



You Are Doing IT Security Wrong Understanding the Threat of Modern Cyberattacks

Michael Noel • @MichaelTNoel

BIWUG



Code of Conduct



As event and experience organizers, we seek to provide a respectful, friendly, professional experience for everyone, regardless of gender, sexual orientation, physical appearance, disability, age, race or religion.

We do not tolerate any behavior that is degrading to any gender, race, sexual orientation, or disability, or any behavior that would be deemed harassment or discrimination.

Individuals are responsible for knowing and abiding by our standards and we encourage everyone to assist in creating a welcoming and safe environment. Please report any concerns, suspicious or disruptive activity or behavior to the organizing team, so that we can address the issue immediately.



More information can be found on the [CollabDays Belgium & Netherlands](https://www.collabdays.org/2021-ben/about) website at <https://www.collabdays.org/2021-ben/about>

Our Platinum Sponsors



Community Sponsor



Our Gold Sponsors



Michael Noel

@MichaelTNoel



Authored/Co-authored 20 books including the best-selling SharePoint, Exchange, and Windows Unleashed series

Presented at over 250 events in 86 unique countries around the world

Partner at Convergent Computing in the San Francisco Bay Area (cco.com)





The Evolution of the Modern Hacker

WHY YOU SHOULD BE VERY CONCERNED

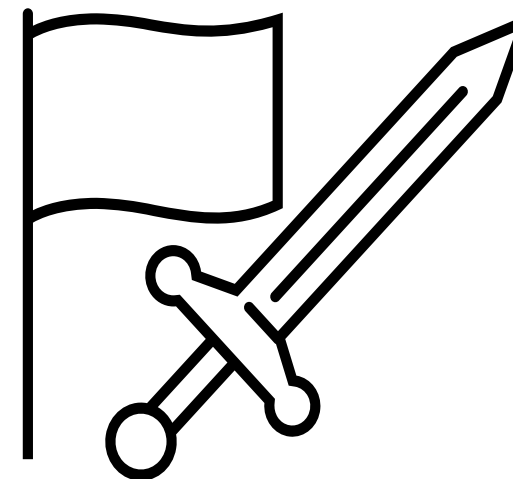
Spear Phishing

- Spear Phishing is a common approach used by hackers to target Executives and/or people in Finance/HR
- List of executives is easy to find from LinkedIn
- Email address formats are easy to discover
- Execs/Finance/HR personnel are targeted with crafted emails that make it look realistic (i.e. “Bob, here are the latest report numbers from ProjectX.”)
- Emails often have a ‘payload’ that is either attached or is a link to a nefarious website controlled by the attacker that then performs ‘credential harvesting’ by prompting the user to enter username/password
- Once username and password is obtained, the hacker is then able to login as that user and perform other lateral attacks or attempt to exfiltrate financial data or perform unauthorized transactions.



State Sponsored Attacks

- A rising number of hacking cases is coming from well-organized and well-funded hacking 'farms' that are sponsored by nation-states
- These hacking organizations are designed to steal trade and/or national secrets from organizations in a competing state
- Targets are not only defense or NGOs, but also include 'regular' organizations that can be targeted for financial reasons for for stealing intellectual property (IP.)



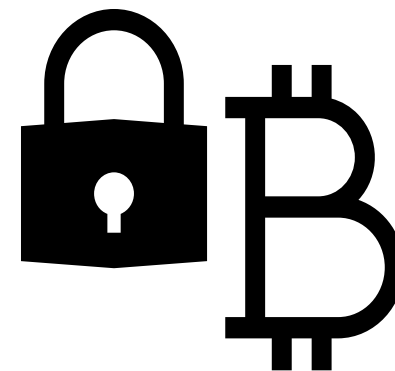


Ransomware

A major issue in recent years has been the rise of so-called 'ransomware' attacks.

These attacks work by using compromised account credentials to encrypt all data the hacker can find and then to 'throw away' the decryption key and only make it available after the payment of a cryptocurrency 'ransom.'

Aside from paying the ransom (which doesn't always work,) the only way to recover from this is via full restores, which can take days or weeks



Device Theft

The rise in 'petty theft' and 'smash and grab' theft has led to a rise in the theft of information devices such as laptops and cell phones

Thieves are getting more sophisticated and are starting to go after devices in car trunks by looking for active Bluetooth signals

Once stolen, if the contents of the device are not encrypted they are likely to be sold to competitors and/or other people interested in the IP



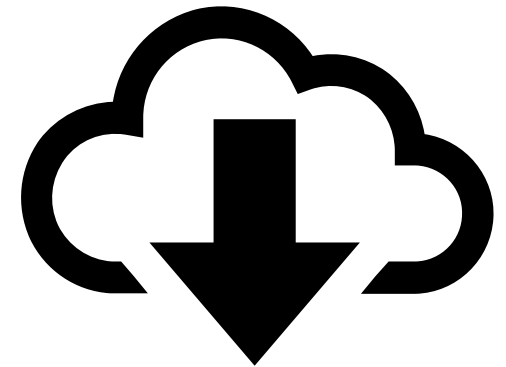
Intellectual Property Loss through “Oversharing”



Much of the IP that is lost or compromised is not lost via nefarious means, often it is simply ‘overshared.’

This is often due to well-meaning individuals who share documents via links or with poor security and then the email chain is publicized.

It can also happen if the proper security protocols are not chosen during the creation of cloud services



