Microsoft

Defense in depth:

Enterprise Mobility + Security advanced protection capabilities

by Alex Weinert, Microsoft Identity Services, @alex_t_weinert

My grandfather was a Welsh Guardsman. You may know them as the guys in the bearskin hats and red coats who guard Buckingham Palace (though they are more than that).

Having family in North Wales has allowed me to study the castles built there in the 13th century. Even in their weathered state, now abandoned to tourism, they are awesome to behold. The pinnacle of military technology in their day, they allowed a small garrison to hold off hordes of attackers, due in part to their rings of defense.

Defensive rings map well to the cybersecurity principle of "defense in depth," the idea of building multiple redundant defenses into systems. We build each ring to be effective, but if the barbarians manage to cross the moat, it's great if we can retreat to the walls and defend from there. If a bad guy gets through one ring, the next one can catch him.

Microsoft Enterprise Mobility + Security has similar defensive rings:

- **Azure Active Directory (Azure AD) Identity Protection Security Reports**, like watchmen in the towers, allow you to see configuration vulnerabilities, which are session and user risk signals that our machine learning, heuristic, and research systems detect.
- **Azure Active Directory Risk-Based Conditional Access**, like guards at the gate, allows you to put those risk signals to work, automatically intercepting bad sign-ins and deactivating compromised passwords.
- **Microsoft Cloud Application Security**, like a security escort, allows you to monitor and control activity between an app and the user.
- **Advanced Threat Analytics**, like a watchman in the treasury, provides deep forensic insights into what's happening in your on-premises environment, allowing you to see precisely how a hacker acted in your environment so you can provide a rapid response.
- **Azure Active Directory Privileged Identity Management**, like a keeper of keys, ensures that you have the minimum possible administrative attack surface by giving you just-in-time and just-enough administrative access.
- **Azure Information Protection**, like guards who protect treasure in transit, allows you to protect data with strong encryption and access policies regardless of where it goes.
- **Microsoft Intune Mobile Device Management and Mobile Application Management**, like a protector of the armory, help you ensure that devices and apps used in your organization are secure and healthy, again protecting data on these devices against device loss, malware, or other threats.

Let's garrison the castle and briefly talk about how these technologies work together to create a Secure Productive Enterprise. With the realities of shrinking IT budgets and increasing attacks it's a good time to learn how even a small garrison can hold off hordes of attackers.

Azure AD Identity Protection Security Reports: *the watchmen in the tower*

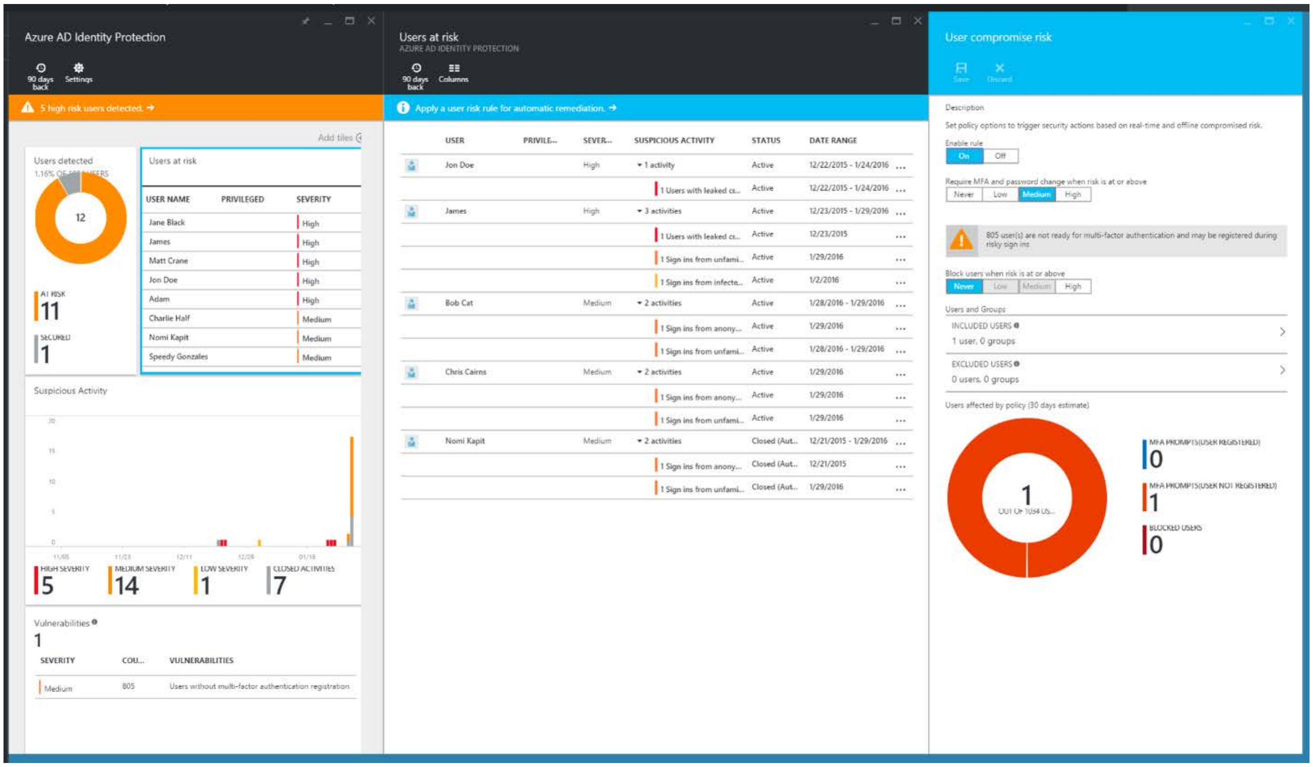
In addition to single sign-on for millions of companies and thousands of SaaS and on-premises applications (including, of course, Office 365), Microsoft's Identity Division also provides Microsoft account, our consumer-facing IdP, which supports Xbox, Outlook, OneDrive, Skype, and more. The combined data from these services—more than 10TB every day—gives us tremendous insight into what's normal behavior and, critically, what deviates from normal and indicates risk. This is our strongest signal source for Azure AD Identity Protection.

