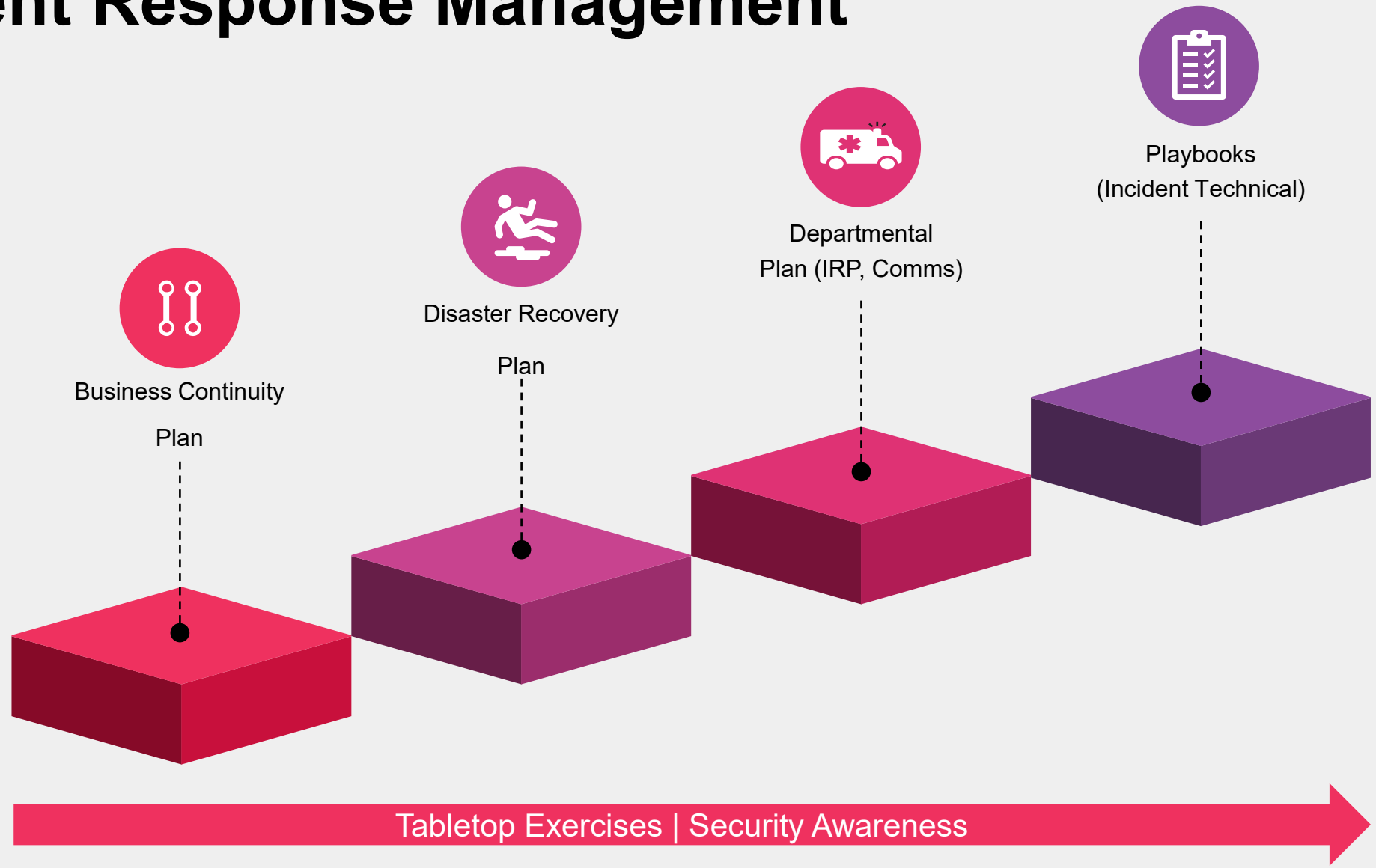
PART - 1

Building a High Impact IR Plan

VIPSS - 2026

Maleena Singh
Director, Incident Response and Resilience

Incident Response Management

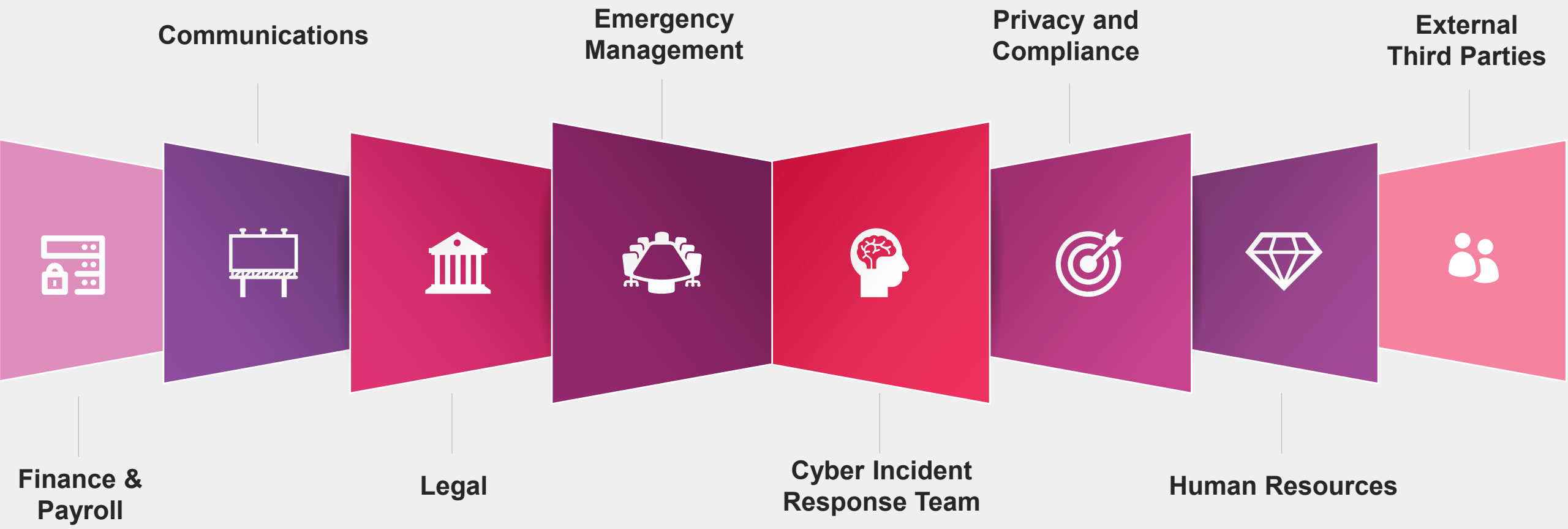


Incident Response Plan

MIRAI

www.miraisecurity.com

Cyber IR isn't just a technical problem



Key Considerations

Accurate & Actionable

Not just nice to haves

Contact List

Don't Bury it – **Bold It!**

Backups

Not those kind….

Activation Plan

What's the actual plan?

Ownership

Who's on First?

Escalation

Who knows what and when?

A Few More Considerations

Enterprise Level
This is for all cyber incidents

Not just the Techies
Include all stakeholders needed – Legal, Comms, Finance

Go with the Flow
The plan should align with all other crisis plans. Reference and link where necessary

Don’t forget about your Supply Chain
What if they are a victim, what if you are?

Limited Technical Speak