Passwords are Not as Secure as You Think

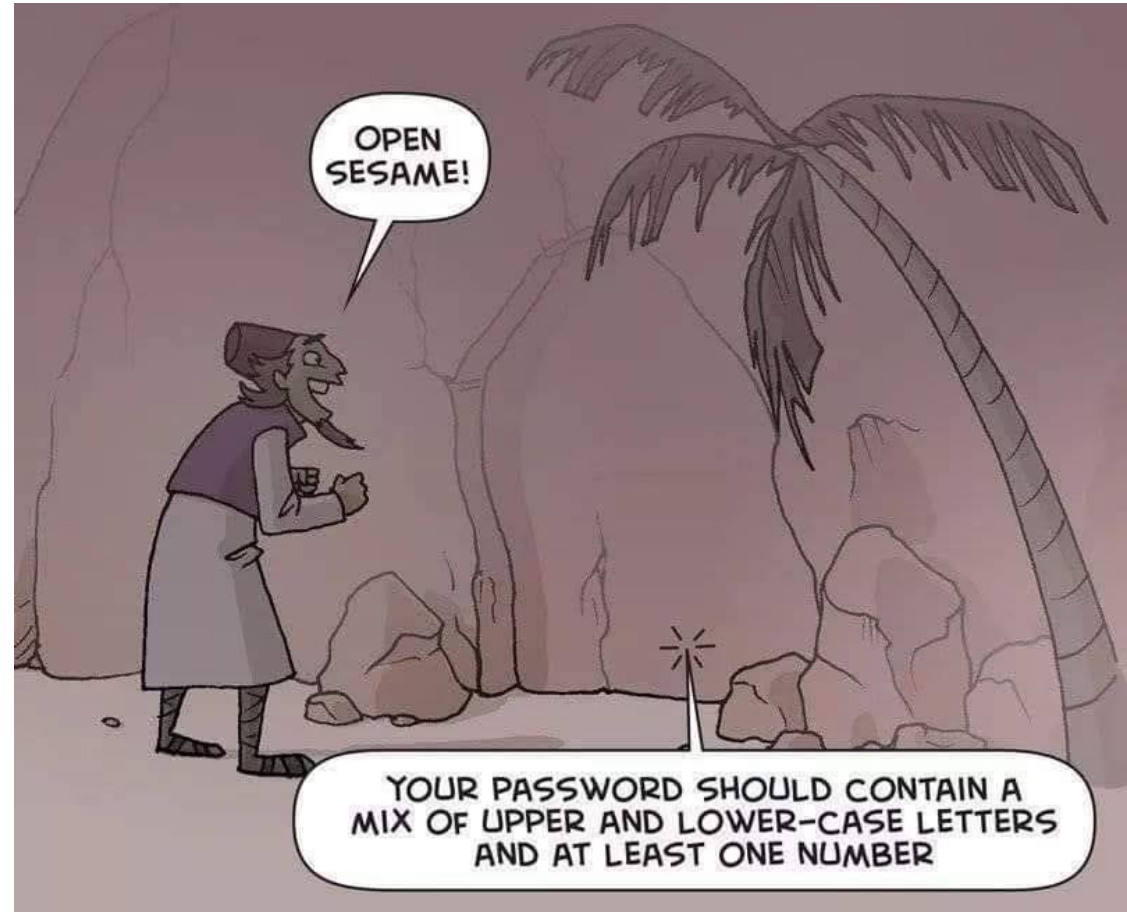


Key to password security is not necessarily length, complexity, or even age; but global **uniqueness**

Hackers have access to databases of 'pwned' passwords and can run password hashes against these databases in a matter of milliseconds

'Passphrases' that consist of unique seed words are infinitely more complex and much harder to crack (i.e. "Yellow birdseed hat pumpkin")

Test your password at <https://haveibeenpwned.com>





Cached Credentials

Exploiting Cached credentials on workstations are a common attack vector

Any user with local admin rights to a workstation (obtained legitimately or via phishing) can access the cached credentials of any other user who logged in at some point. If the passwords are not sufficiently complex or match any darknet database entries, they are EASILY cracked.





Lateral Attacks

Once a hacker has access to some small portion of your organization, they typically try to then perform 'lateral' attacks on other system, especially ones that provide for better access.

The goal is to get access to highly privileged accounts such as the Active Directory 'Domain Admins.'

"Golden Ticket" attacks using hacking tools such as Mimikatz can then leverage elevated domain rights (i.e. Domain Admin) to hack the krbst account and create non-expiring 'Golden Tickets' that give unfettered rights to all domain resources

11:11 AM Sep 1, 2018	<p>Suspected Golden Ticket usage (time anomaly)</p> <p>Jeff Leatherman used a Kerberos ticket from RDPSRV to access Contoso-DC (LDAP), exc ticket.</p> <p>Started at 12:00 AM Sep 1, 2018</p>
2:42 AM Sep 1, 2018	<p>Suspected Golden Ticket usage (nonexistent account)</p> <p>contoso.com\Boni, which does not exist in Active Directory, used a Kerberos ticket from</p>
11:56 AM Aug 30, 2018	<p>Suspected DCSync attack (replication of directory services)</p> <p>Nick Cowley on JEFFL-DESKTOP sent 1 replication request to Contoso-DC.</p>



Tips and Tricks to Protect your IP from Theft

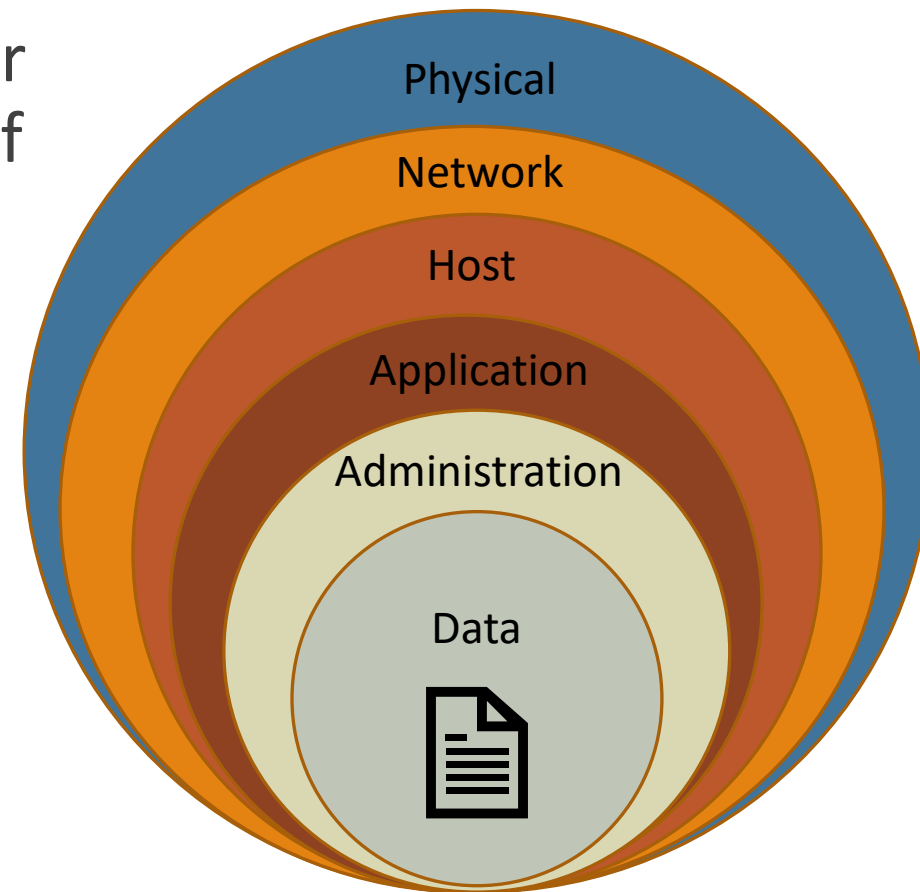
WHAT DO I DO TO PROTECT MY ORGANIZATION?



Defense in Depth Concepts

Defense in Depth is a concept in which your data is protected by multiple layers, each of which would need to be compromised before the data itself is accessed