We get even more signal sources from other data in the Microsoft Intelligent Security Graph—botnet infections from the Digital Crimes Unit, data contributions, security research, and threat reports from the Microsoft Security Response Center, as well as SaaS specific data from services like Office 365 Exchange (for example, a good user started sending spam)—providing great triangulation on the signal from our identity services.

Security reports fall into three broad categories:

- Cases where a sign-in is anomalous and associated with some level of risk that it is an attempt at unauthorized access.
- Cases with significant indication that a user's credentials have been compromised, because they are showing up frequently in risky sign-ins, or because we have discovered them in criminal hands.
- Cases where your security posture could be improved, that is, vulnerabilities in your defenses that configuration changes can mitigate.

Azure AD Identity Protection Security Reports provide you all of this information, either in the Azure AD Portal or programmatically (so you can integrate it into your SIEM or ticketing system).



5 high risk users detected. →

Users at risk

USER NAME	PRIVILEGED	SEVERITY
Jane Black		High
James		High
Matt Crane		High
Jon Doe		High
Adam		High
Charlie Half		Medium
Nomi Kapit		Medium
Speedy Gonzales		Medium

Vulnerabilities
1

SEVERITY	COU...	VULNERABILITIES
Medium	805	Users without multi-factor authentication registration

Apply a user risk rule for automatic remediation. →

USER	PRIVILE...	SEVER...	SUSPICIOUS ACTIVITY	STATUS	DATE RANGE
Jon Doe		High	▾ 1 activity	Active	12/22/2015 - 1/24/2016
			1 Users with leaked cr...	Active	12/22/2015 - 1/24/2016
James		High	▾ 3 activities	Active	12/23/2015 - 1/29/2016
			1 Users with leaked cr...	Active	12/23/2015
			1 Sign ins from unfami...	Active	1/29/2016
			1 Sign ins from infecte...	Active	1/2/2016
Bob Cat		Medium	▾ 2 activities	Active	1/28/2016 - 1/29/2016
			1 Sign ins from anony...	Active	1/29/2016
			1 Sign ins from unfami...	Active	1/28/2016 - 1/29/2016
Chris Cairns		Medium	▾ 2 activities	Active	1/29/2016
			1 Sign ins from anony...	Active	1/29/2016
			1 Sign ins from unfami...	Active	1/29/2016
Nomi Kapit		Medium	▾ 2 activities	Closed (Aut...	12/21/2015 - 1/29/2016
			1 Sign ins from anony...	Closed (Aut...	12/21/2015
			1 Sign ins from unfami...	Closed (Aut...	1/29/2016

Description

Set policy options to trigger security actions based on real-time and offline compromised risk.

Enable rule
[✓ On] Off

Require MFA and password change when risk is at or above
Never Low [✓ Medium] High

805 user(s) are not ready for multi-factor authentication and may be registered during risky sign ins

Block users when risk is at or above
[✓ Never] Low Medium High

Users and Groups

INCLUDED USERS
1 user, 0 groups

EXCLUDED USERS
0 users, 0 groups

Azure AD Identity Protection Security Reports display risky users and sign-ins.

Learn more about Azure AD Identity Protection Security Reports here.

Like the watchmen posted high atop the castle tower, Azure AD Identity Protection Security Reports give you insights into what's happening in your environment so you can take action.

Now, imagine the watchmen see a problem and call down to the guards at the gate to give them warning…

Azure AD Conditional Access: *the guards at the gate*

One critical aspect of good security is that it's nearly invisible to most users. Excessive friction inhibits productivity, and clever users will find ways to work around things that block their productivity, which can create risk. While we could challenge every user at every sign-in, ideally, we maximize productivity by allowing users to get their work done with minimal interruption, while stopping the bad guys in their tracks.

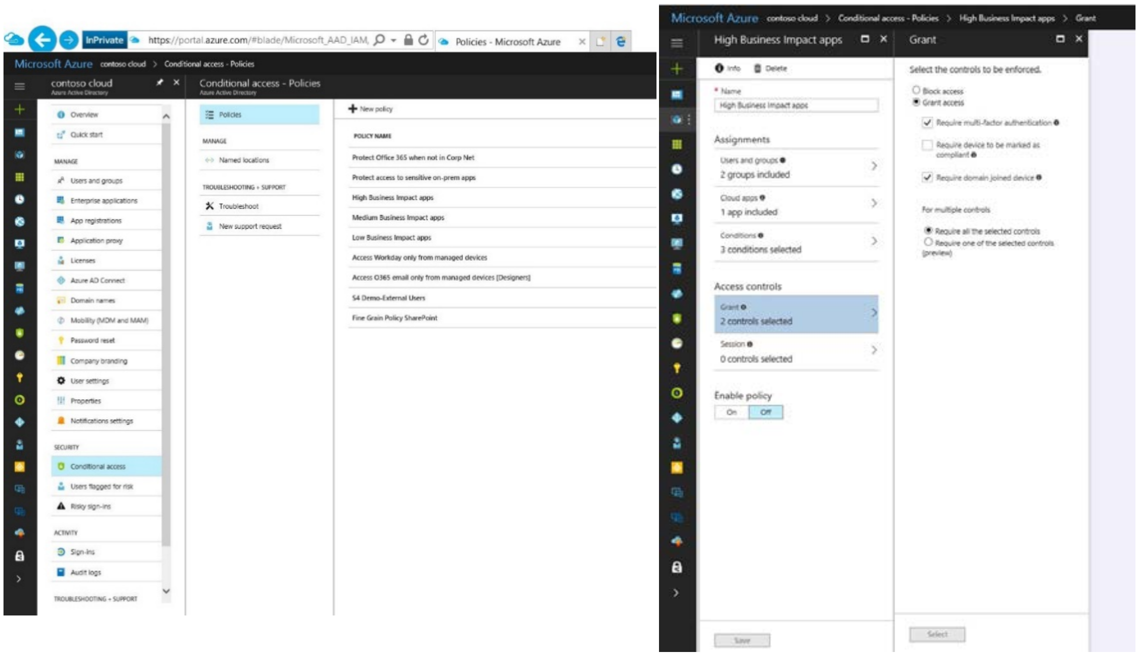
Azure AD Conditional Access allows us to do just that. Previously, you might've had to say, "No access from off the corporate network" or "No access from a personal device," but Azure AD Conditional Access allows you to say, effectively, "Yes, but there are conditions." For example, instead of blocking access to work email from a personal device, you can say one of the following:

- Yes, but you must be on a secure, compliant device (using Intune).
- Yes, but you must first pass a Multi-Factor Authentication challenge.
- Yes, but you won't be allowed to print, save, or download documents.