Make sure anyone could pick up this plan and read it

Phone a Friend?
Ensure your third parties are identified and listed

Include Ownership and Authority
Who will contact whom? Who needs to have approval?

Post Incident
An important part of the incident lifecycle.

External Parties & Support

Cyber Breach Coach

Incident Response Retainers

External Legal Counsel

Cyber Insurance

Managed Service Provider

Enterprise Considerations

Cyber Insurance

- When and how involved are they?
- Pre-Approved Vendors
- What do they really cover?
- Clear the details of the plan

Legal

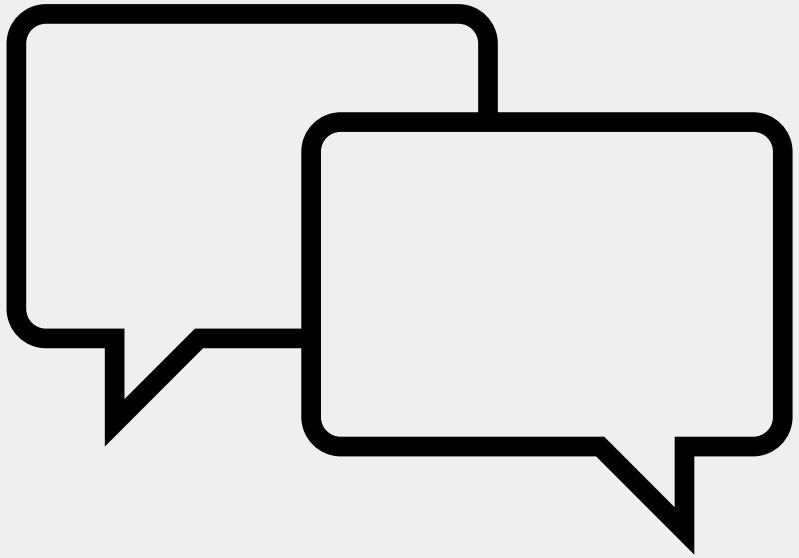
- Do you have contracts with your retainer companies?
- Are they aware of each others' terms?
- Importance of Legal Privilege?
- Boundaries of internal and external counsel

Communications

- Holding statements for the first 48 hours
- Cadence of updates, tone of notifications
- Considerations: Internal / External / Critical Vendors / Third Party (Supply Chain)

