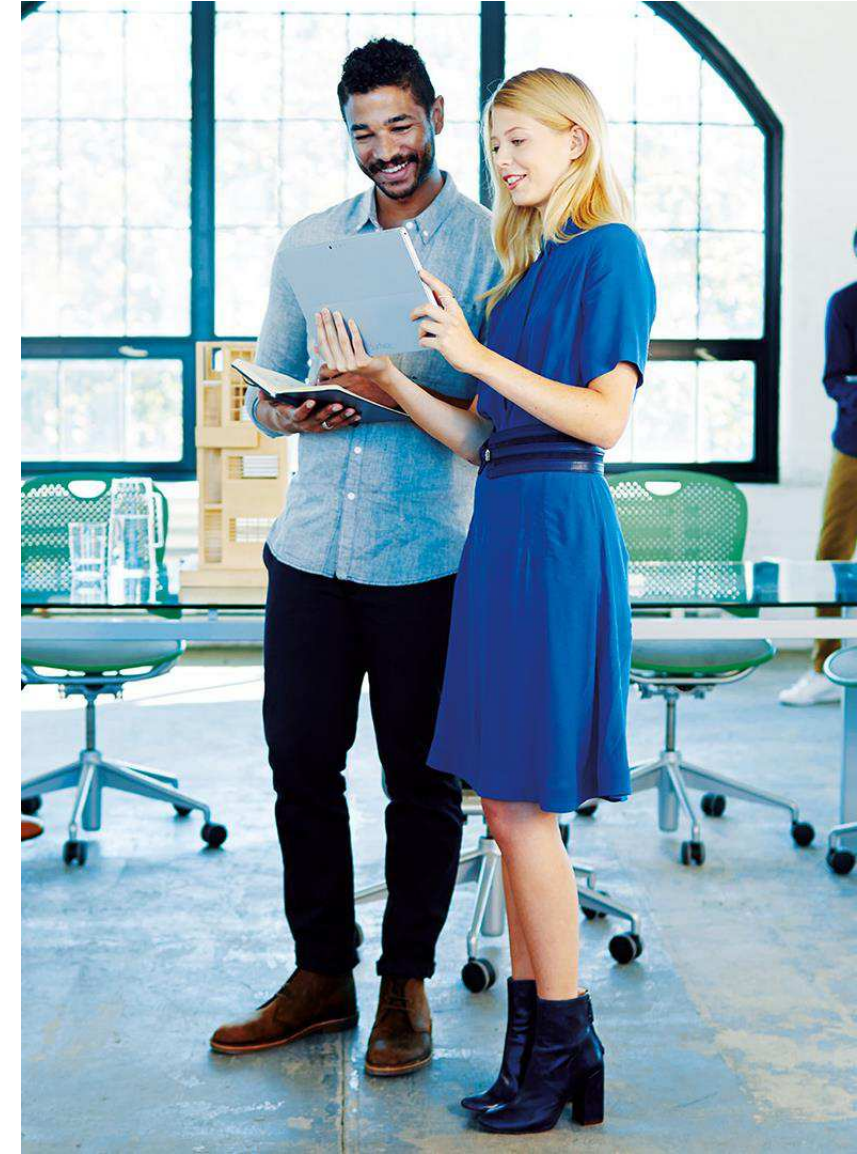
## Correlate Data

- Gain insight into issues



## Create Alerts

- Trigger notifications and automation



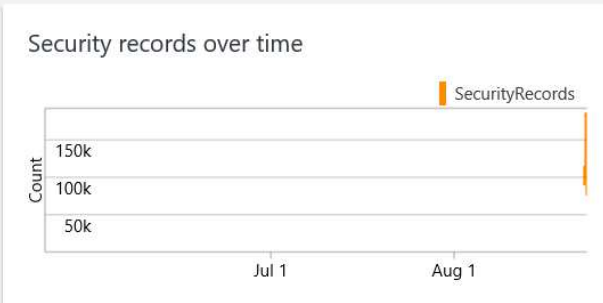


# Gain Insight



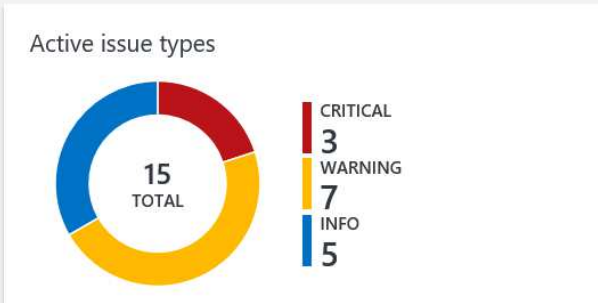
Overview ▶ Security And Audit

SECURITY DOMAINS



<b>Antimalware Assessment</b> Computers with Antimalware Assessment <b>63</b>	<b>Update Assessment</b> Computers missing updates <b>19</b>
<b>Network Security</b> Distinct IP addresses <b>2K</b>	<b>Identity and Access</b> Accounts attempted to log on <b>7.2K</b>
<b>Computers</b> Computers with security events <b>41</b>	<b>Threat Intelligence</b> Malicious traffic events <b>27</b>
<b>Baseline Assessment</b> Critical failed rules in the last day <b>106</b>	<b>Azure Security Center</b>