These are just a few examples. Azure AD Conditional Access provides a powerful framework for regulating access in governance, risk, and compliance scenarios. When combined with the information from AADIP, it gains even more power, allowing you to say, effectively, one of the following:

- Yes, unless there is risk in your session.
- Yes, but because your credentials are at risk you must first change your password.
- Yes, but we will monitor your session because of security concerns.

Adding Azure AD Identity Protection risk assessments to Azure AD Conditional Access allows you to relax challenges and friction in cases where no risk is present. It also allows you to have an "umbrella policy"—whatever else your corporate policies dictate, you can issue challenges in cases of unanticipated risks that the Intelligent Security Graph has detected in the sign-in, ensuring you stay secure in the face of evolving threats (this is by far the most important thing you can do to protect against compromised credentials!).



POLICY NAME

- Protect Office 365 when not in Corp Net
- Protect access to sensitive on-prem apps
- High Business Impact apps
- Medium Business Impact apps
- Low Business Impact apps
- Access Workday only from managed devices
- Access O365 email only from managed devices [Designers]
- S4 Demo-External Users
- Fine Grain Policy SharePoint

Microsoft Azure
contoso cloud > Conditional access - Policies > High Business Impact apps > Grant
High Business Impact apps
Info
Delete
Grant
Save
Select

* Name: High Business Impact apps

Assignments
- Users and groups: 2 groups included
- Cloud apps: 1 app included
- Conditions: 3 conditions selected

Access controls
- Grant: 2 controls selected
- Session: 0 controls selected

Enable policy: On [✓ Off]

Select the controls to be enforced.

○ Block access
● Grant access

☑ Require multi-factor authentication
□ Require device to be marked as compliant
☑ Require domain joined device

For multiple controls

● Require all the selected controls
○ Require one of the selected controls (preview)

Azure AD Conditional Access allows good users to get their work done with minimal interruption.

In our castle analogy, you can think of Azure AD Conditional Access as the guards at the gate, welcoming good citizens into the castle while challenging others to confirm their identities, and denying entry to the riskiest.

Or perhaps we'll let them pass, but assign a security escort…

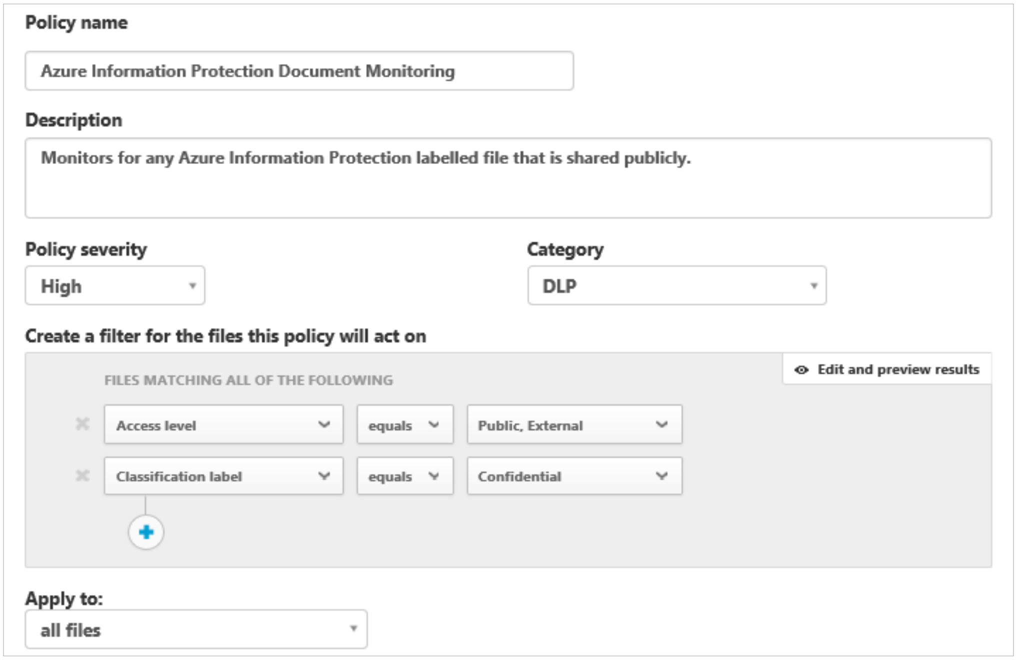
Microsoft Cloud App Security: *the security escort*

The primary role of Azure AD is to provide secure, reliable single sign-on for users across all applications, ensuring that only authorized users gain access. Effectively, it allows users to access all the critical resources they need to be productive once they've been authenticated.

But what if the authorized user does something wrong? What if they are no longer loyal to the organization, or are under duress? Or some malware is riding along in their session? Once Azure AD grants a user access, Azure AD can't see the specifics of what they do during their interactions with the application, making in-session anomalies invisible to Azure AD.

That's where Microsoft Cloud App Security comes in. Cloud App Security provides a mechanism to observe and manage what happens inside sessions between users and the applications they access. For example, Cloud App Security can tell you if a large volume of data is being accessed, apply specific API level restrictions based on configured policies, or even shut down a session if behavior become anomalous.

Together with Azure AD Conditional Access, Cloud App Security allows you to apply this enhanced monitoring and control when your policy requires it, and to protect yourself from session hijack, rogue users, and other session anomalies while ensuring good users can access resources with specific download or action restrictions to mitigate session risks.