The Role of the Board - Engagement must be defined *before* an incident occurs

- Greater emphasis on Board involvement
- Clear Communications at the right levels
- Understanding Approval Authority
- Regulatory & Governance Pressure
- Heavy penalties for late or unclear disclosures



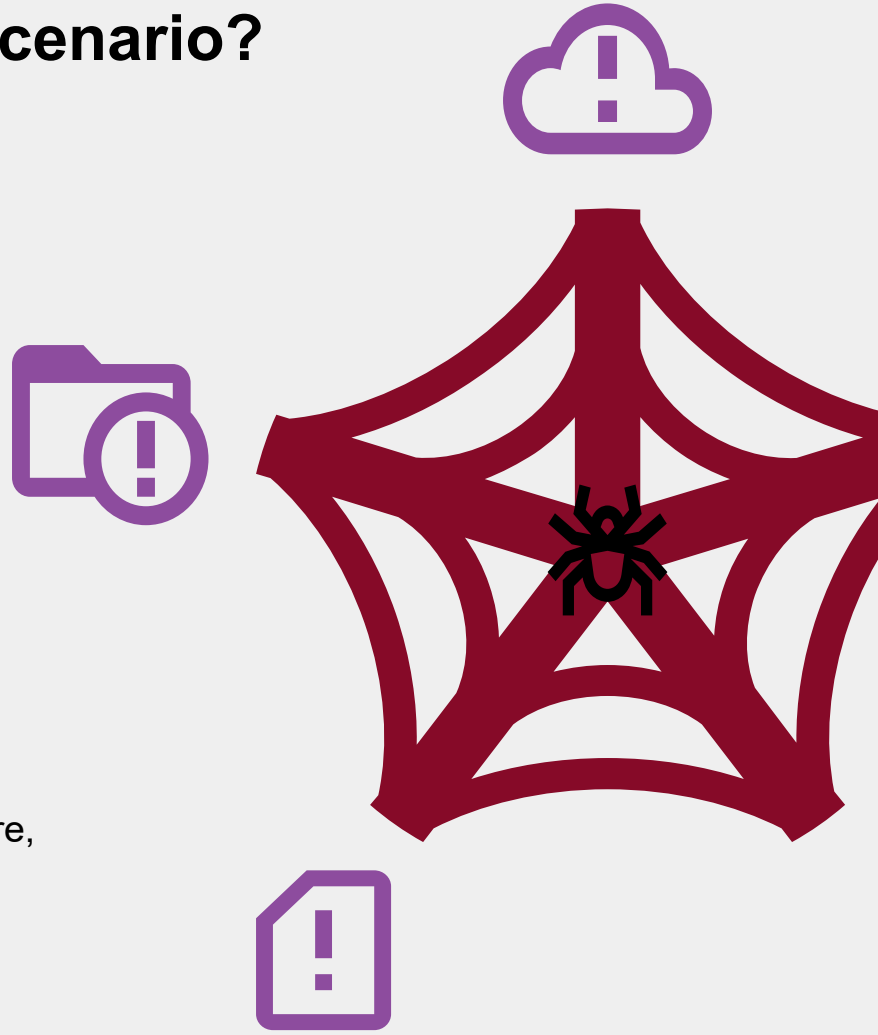
What can you do?

- Pre-Define Escalation & Approval Authority
- Establish a Structured Communication Protocol
- Integrate Cyber into Enterprise Risk Governance
- Conduct Board-Level Tabletop Exercises
- Formalize Documentation & Evidence of Oversight

Ransomware

How does org resources handle a Ransomware scenario?

- Who do you inform?
  - Board Authorization?
  - Authorities? Government?
- Do you respond to the demand?
  - If so, How? Who?
- How do you prioritize the decisions factors for paying?
- Do you negotiate?
- Do you pay?
  - Who do you inform of the payment decision?
  - What are the consequences of not paying?
- Who owns the decision (& risk) of ransomware?



Key Takeaways

- Develop and implement procedures and guidelines for addressing ransomware, encompassing impact and financial thresholds, and designated authoritative oversight