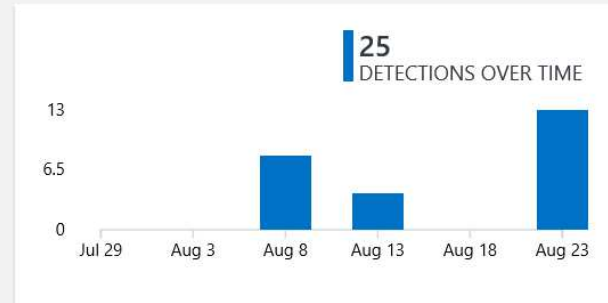
NOTABLE ISSUES



NAME	COUNT	SEVERITY
Computers missing security updates	12	CRITICAL
High priority AD assessment security r...	2	CRITICAL
Distinct malicious IP addresses accessed	1	CRITICAL
Computers with insufficient protection	30	WARNING
Computers missing critical updates	9	WARNING
Low priority AD assessment security re...	4	WARNING
Low priority SQL assessment security r...	4	WARNING
Logons with a clear text password	2	WARNING
Members added To security-enabled g...	1	WARNING
MyTestDetection	1	WARNING

< 1 of 2 >

DETECTIONS (PREVIEW)



NAME	COUNT	SEVERITY
Suspicious double extension file execu...	5	CRITICAL
Failed RDP Brute Force Attack	13	WARNING
Suspicious SVCHOST process executed	7	WARNING