Policy name: Azure Information Protection Document Monitoring

Description: Monitors for any Azure Information Protection labelled file that is shared publicly.

Policy severity: High

Category: DLP

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING

- Access level equals Public, External
- Classification label equals Confidential

Apply to: all files

Microsoft Cloud App Security helps you observe and manage sessions between users and the apps they access.

You can think of Microsoft Cloud App Security as the security escort, going along to ensure the user doesn't do—or come to—any harm.

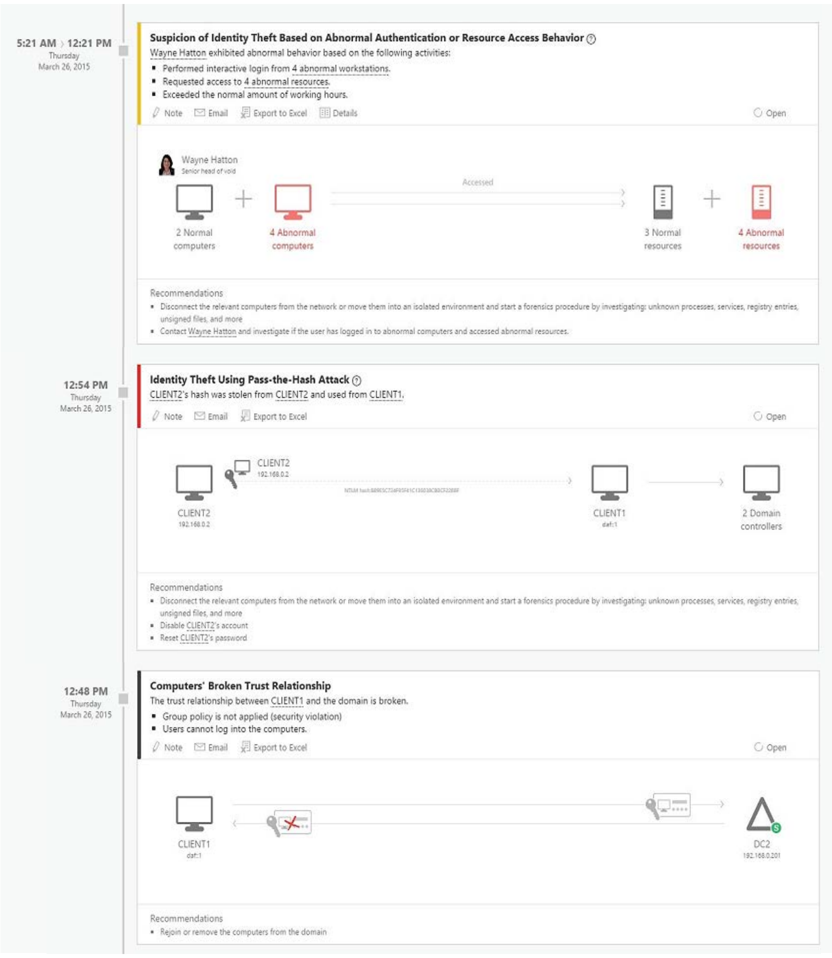
Microsoft Advanced Threat Analytics: *the watcher in the treasury*

The layers of defense described above provide very effective protection for your organization. Unfortunately, user behavior (e.g. falling for phishing attacks or re-using credentials on insecure sites), vulnerabilities of traditional on-premises infrastructure (e.g. VPNs), and clever attacks sometimes allow an attacker to get through.

Attackers move incredibly quickly once they gain access to a working credential, often VPN'ing into a corporate network and using log files, memory resident tokens, unencrypted files, and a host of other mechanisms to dig in and elevate privilege until, before you know it, they are domain admins and nearly impossible to get rid of.

Worse, where on-premises attacks are concerned, the network boundaries you relied on to keep you safe actually make it impossible for our cloud-based intelligence and protection mechanisms like Azure AD Identity Protection, Azure AD Conditional Access, and Cloud App Security to keep you safe.

Most companies have a great many legacy applications and resources running in their on-premises networks, so the hybrid environment is a reality for the foreseeable future. Unfortunately, these on-premises resources are often the most vulnerable when they have both inadequate security capabilities and valuable data.



5:21 AM › 12:21 PM
Thursday
March 26, 2015

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior

Wayne Hatton exhibited abnormal behavior based on the following activities:

- Performed interactive login from 4 abnormal workstations.
- Requested access to 4 abnormal resources.
- Exceeded the normal amount of working hours.

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Contact Wayne Hatton and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

12:54 PM
Thursday
March 26, 2015

Identity Theft Using Pass-the-Hash Attack

CLIENT2's hash was stolen from CLIENT2 and used from CLIENT1.

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable CLIENT2's account
- Reset CLIENT2's password

12:48 PM
Thursday
March 26, 2015

Computers' Broken Trust Relationship

The trust relationship between CLIENT1 and the domain is broken.

- Group policy is not applied (security violation)
- Users cannot log into the computers.

Recommendations

- Rejoin or remove the computers from the domain

Microsoft Advanced Threat Analytics helps you rapidly detect penetration of your on-premises environment.

The reality is that, as of this writing, if an attacker establishes a foothold in your on-premises environment, they will maintain it for an average of 140 days before you can begin to remove them—if you can remove them.

Luckily, Microsoft Advanced Threat Analytics gives you a tool to rapidly detect penetration of your on-premises environment so you can get attackers out before they dig in.

Advanced Threat Analytics quietly:

- builds a profile of what normal behavior looks like in your environment, and then
- notes any activity which differs from normal behavior, and then
- alerts you to these anomalies, along with an explanation of what attack the anomaly maps to, which resources are affected, and any recommended remediation.

Advanced Threat Analytics can you give you the rapid warning you need to respond before lateral movement or data exfiltration begin.

If your on-premises environment is like the royal treasury, Microsoft Advanced Threat Analytics is like the watcher hidden in the room, ready to sound the alarm if an attacker has broken in.