PART - 2

M365 Security & Investigation Basics

VIPSS - 2026

Sonik Surelia
Senior Technical Lead, Incident Response and Resilience

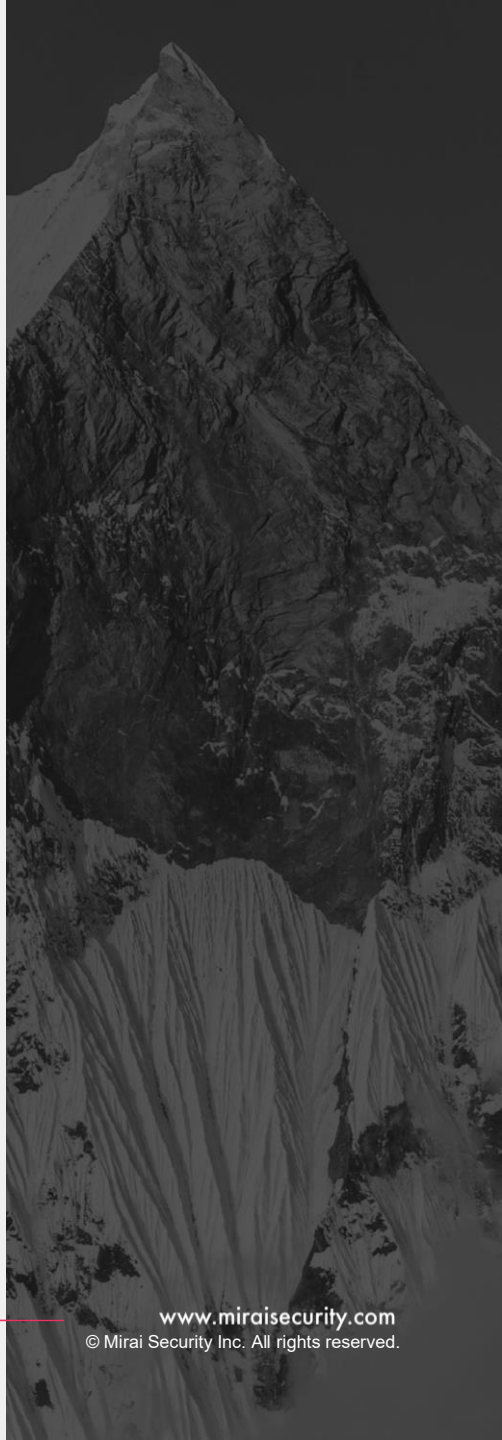
www.miraisecurity.com

Current State of M365

Your business runs on M365. So do the attackers.

- Microsoft 365: One of the most targeted cloud platform by attackers. Not because it's weak, but because mostly every business is on it.
- Email, files, identity, finance approvals, HR records all under one roof.

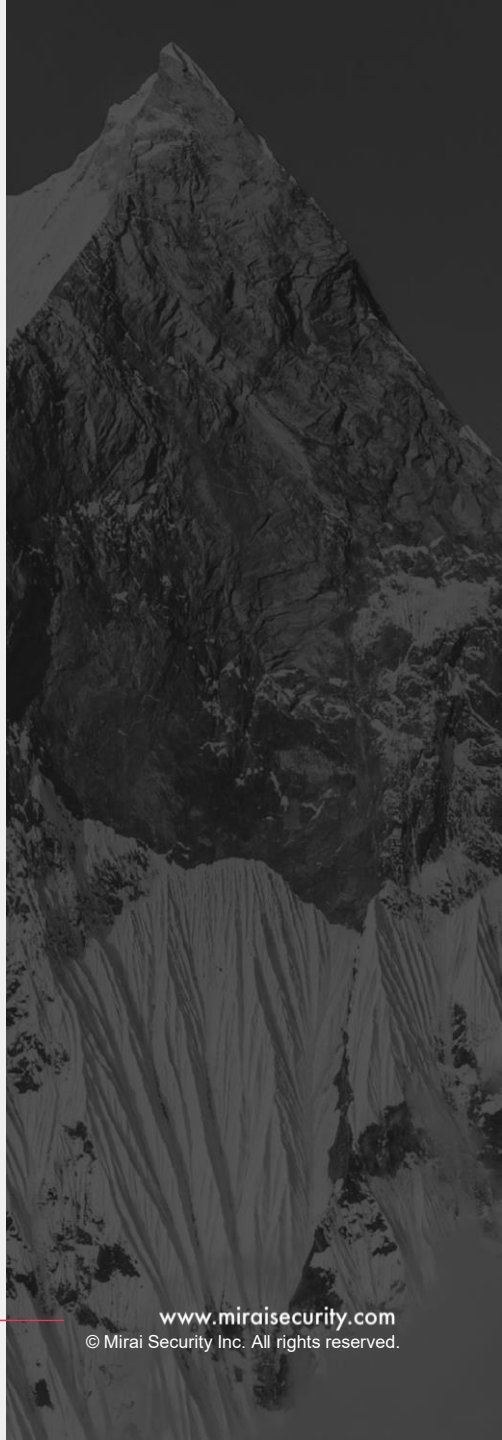
The Business Reality	The Attacker Reality
450M+ commercial M365 seats globally (1)	Email is the #1 attack vector (4). Phishing, BEC, credential theft which makes M365 a primary target
BEC losses: $2.77B across 21,442 complaints in 2024 (2)	Attackers don't break in they log in using stolen credentials
Average breach detection & containment: 241 days (3)	By then, email has been read, files exfiltrated, rules set
Regulatory consequences: PIPEDA, HIPAA, SOC 2 reporting obligations	One undetected compromise = data breach notification + legal exposure



Most common M365 Incident types

Incidents	What it looks like
Phishing / Malware Delivery	Email delivers malicious link or attachment > user clicks > Credential or endpoint compromise follows.
Account Takeover	Attacker logs in with stolen credentials, often from a foreign IP.
Business Email Compromise	Attacker reads email, sets forwarding rules, impersonates exec for wire transfer.
OAuth App Abuse	Attacker tricks user into consenting to a malicious app and maintains access without a password.
Data Exfiltration	Mass file download, anonymous sharing links, email forwarding to external addresses.