Focus on all layers of the DiD model when designing your IT security





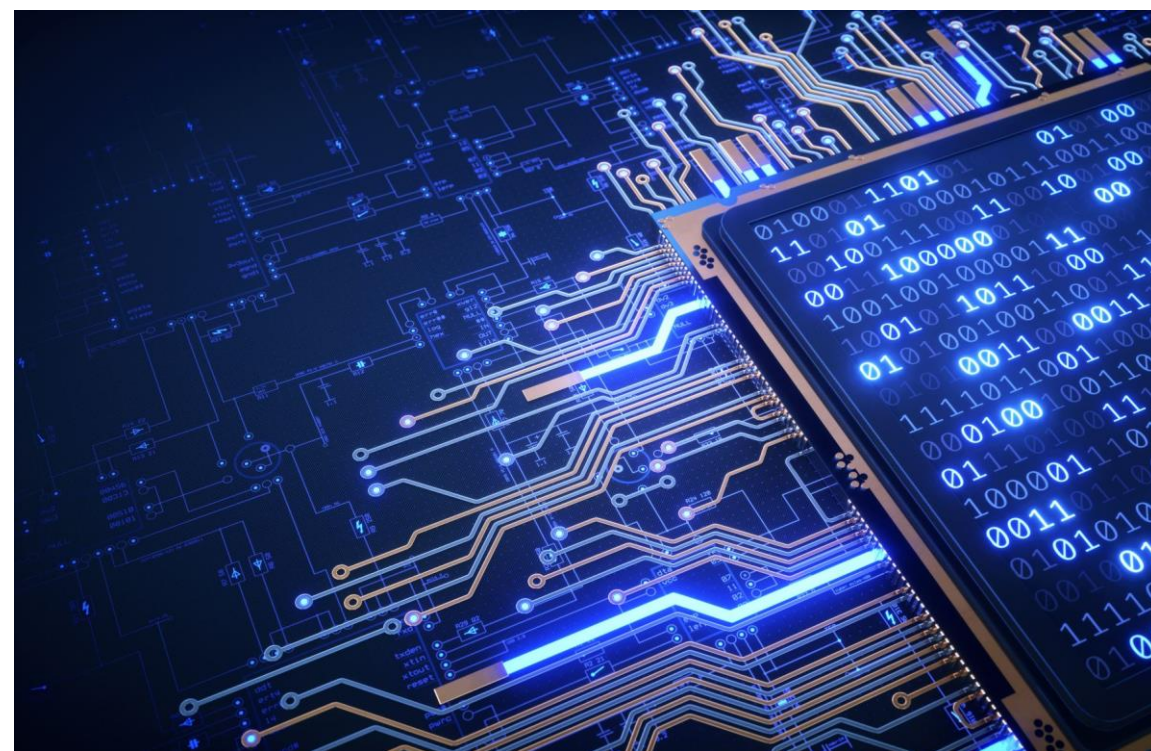
Password Best Practices

As previously mentioned, use passphrases instead of passwords

Don't change your password as often, but instead choose globally unique passwords

Use a password manager tool such as 1Password, LastPass, or the ones provided by Apple, Google

Never re-use passwords!





Hyperlink Safety

ALWAYS check your hyper-links (right-click if you can or hover over before you click) to see if they go to an site that makes sense. For example, an email from your bank should go to 'yourbank.com' and not 'susahkaya.net'.

Better yet, NEVER click on links in emails. If you think an email is legitimate, manually login to the site by opening a browser and typing in the site name or using a known-good bookmark.

We've changed the way we verify accounts at JP Morgan Chase and as a result you are required to complete an additional verification on your Bank Chase.

Verifying your account is simple: [click here](#) and follow the onscreen instructions.

Original URL:
http://reporting.ziffit.com/cgi-bin/rr/nobook:7486,nosent:1706,nosrep:20848/http://susahkaya.net/zq3yvrz?id=uk.co.brightec.ziffit&hl=en_gb?trackinglink=yyuusvfgdt
Click or tap to follow link.



Physical Security

Don't allow 'tailgating' into your facilities if you can physically prevent this. Modern 'subway-turnstile' type entryways can help prevent this

Instruct your employees to NEVER plug in loose thumbdrives into company systems. Dropping thumbdrives around a facility is a common approach to planting viruses

Follow best practice protocol around guest wireless isolation so that guests can't access anything internally. This also goes for wired connections (802.1x is a great way to prevent this.)



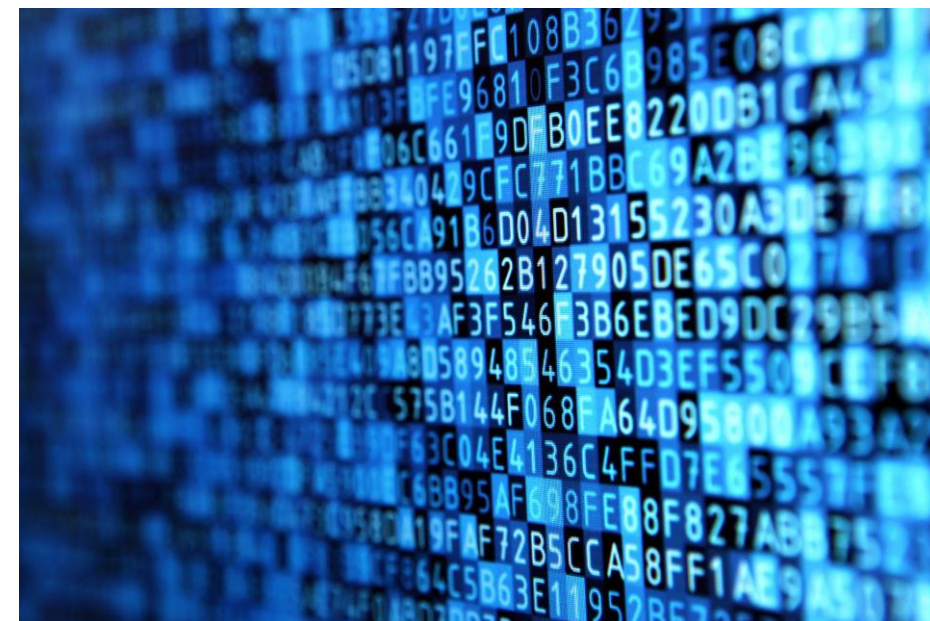


Full Disk Encryption

Always use full disk encryption (FDE) on ALL devices you use, including mobile devices. This will prevent the loss of data in the event of device theft.

Force devices to use PINs or Biometrics to unlock their devices before they are decrypted.

Put policies in place to 'wipe' systems remotely that have been compromised or that have had too many failed attempts to login.





Data Loss Prevention

Consider the use of Data Loss Prevention (DLP) technologies that restrict what happens AFTER the data has been accessed. This allows for restrictions on activities such as:

- Copy/Paste
- Print
- Save As.
- Programmatically access
- Etc.

DLP policies are your best tool to avoid IP theft



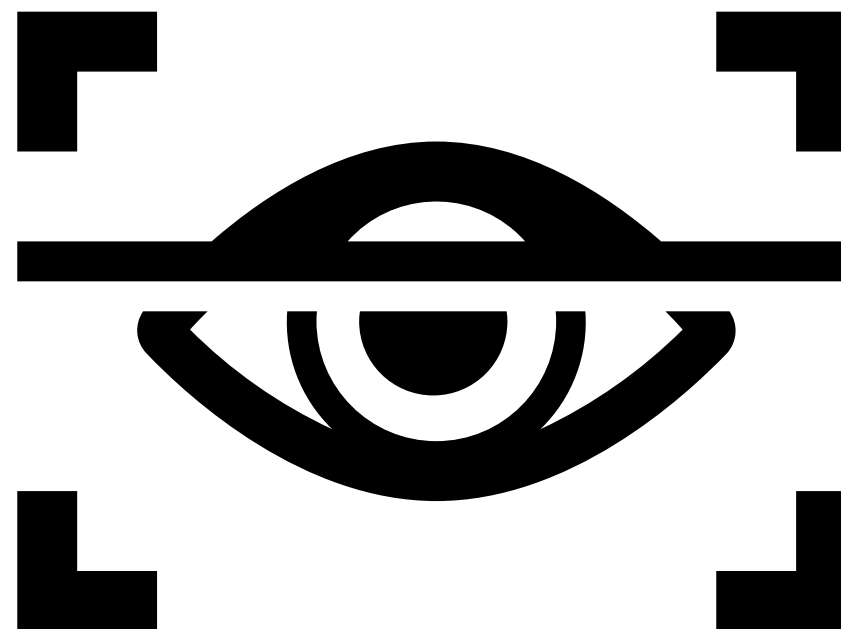


Multi-Factor Authentication

And the #1 most important thing you can enable today to protect your startup is Multi-factor Authentication (MFA.) This will ensure that if an attacker gets the username and password of a user that they won't be able to get in as the system will prompt for an additional factor.