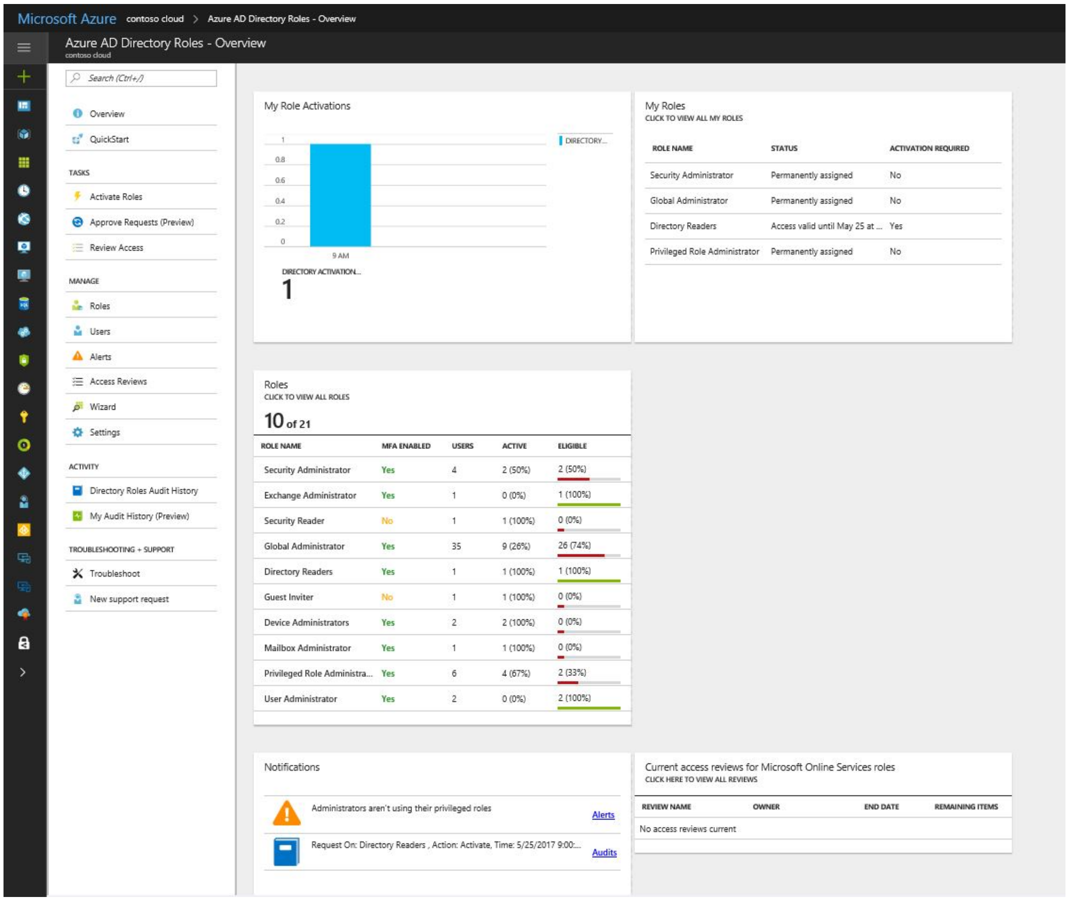
Azure AD Privileged Identity Management: *the keeper of keys*

The harsh reality is that with phishing, malware, breach, weak passwords, and lack of conditional access policies, determined attackers have a chance. Detection isn't always in real time, and sometimes false negatives occur. Since account compromise remains a possibility, the best way to minimize risk to your organization is to assume breach has happened or will happen.

While any compromised account is bad, a compromised admin account is catastrophic. If you assume some number of your organization's accounts will eventually be breached, it's critical to minimize the probability that those accounts have admin privileges.

Azure AD Privileged Identity Management gives you the tool you need to do just that. It empowers you to ensure you have the smallest possible number of admin-privileged users:

- It analyzes your environment to help identify whether you have admin privileges that are going unused or an excessive number of privileged users relative to your industry, allowing you to remove privileges from users who no longer need them.
- It helps you set up policies to grant admin access only when needed, on for as long as needed, and only in compliance with your elevation policies.



My Roles
CLICK TO VIEW ALL MY ROLES

ROLE NAME	STATUS	ACTIVATION REQUIRED
Security Administrator	Permanently assigned	No
Global Administrator	Permanently assigned	No
Directory Readers	Access valid until May 25 at ...	Yes
Privileged Role Administrator	Permanently assigned	No

Roles
CLICK TO VIEW ALL ROLES
10 of 21

ROLE NAME	MFA ENABLED	USERS	ACTIVE	ELIGIBLE
Security Administrator	Yes	4	2 (50%)	2 (50%)
Exchange Administrator	Yes	1	0 (0%)	1 (100%)
Security Reader	No	1	1 (100%)	0 (0%)
Global Administrator	Yes	35	9 (26%)	26 (74%)
Directory Readers	Yes	1	1 (100%)	1 (100%)
Guest Inviter	No	1	1 (100%)	0 (0%)
Device Administrators	Yes	2	2 (100%)	0 (0%)
Mailbox Administrator	Yes	1	1 (100%)	0 (0%)
Privileged Role Administra...	Yes	6	4 (67%)	2 (33%)
User Administrator	Yes	2	0 (0%)	2 (100%)

Notifications

Administrators aren't using their privileged roles — Alerts

Request On: Directory Readers , Action: Activate, Time: 5/25/2017 9:00:... — Audits

Current access reviews for Microsoft Online Services roles
CLICK HERE TO VIEW ALL REVIEWS

REVIEW NAME	OWNER	END DATE	REMAINING ITEMS
No access reviews current			

Azure AD Privileged Identity Management helps you minimize the number of admin-privileged users.

Most users who need to do privileged tasks only do so for a small fraction of their day. Using Azure AD Privileged Identity Management, you can set up a policy so that, for example, privileged access is only granted with manager approval, and only within a multi-factor authentication session, and only lasts for 60 minutes. In other words, policies are configurable to whatever makes most sense for your organization.