⚠ **Every phase above depends on logs.**
No logs = no timeline. No timeline = no scope. No scope = no case.



MIRAI

Why Protection Controls Matter?

Protection controls are your first line the mechanisms that stop an attacker before they get in.

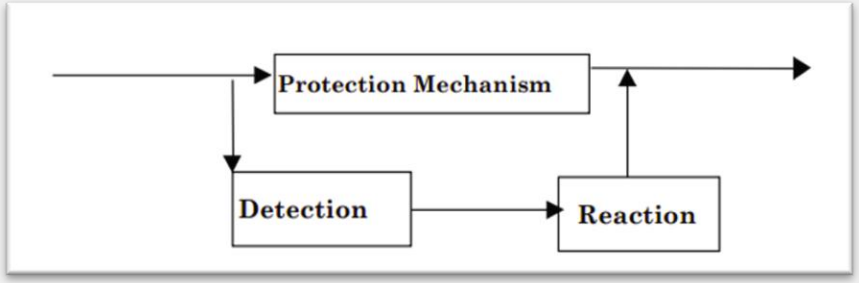
For example:

Control	What It Does	Why It Matters
Multi-Factor Authentication (MFA)	Requires a second verification factor beyond password	Reduces account compromise risk by 99.22% (5)
Conditional Access	Enforces who can sign in, from where, on what device, under what conditions	Zero Trust at the identity layer. The policy engine of modern security
Safe Links / Safe Attachments	Scans URLs and files in email at time-of-click	Stops phishing payloads that bypass traditional filters
Intune / Device Compliance	Ensures only managed, healthy devices can access corporate data	Prevents compromised personal devices from becoming entry points
Data Loss Prevention (DLP)	Detects and blocks sensitive data leaving the organization	Reduces exfiltration risk even if an attacker is already inside

What happens when protection fails?

Security is a race. The question is who wins it.

- The **Time-Based Security (TBS)** (6) model, introduced by security researcher **Winn Schwartau**, frames security as a measurable relationship:



$$Protection\ Time\ (Pt) > Detection\ Time\ (Dt) + Response\ Time\ (Rt)$$

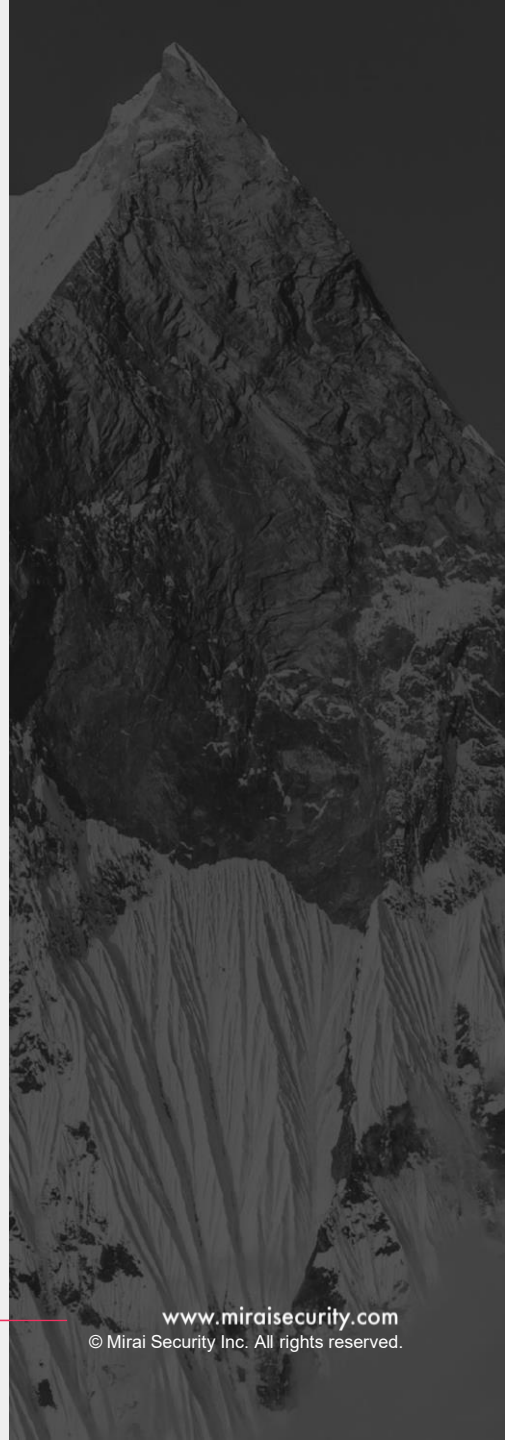
- Your protection must hold long enough for you to detect the breach and respond before damage is done.