In order of effectiveness, the factors can include:

- SMS Text
- Biometrics
- Authenticator Apps (MS, Google)
- Hardware keys





What Microsoft IT Tools Can Help Improve Security?

EXAMINING MICROSOFT CLOUD SECURITY OPTIONS

Microsoft Security in Relation to the NIST Cyber Security Framework



Identify

- Azure Active Directory
- Microsoft Intune
- SCCM
- Microsoft Defender for EndPoint



Protect

- Azure MFA
- Azure AD Privileged Identity Management
- Microsoft Identity Manager / Privileged Access Management
- Azure Information Protection
- Azure AD Password Protection



Detect

- Azure Sentinel
- Microsoft Cloud App Security
- Microsoft Defender for Endpoint
- MDI
- Azure Security Center
- Azure AD Identity Protection



Respond

- Azure Sentinel
- Microsoft Defender for Identity (Azure ATP)



Recover

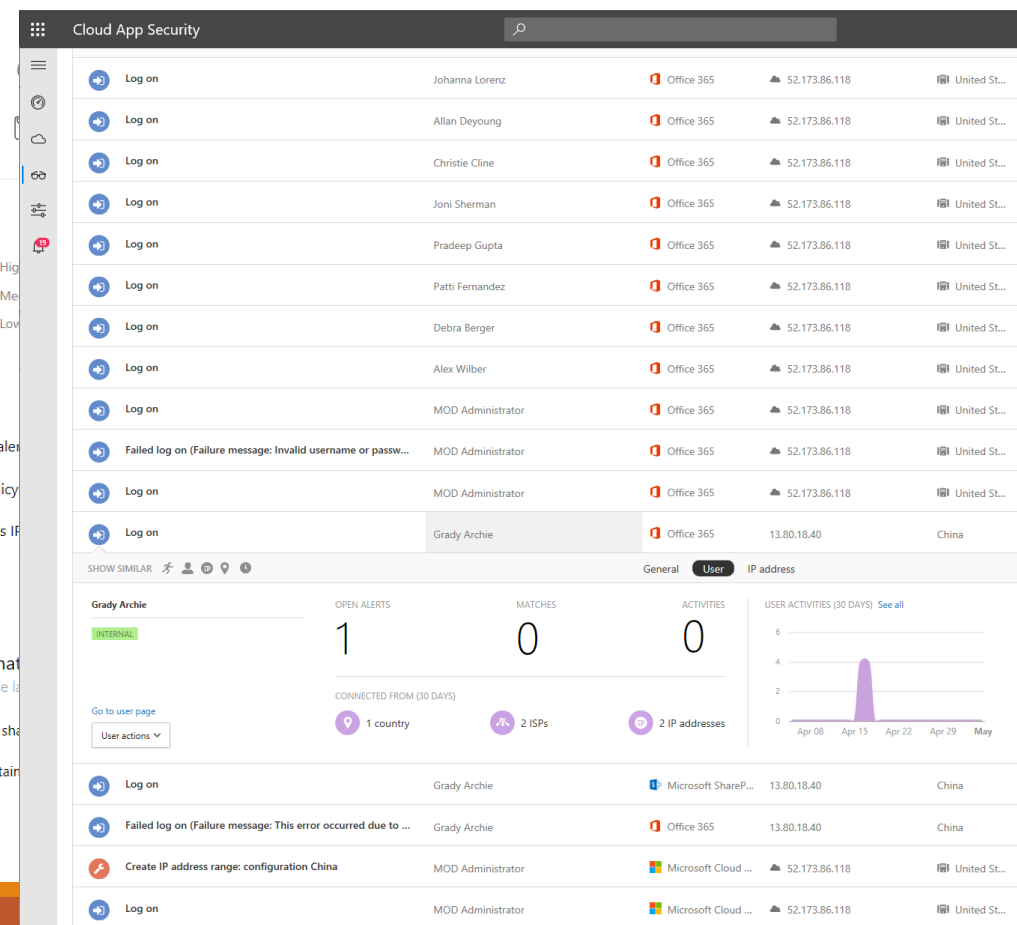
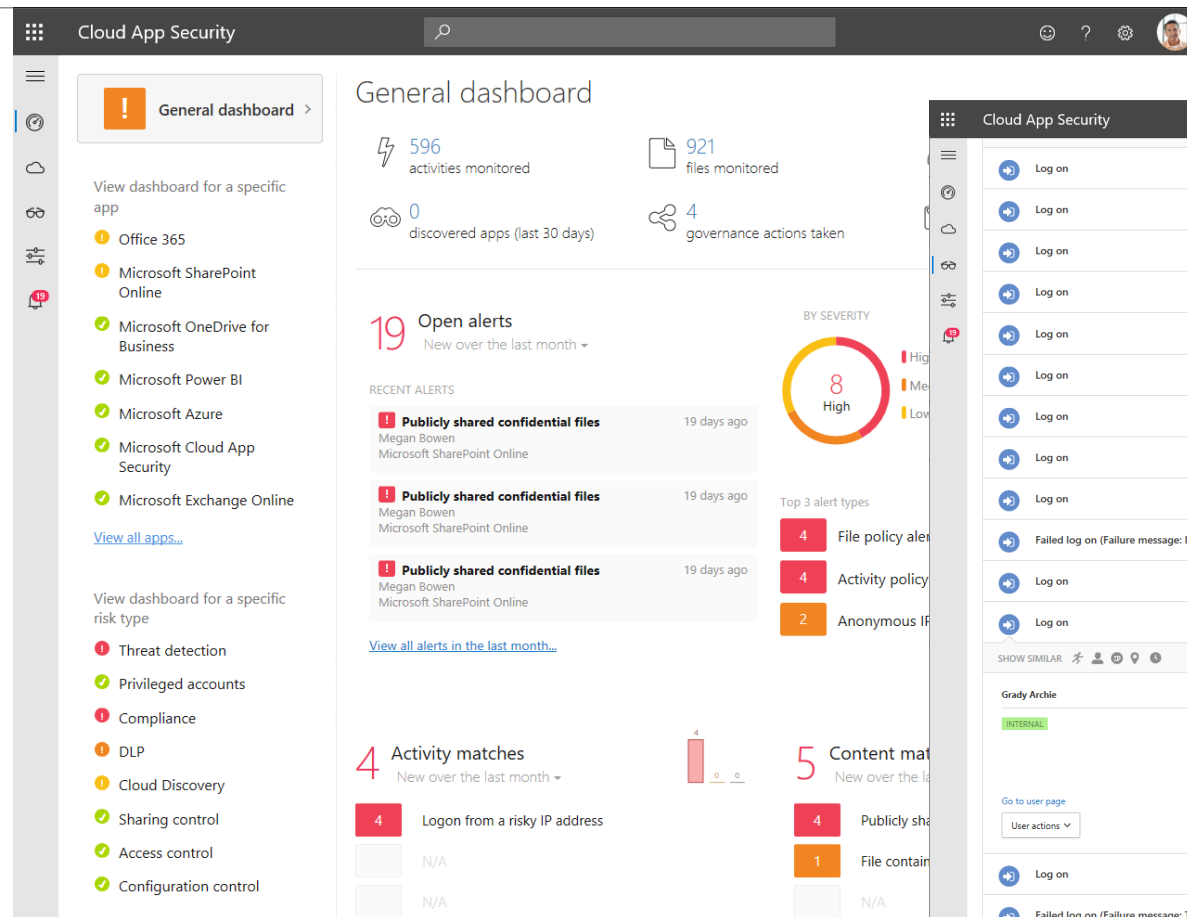
- Azure Security Center
- Azure Backup