In this way, Azure AD Privileged Identity Management acts as a keeper of the keys, helping ensure that if a user is compromised, the most critical assets remain safe.

Microsoft Intune: *protect treasure in transit (part one)*

Even when we're sure an identity isn't compromised, there's always a chance a user will download content onto an unhealthy device, such as one that's unencrypted and missing PIN protection.

For example, if a user is synchronizing corporate mail onto a mobile phone which is not PIN locked, then anyone picking up that phone has unfettered access to everything in their mailbox. If a user has downloaded a spreadsheet full of key contract information onto their personal laptop and that laptop is stolen, so is the contract information.

Many devices act as a trust factor for user authentication or have active sessions, making unhealthy devices a threat to online resources as well. And malware, leaking user credentials every time the user does an interactive sign-in, is a real threat.

The age of Bring Your Own Device is here, but we must acknowledge the reality that bad things happen to good devices, whether malware, theft, or loss. Microsoft Intune can ensure that devices are safely in compliance and as resistant as possible to issues like malware and device theft.

In some cases, it may also make sense to ensure that only properly configured and approved applications are used to access sensitive data. Intune also supports mobile application management, ensuring that the application and its configuration is approved by your organization.

You can think of Intune as ensuring the integrity of the treasure chest and its locks, helping guarantee the security of what's inside.

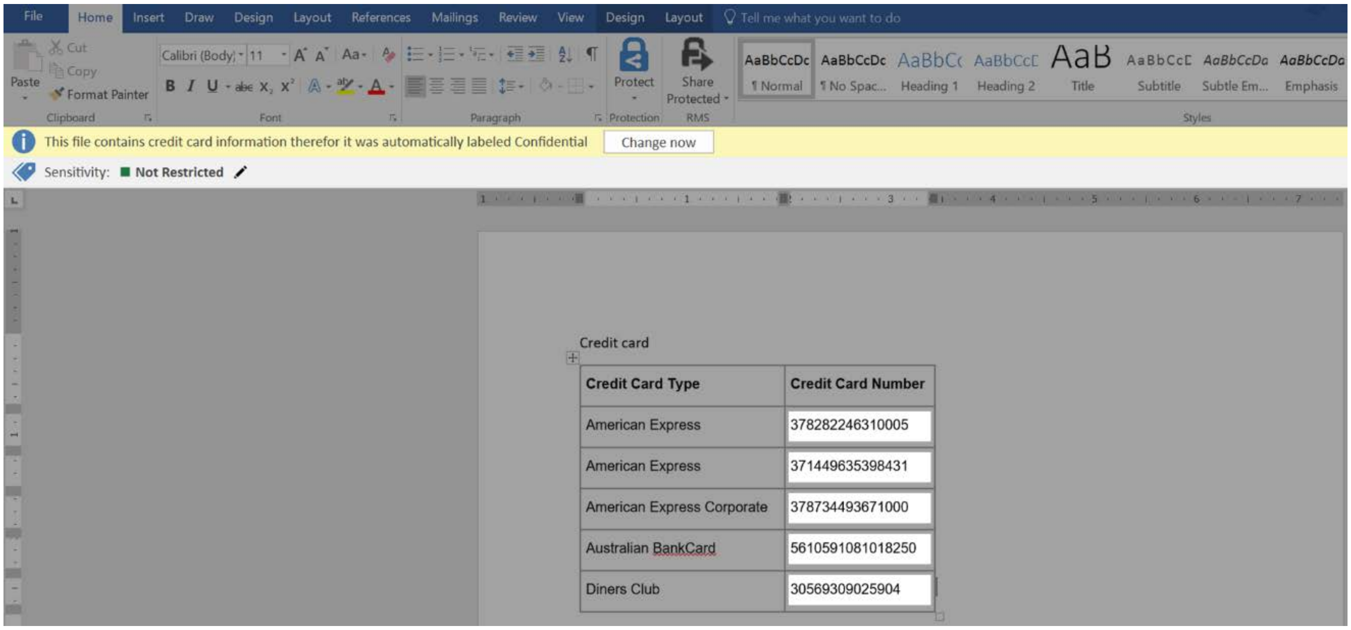
Azure Information Protection: *protect treasure in transit (part two)*

Even when we're able to ensure that the user accessing a resource in our environment is who they say they are and is well-behaved and in a healthy environment, the risk remains that they'll share a document with someone who's not, or become compromised after they've downloaded the content.

Azure Information Protection allows you to encrypt documents to ensure that even if the document is transmitted to an insecure environment, only authorized users, as defined by your policies, can access the document.

Better still, it can do the following:

- Automatically classify documents, detecting when someone has copied from a secure document or is typing sensitive data, such as social security numbers or credit card numbers.
- Show you where documents are being opened, and by whom.
- Allow you to revoke all copies of a document, making it unreadable wherever it has gone.



This file contains credit card information therefor it was automatically labeled Confidential