< 1 of 1 >

# Create Alerts

Microsoft Operations Management Suite

Log Search > Add Alert Rule

### General

Alert information

Name  
  
Enter an alert name

Description

Severity

Search query

Time window

This search returned  
**0 results** for the time window selected

### Schedule

Threshold  
Generate an alert when the number of results is  
   
Threshold should be a positive integer between 0 and 10000

Alert frequency  
Check for this alert every

Suppress alerts  
When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

### Actions

Email notification

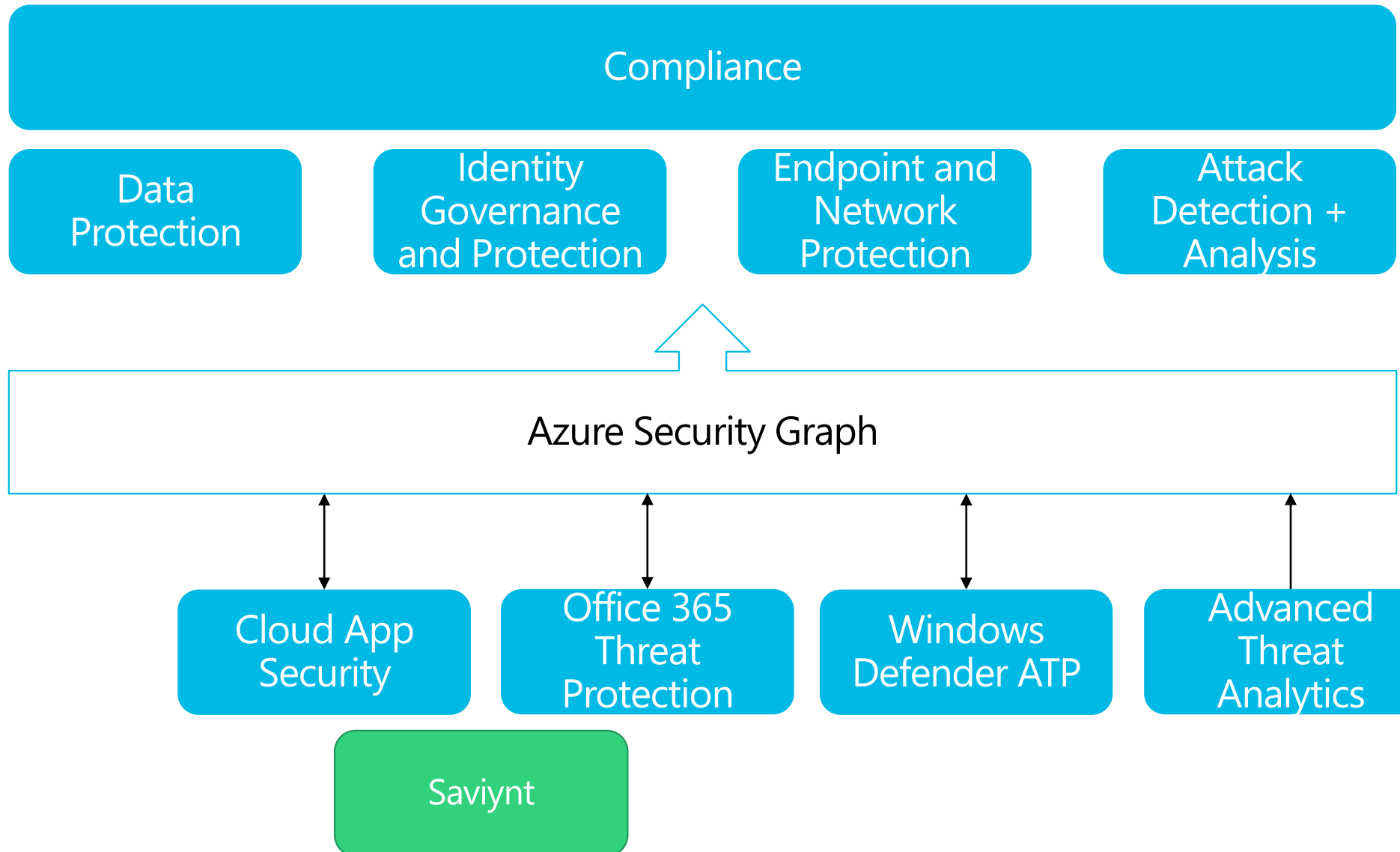
Subject

Recipients (semi-colon separated)