$$Protection\ Time\ (Pt) < Detection\ Time\ (Dt) + Response\ Time\ (Rt)$$

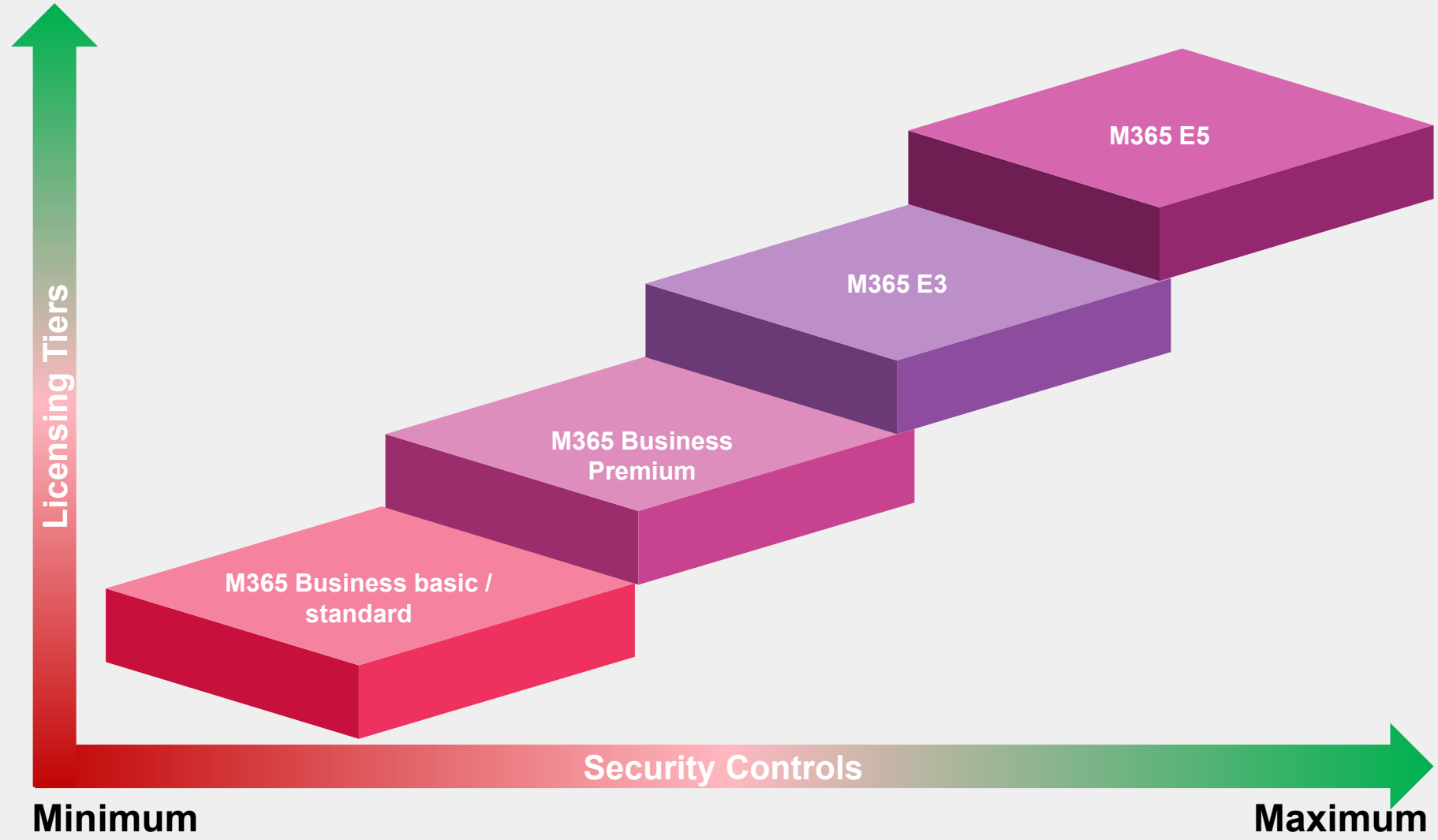
- If the protection doesn't hold long enough to detect the breach and respond. **You are compromised.**

What logs are available in M365

Log Source	Area	What It Contributes
Entra Sign-In Logs	Identity	Who authenticated, from where, how, whether MFA fired
Entra ID Protection	Identity Risk signals	Risky users, risk detections, leaked credentials
Unified Audit Log	M365 Activity	Mailbox rules, file access, admin changes, Teams activity, Items accessed.
Defender for Endpoint	Device telemetry	Process execution, file changes, network connections.
Defender for Office 365	Email	Mail delivery events, URL clicks, malware verdicts, Spam/Phishing detections.
Defender for Cloud Apps	SaaS behavior	Anomalies, OAuth app consent, shadow IT
Microsoft Graph Activity Logs	API Activity	Programmatic enumeration and exfiltration via Graph.
Co-Pilot Activity Logs	AI Interaction	Copilot prompts, accessed resources, external URLs fetched