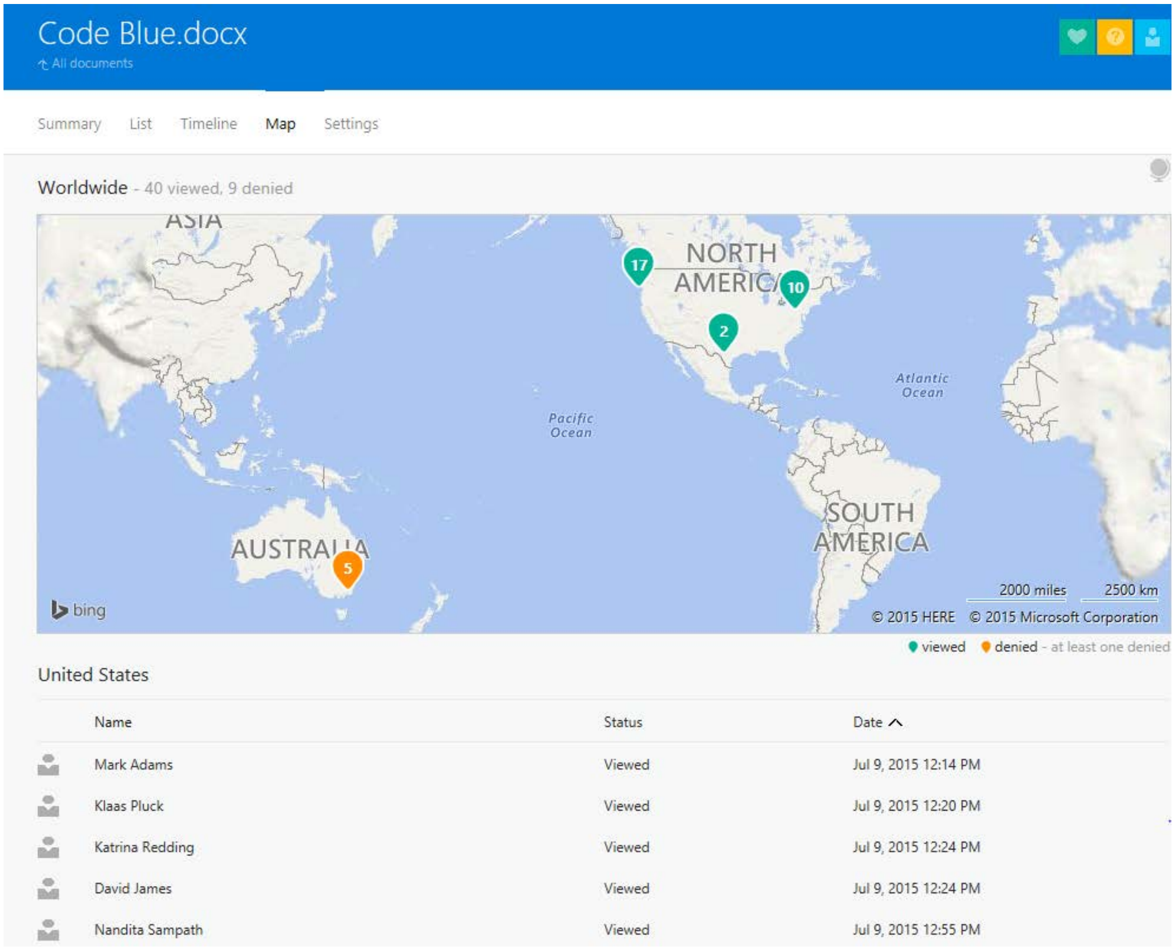
Change now

Sensitivity: 🟩 Not Restricted

Credit card

Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904

Azure Information Protection can automatically classify documents, detecting when someone has copied from a secure document or is typing sensitive data, such as social security numbers or credit card numbers.



Worldwide - 40 viewed, 9 denied

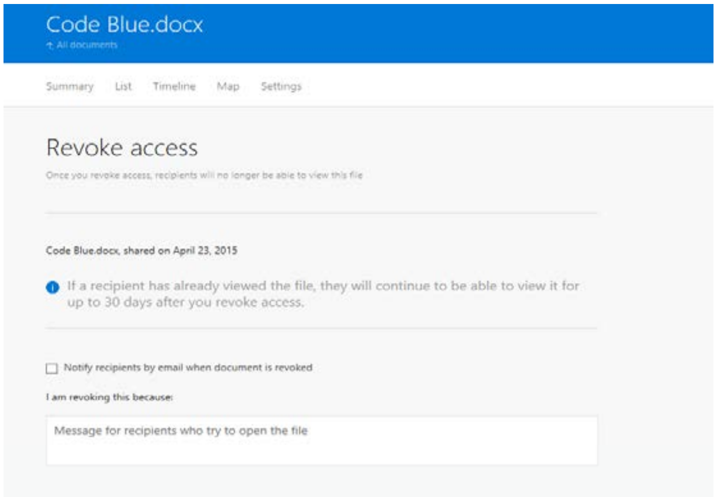
United States

Name	Status	Date
Mark Adams	Viewed	Jul 9, 2015 12:14 PM
Klaas Pluck	Viewed	Jul 9, 2015 12:20 PM
Katrina Redding	Viewed	Jul 9, 2015 12:24 PM
David James	Viewed	Jul 9, 2015 12:24 PM
Nandita Sampath	Viewed	Jul 9, 2015 12:55 PM

Azure Information Protection can let you know where documents are being opened, and by whom.

Azure Information Protection gives you the power to protect data in transit—wherever your data goes, you can be sure that only authorized people can read it.

In our castle analogy, Azure Information Protection is a bit of sorcery, ensuring the treasure turns to dust if it falls into the wrong hands.



Code Blue.docx
↑ All documents

Summary List Timeline Map Settings

Revoke access

Once you revoke access, recipients will no longer be able to view this file

Code Blue.docx, shared on April 23, 2015

If a recipient has already viewed the file, they will continue to be able to view it for up to 30 days after you revoke access.