Microsoft Cloud App Security

MCAS is a multimode Cloud Access Security Broker (CASB)

Proactively identifies threats across and in between cloud platforms





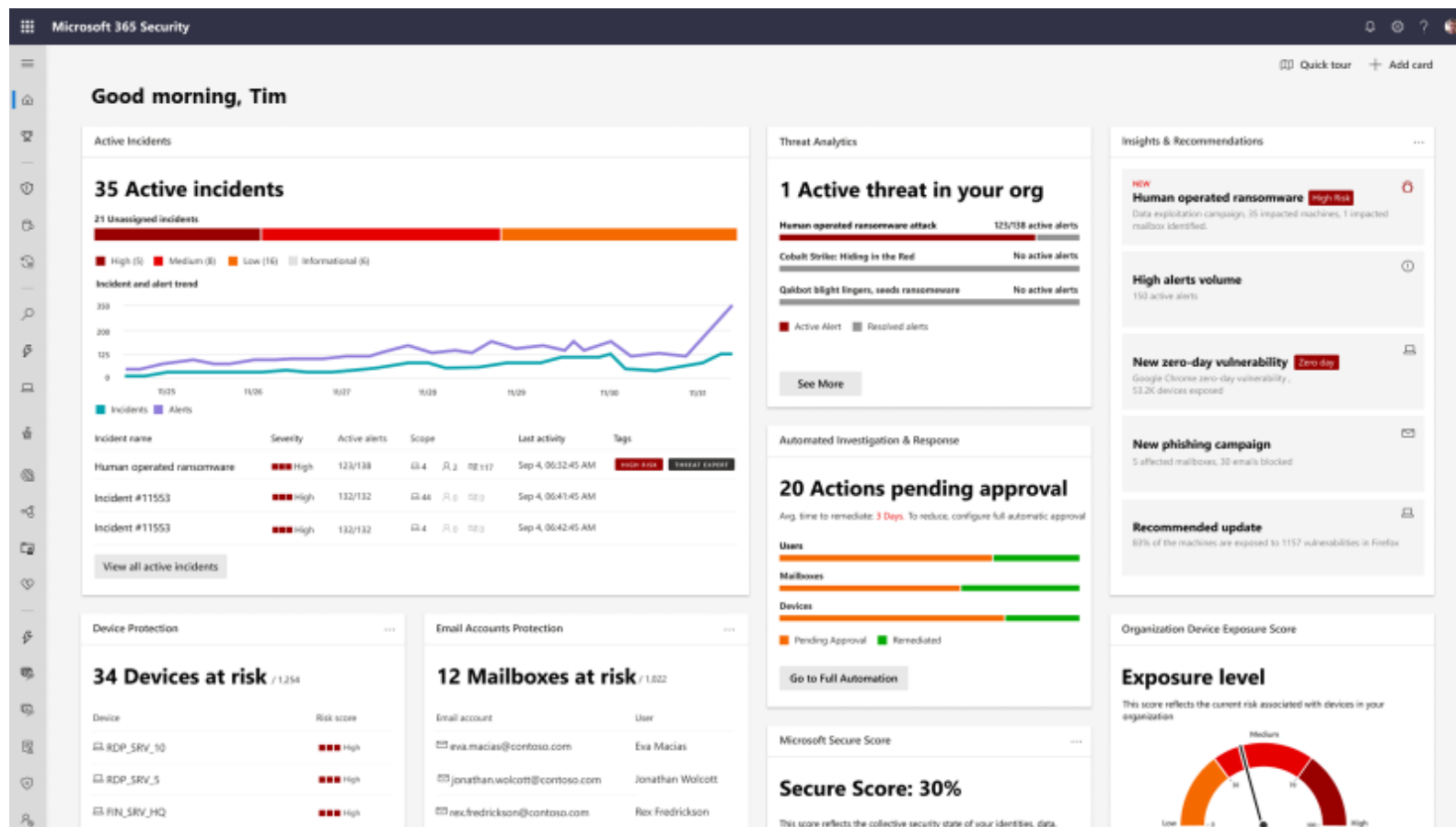
Microsoft 365 Defender

Microsoft 365 Defender
(previously Microsoft Threat Protection).

Microsoft Defender for Endpoint (previously Microsoft Defender Advanced Threat Protection).

Microsoft Defender for Office 365 (previously Office 365 Advanced Threat Protection).

Microsoft Defender for Identity (previously Azure Advanced Threat Protection).