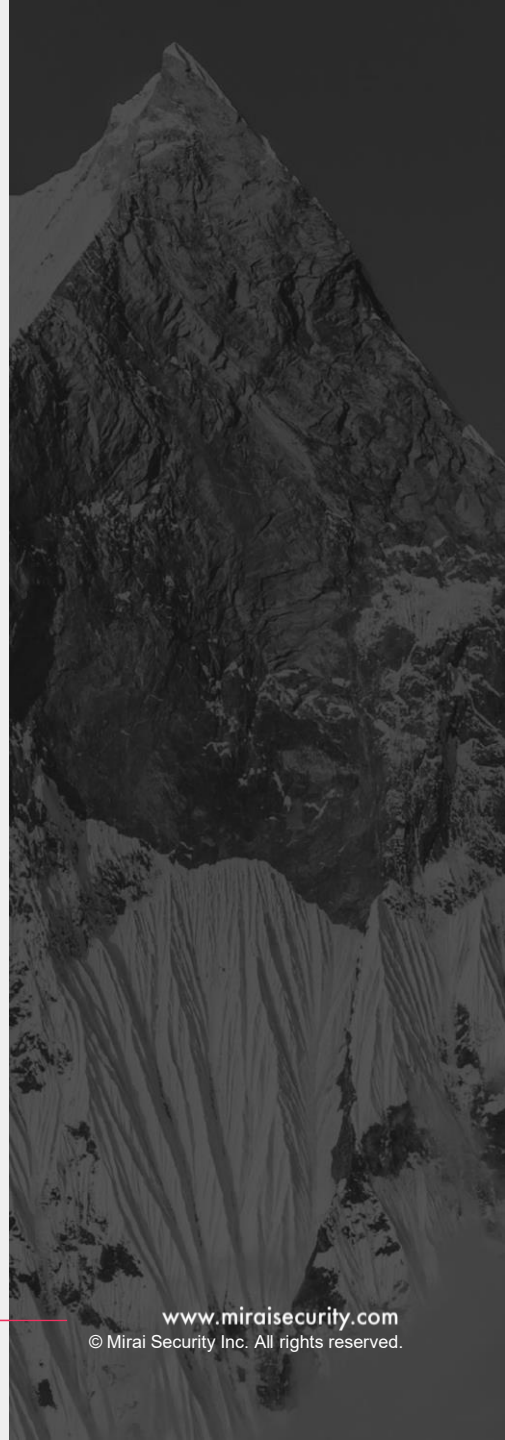


M365 License Structure vs Security Controls



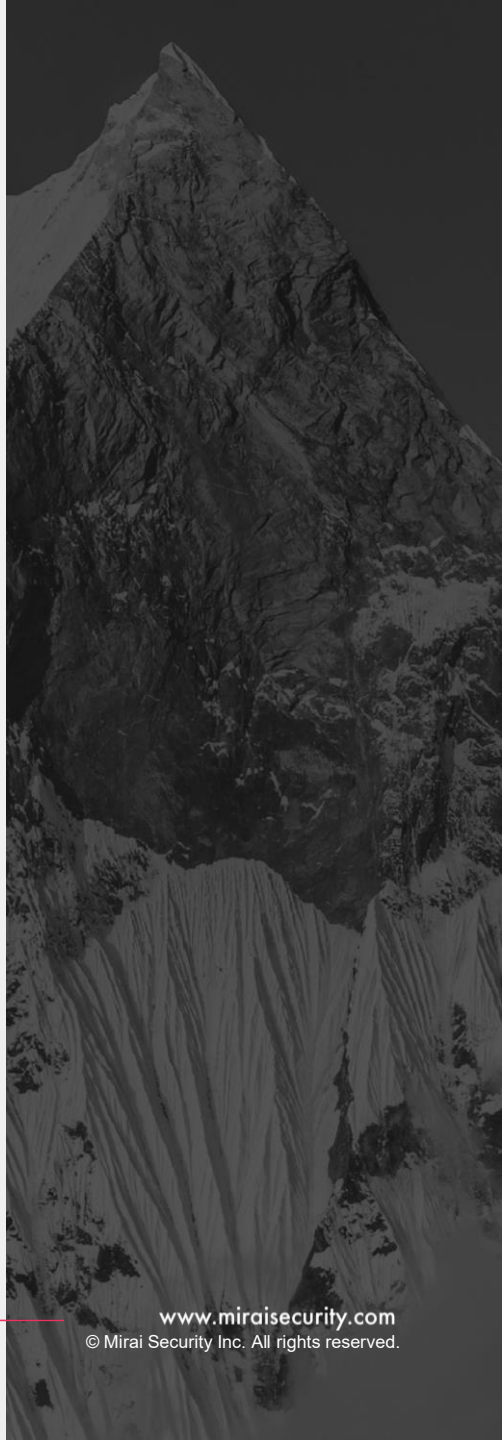
Entra ID Logs

What It Shows	Forensic Meaning
User sign-ins: IP address, location, device, browser	Establishes where the attacker authenticated from and when
MFA result: success, failure, bypassed	Reveals if MFA was defeated, bypassed, or never required
Conditional Access policy applied or blocked	Shows which security policies fired or which gaps were exploited
Failed sign-in error codes	Repeated failures followed by success = credential stuffing or brute force
Non-interactive sign-ins (app/token-based)	Where persistent access hides after the password is changed attacker may still hold a valid token
Service principal sign-ins (app-to-app)	Reveals rogue OAuth apps authenticating silently without user involvement
User Audit Logs	Recent changes to the user, Role Assignment, Role Activation, Password change, Group Assignments.



Microsoft Graph API Logs

What it Shows	Forensic Meaning
API Calls made to Microsoft Graph	What data was programmatically accessed or enumerated
Application and user identity behind each call	Was it a legitimate app or a rogue Oauth application