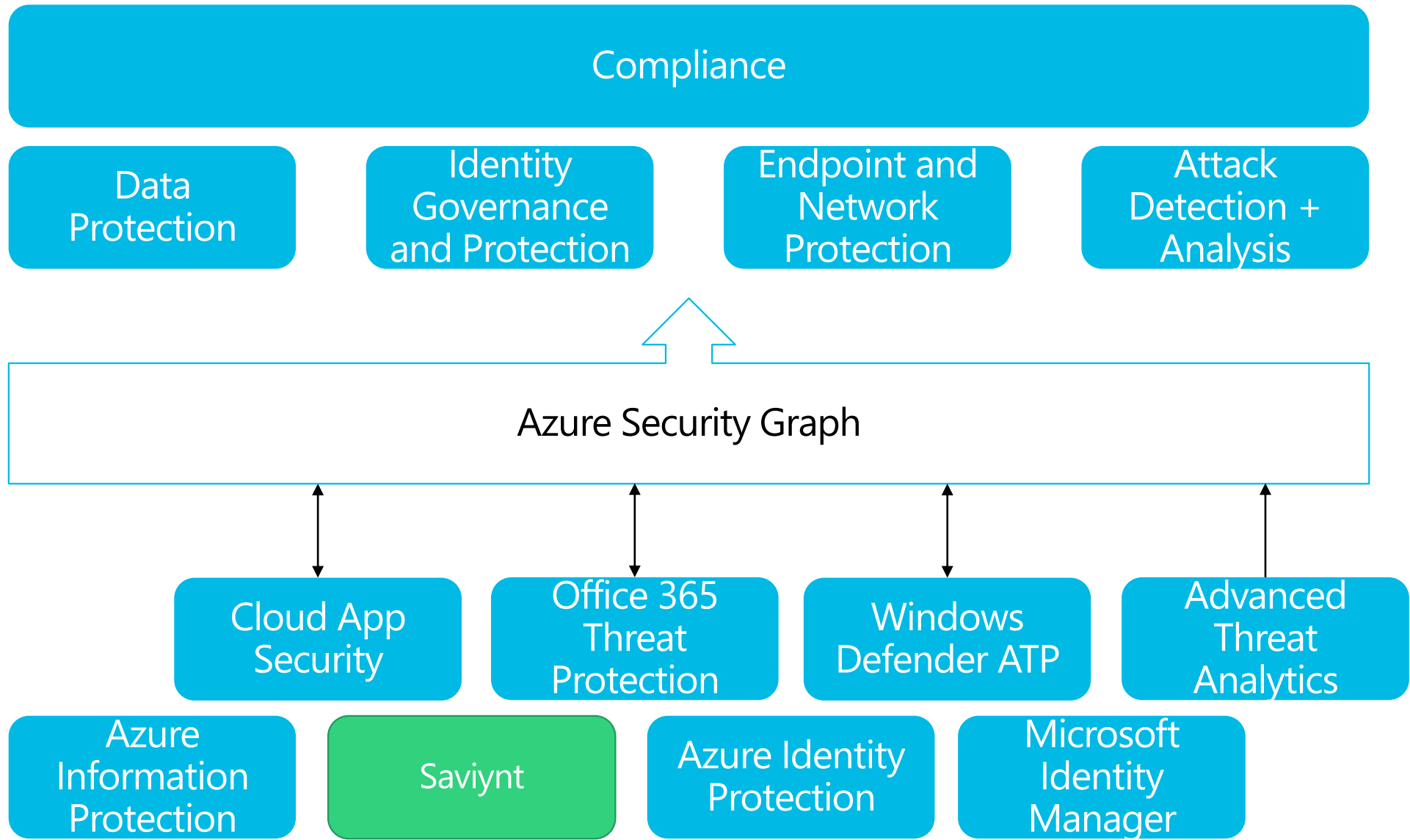
Webhook

Runbook

# Security Solutions



# Security Solutions



# Identity Governance and Protection

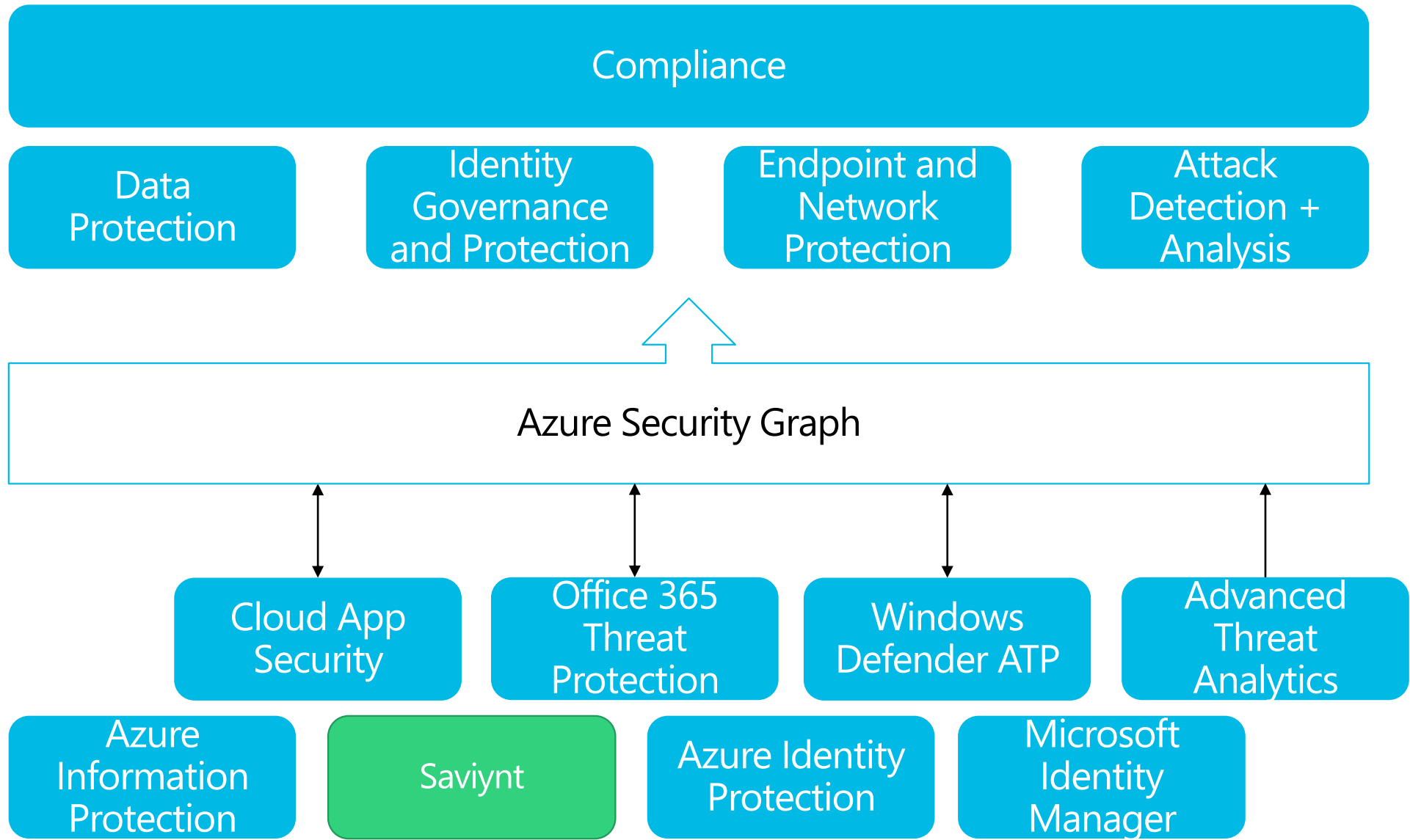


- Primary goals: to ensure that accounts and entitlements
  - Grant the minimum necessary access
  - Are modified in a timely and accurate manner
  - Are auditable for appropriate periods of time
  - Fulfil the compliance requirements of the organization
  - Do not combine to allow risky behaviour
- Machine Learning is used to identify risky behaviors
- Well-managed identities (including their credentials) are key to security
  - Password management, password replacement, MFA, certificates, biometrics contribute to better security
  - Just-In-Time approaches reduce attack surface