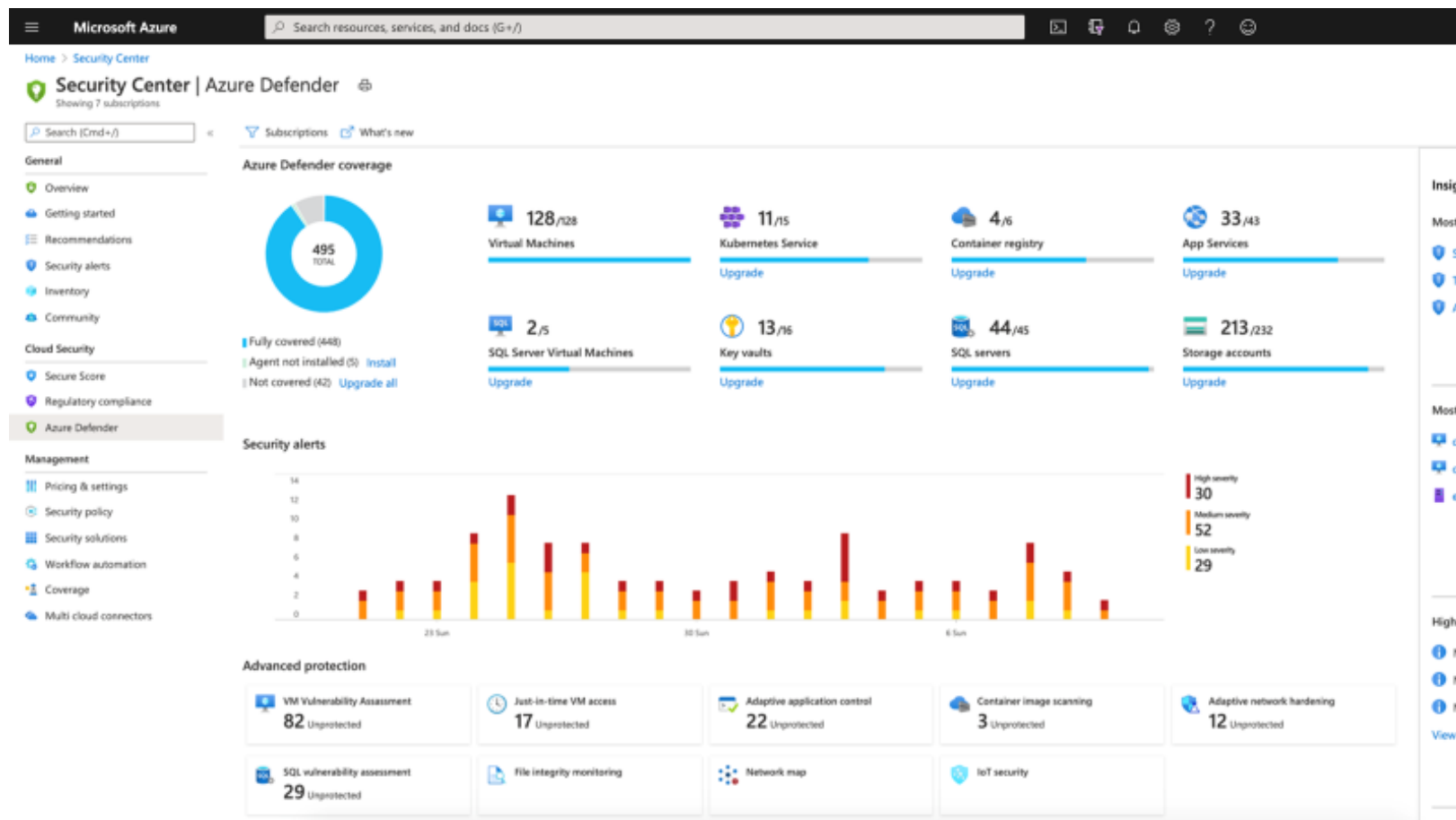


Azure Defender

Azure Defender for Servers (previously Azure Security Center Standard Edition).

Azure Defender for IoT (previously Azure Security Center for IoT).

Azure Defender for SQL (previously Advanced Threat Protection for SQL).



Microsoft Defender for Identity (MDI)

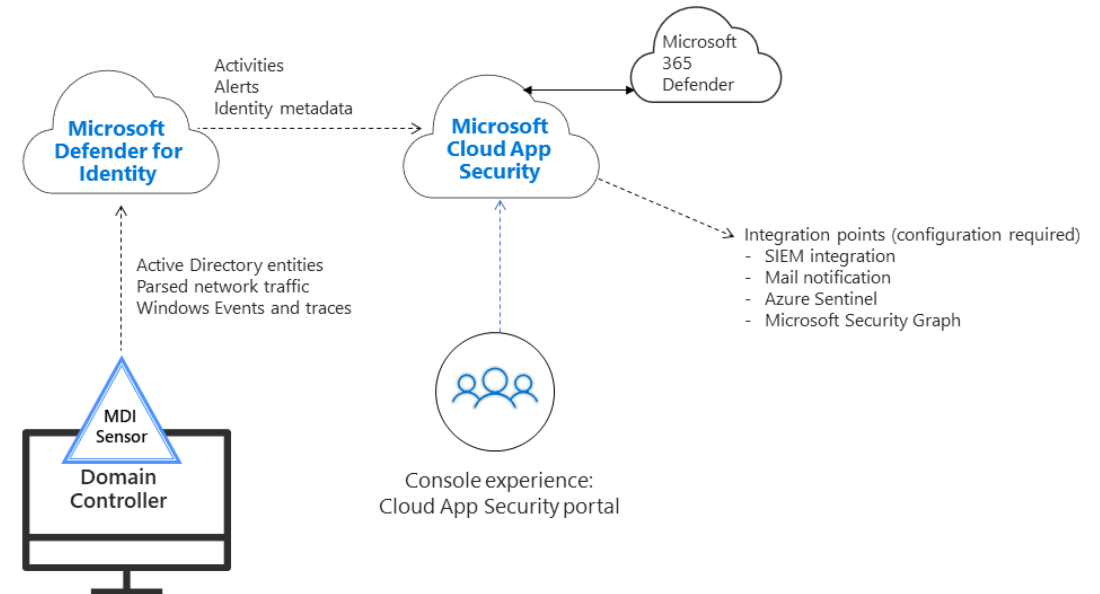


MDI deploys sensors to domain controllers to look for behaviors associated with compromised internal systems

MDI Sensors perform their calculation locally and then forward their alerts to the cloud

MDI Integrates with MCAS to provide single console experience for hybrid events (On-Prem with MDI and Online with MCAS)

Microsoft Defender for Identity Architecture



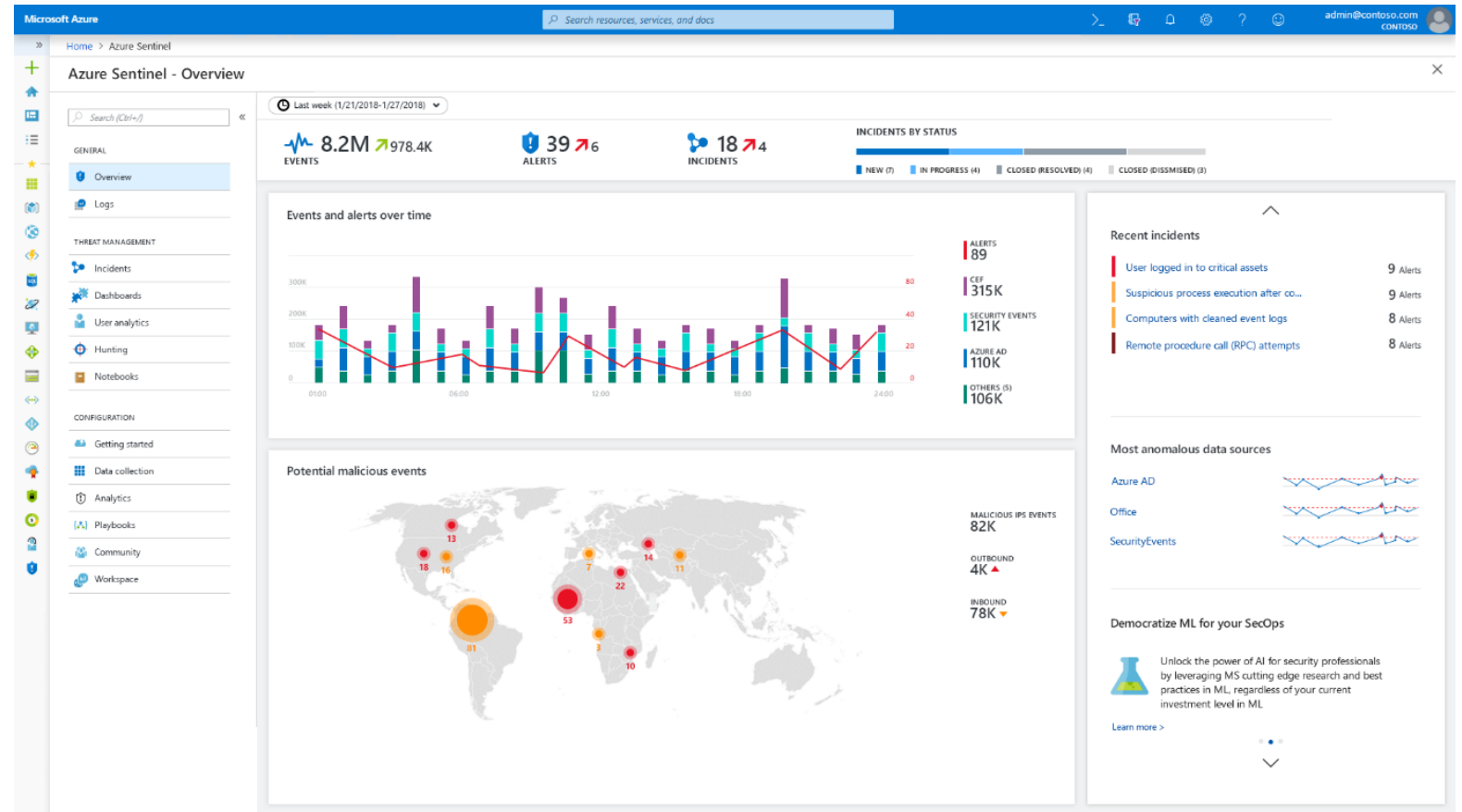
Azure Sentinel



Security Information & Event Management (SIEM) Platform built on Azure Monitor

Azure Sentinel provides for centralized SIEM capabilities for logs, alerting and providing for reporting trends