□ Notify recipients by email when document is revoked

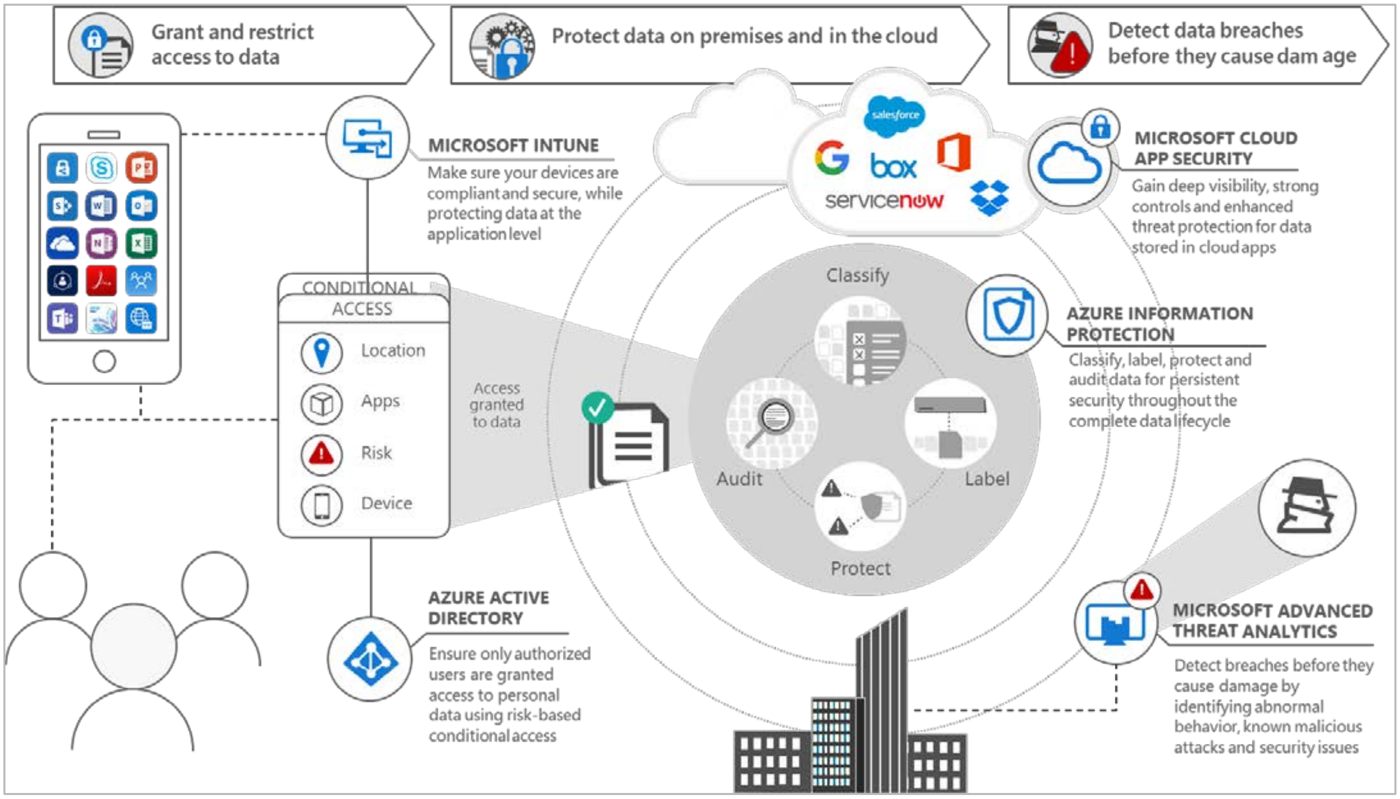
I am revoking this because:

Message for recipients who try to open the file

Azure Information Protection allows you to revoke all copies of a document, making it unreadable wherever it has gone.

Putting it together: *defense in depth and EMS*

Now that you've toured the rings of defense, here's a map and table that summarize them:



Grant and restrict access to data

Protect data on premises and in the cloud

Detect data breaches before they cause dam age

MICROSOFT INTUNE
Make sure your devices are compliant and secure, while protecting data at the application level

MICROSOFT CLOUD APP SECURITY
Gain deep visibility, strong controls and enhanced threat protection for data stored in cloud apps

AZURE INFORMATION PROTECTION
Classify, label, protect and audit data for persistent security throughout the complete data lifecycle

AZURE ACTIVE DIRECTORY
Ensure only authorized users are granted access to personal data using risk-based conditional access

MICROSOFT ADVANCED THREAT ANALYTICS
Detect breaches before they cause damage by identifying abnormal behavior, known malicious attacks and security issues

Microsoft Enterprise Mobility + Security offers multiple rings of defense.

Feature	Capabilities	Threats Mitigated	Because
Azure AD Identity Protection Reports	Insights into risky sign-in attempts and users whose credentials are compromised	Undetected intrusion, highly vulnerable users	Criminals attempt almost 100M fraudulent sign-ins every day, and you should know if one impacts you.
Azure AD Conditional Access	Automated sign-in challenge (with multi-factor) or block based on governance, compliance, or risk factors	Attempted malicious sign-in, vulnerable users	You can intercept the clear majority of attacks before they can cause harm by having policy-based risk response to disrupt criminals.
Microsoft Cloud App Security	In-session monitoring and control	Rogue users, malware on machine	Sometimes an authorized user does unauthorized things—or their machine does.
Microsoft Advanced Threat Analytics	On-premises behavior analysis and anomaly detection, detection of bad actors in your organizational network	Undetected inside attackers or undetected attackers using stolen credentials via VPN	Your on-premises environment represents your greatest risk, making rapid response to intrusion your best hope.
Azure AD Privileged Identity Management	Detection and mitigation of excess administrative privilege, just-enough and just-in-time access for privileged tasks	Compromise of privileged accounts	Every admin account represents substantial risk if the account is compromised. For privileged access, less is more.
Microsoft Intune	Enforcement of device compliance with policies to ensure device health and safety, including PIN lock, encryption, and current malware protection	Data loss due to lost or stolen devices, infected devices	Machines get lost or stolen and malware can exfiltrate data.
Azure Information Protection	Securing of data in transit with encryption, document tracking, and auto-classification	Data loss due to non-compliant opening of documents	Documents get emailed outside of your span of control (to users and machines that may be insecure).

Summary

The brutal truth is that the rate and sophistication of attacks are increasing. Leaks of highly sophisticated attacks mated to old fashioned malware create new intersections of capabilities, while old techniques find new targets in governments and industry. The enemy is at the gates.

In a hostile environment with sophisticated attackers, we must assume breach—no one defense will suffice. Using the technologies and techniques above will help you establish a defensible fortress to protect your organization’s integrity and operations.

And a guard in a bearskin hat can’t hurt.

This paper explored the defense-in-depth capabilities of EMS. There are advanced security features in many Microsoft products, such as Windows Defender Advanced Threat Protection, the Microsoft Azure Security Center, or advanced security features in Windows Server. To learn more about these, please visit http://www.microsoft.com/security