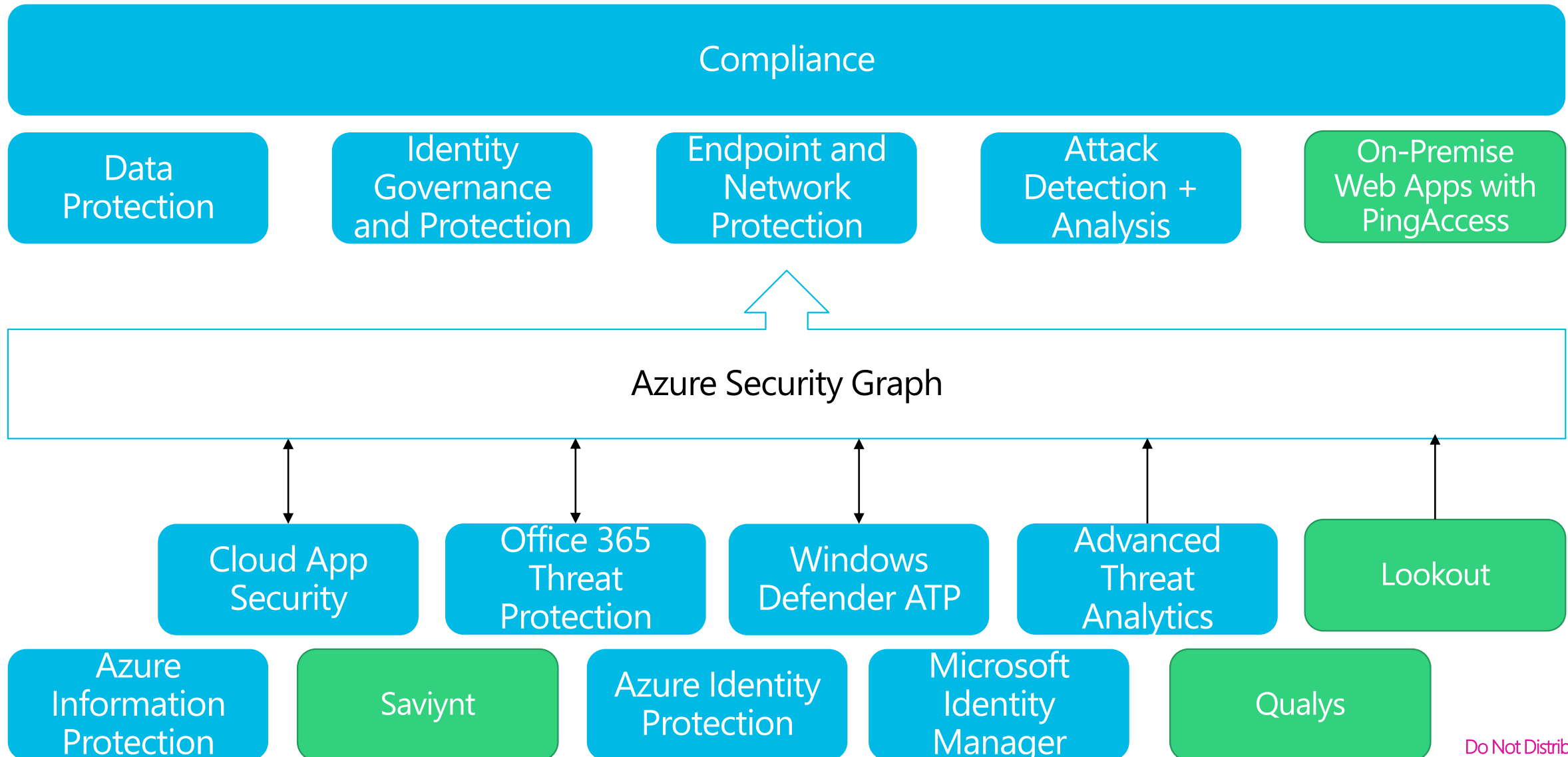
# Third Party solutions

- Third parties are increasingly becoming part of the ecosystem
  - Savyint (Identity and Entitlement Risk)
  - Qualys (Configuration)
  - Lookout (Endpoint Risk)
  - PingAccess (Identity Risk-Aware Application Access)
- This will only increase over time

# Security Solutions



# Security Solutions





# Impact of the Security Transformation



- Security integration features, and interaction with the Security Graph, are increasingly baked into Microsoft and third-party products
- The speed and reliability with which threats can be detected is increasing
- Rules-based systems can respond to detected threats much faster than human-moderated response, increasing security
- Modern CASB solutions mean that cloud-based systems can be approved with confidence: inappropriate use or sharing of data will be blocked or flagged and remediated effectively and fast

# Can you profit from Security Transformation?



- Consider how your organizations can make use of emerging technologies in security
  - Global-scale signals
  - Machine Learning
  - Integrated Security Correlation and Visualization
- Oxford Computer Group provides workshops and education to help you understand the opportunities, as well as specific design and implementation services



Thank You!

[james.cowling@oxfordcomputergroup.com](mailto:james.cowling@oxfordcomputergroup.com)

[info@oxfordcomputergroup.com](mailto:info@oxfordcomputergroup.com)