Firewall, switch, Windows, and Linux logs can all be forwarded to Sentinel to allow for retroactive forensics or real-time alerts

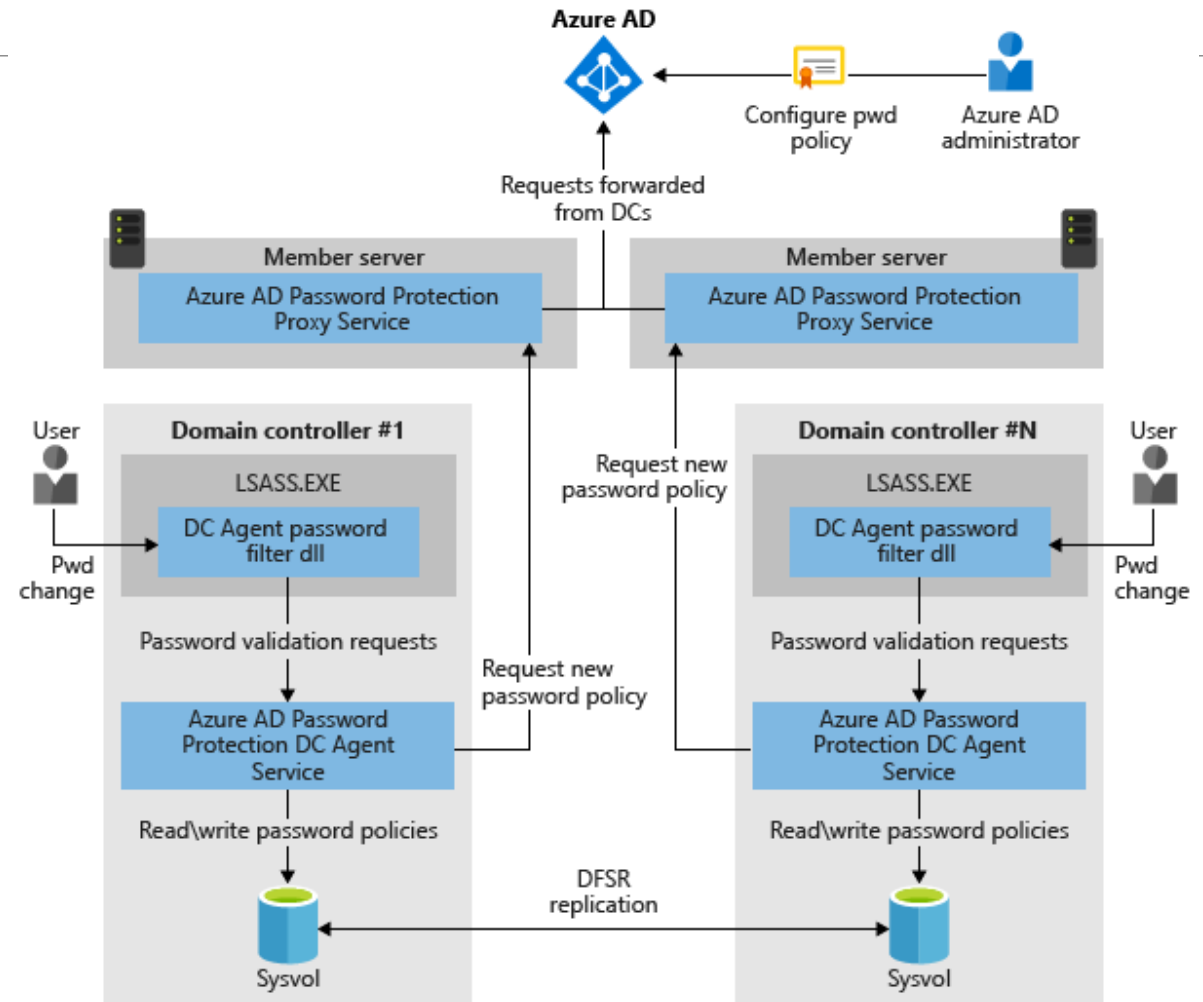


Azure AD Password Protection



Azure AD Password Protection runs as agents on all internal domain controllers that restrict how a password is constructed.

Azure AD Password Protection allows for complexity beyond the default options in an AD environment, disallowing passwords that are known to be compromised and/or include key words





Azure AD Entitlement Management

A component of Azure AD Identity Governance, Azure AD Entitlement Management is a compliance and auditing control platform that allows organizations the ability to better control access to Azure resources

Administrators can create 'access packages' to control what type of rights will be granted, which approvers can grant those rights, and when they expire.

Users who can request access
☒ For users in your directory
☐ For users not in your directory
A guest user will be created in your directory when the external user is assigned access to the access package.
[Learn more.](#)
☐ None (administrator direct assignments only)

Select users and groups
Employees
[+ Add users and groups](#)

Request
Require approval ☒ ☐

Yes No

Select approvers
Chris Green
[+ Add approvers](#)

[Show advanced request settings](#)

Expiration
Access package expires ☒ ☐ ☐
Access expires after 30 ☐
[Show advanced expiration settings](#)

Azure AD Privileged Identity Management (PIM)







A separate component of Azure AD Identity Governance, Azure AD Privileged Identity Management (PIM) allows accounts to be 'privileged by request' and not by default.

Users can initiate requests to raise their privileged roles, and these requests can be moderated by admins and/or monitored.

In the event of a compromise, admin users will have no special rights until they have been elevated, which greatly reduces exposure.

A screenshot of the 'Global Administrator' management console. The interface has a dark header with the title 'Global Administrator' and standard window controls. Below the header is a toolbar with icons for '+ Add', 'Filter', 'Refresh', 'Group', 'Review', 'Export', and 'Settings'. A search bar is located below the toolbar. The main content area displays a table of users with the following columns: 'USER', 'PERMISSION', and 'EXPIRATION'. The table is filtered to show 'GLOBAL ADMINISTRATOR' roles. It lists four users: Jennifer Davey (Permanent), Lee Sperry (Eligible), Jack Smith (Eligible), and Admin (Permanent). Each user entry includes a profile icon, the user's name, and their email address.

USER	PERMISSION	EXPIRATION
GLOBAL ADMINISTRATOR		
 Jennifer Davey jenniferdavey@contoso.com	Permanent	-
 Lee Sperry leesperry@contoso.com	Eligible	-
 Jack Smith jacksmith@contoso.com	Eligible	-
 Admin admin@contoso.com	Permanent	-

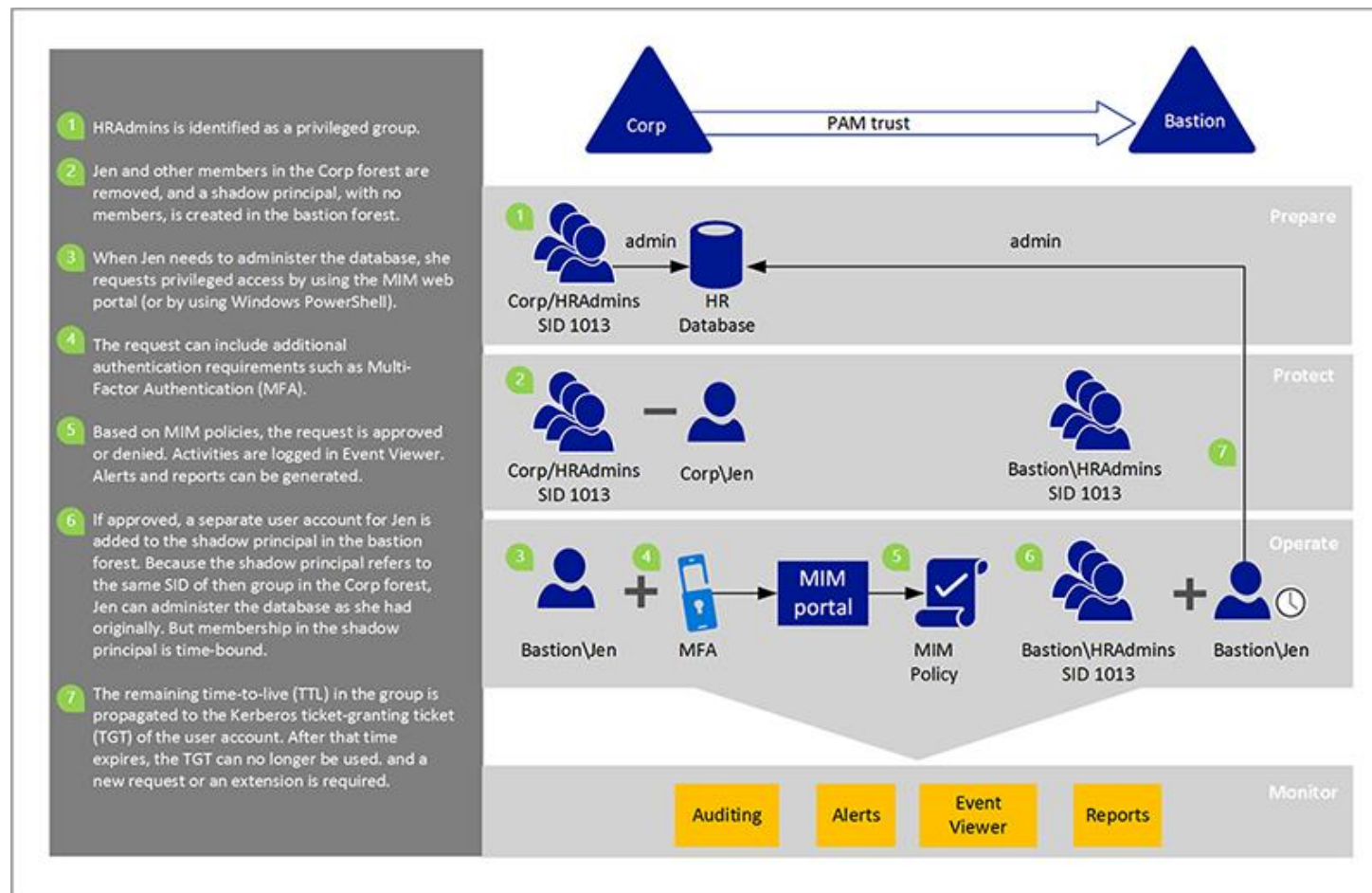


Microsoft Identity Manager / PAM

The On-Prem version of PIM is integrated into the Microsoft Identity Manager (MIM) suite in the form of Privileged Access Management (PAM.)

PAM works similarly to PIM, with the exception being that a Bastion forest is used for accounts with elevated privileges.

A Bastion forest exists across a one-way trust and accounts are only elevated as needed. This leaves membership in privileged groups such as 'Domain Admins' to very few active accounts.





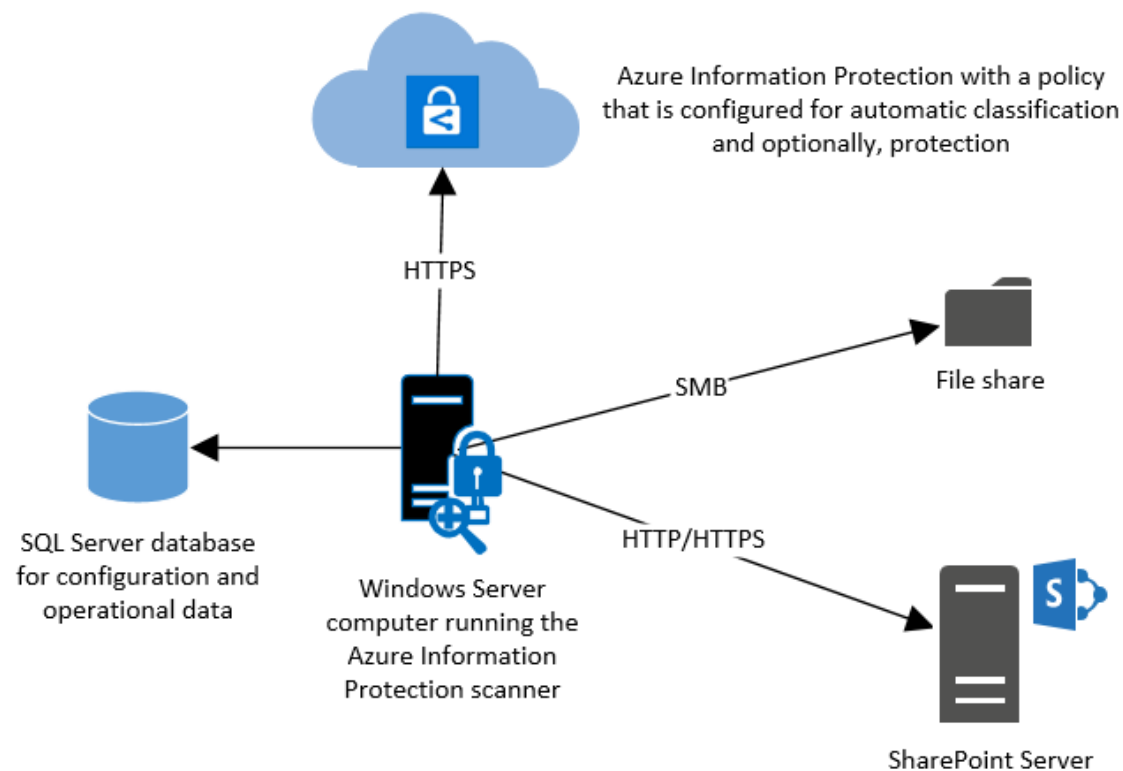
Azure Information Protection

Azure Information Protection provides for the ability to control what happens to data AFTER it has been accessed.

Azure IP assigns Information Protection tags to content either manually or via automatic processes.

The existing Azure Rights Management Services (Azure RMS) service is now integrated into Azure RMS.

Hold Your Own Key (HYOK) allows organizations to secure and encrypt content using their own private key, removing Microsoft from data custody.





Demo

[illegible]



Thank you! Questions?



Michael Noel



CCO.com



@MichaelTNoel



Linkedin.com/in/michaeltnoel



SharingTheGlobe.com



Slideshare.net/michaeltnoel