IP address and user agent of the caller	Attacker tooling fingerprint – GraphRunner, AzureHound
Resources requested via API	Which mailboxes, files, or directory objects were targeted
Volume and frequency of calls	Bulk enumeration pattern – Low and slow exfiltration
Failed or unauthorized API attempts	Attacker probing for accessible resources and permissions.



Entra ID Logs

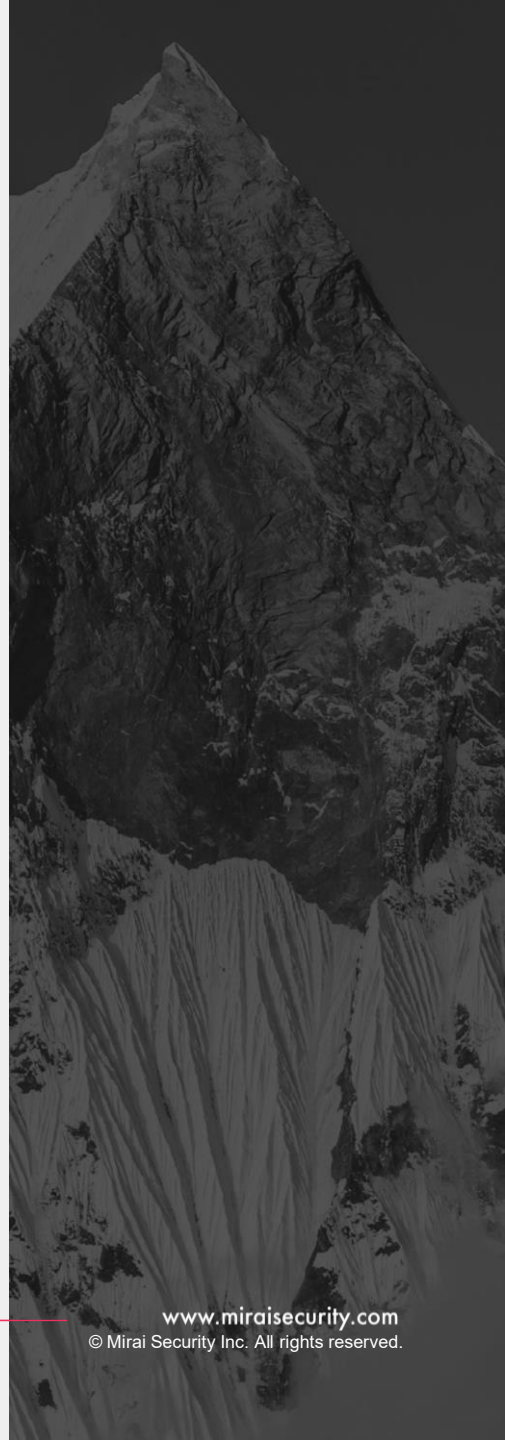
Every login attempt leaves a record. This is where you read it.
What it is:

- The identity layer log. Captures every authentication event against Microsoft Entra ID (formerly Azure AD) successful, failed, and blocked.

License	Interactive Sign-In Logs / Audit Logs / Custom Security Attributes	Non-Interactive & Service Principal Logs / Provision Logs / Health / Microsoft Graph API
Free / no P1 or P2	7 days only	Not available. Zero visibility
Entra ID P1 / P2 (Business Premium, E3, E5)	30 days	30 days
Exported to Sentinel / Log Analytics	Long-term. Defined by your retention policy	Long-term. Defined by your retention policy

Non-interactive and service principal sign-in logs require Entra P1/P2.

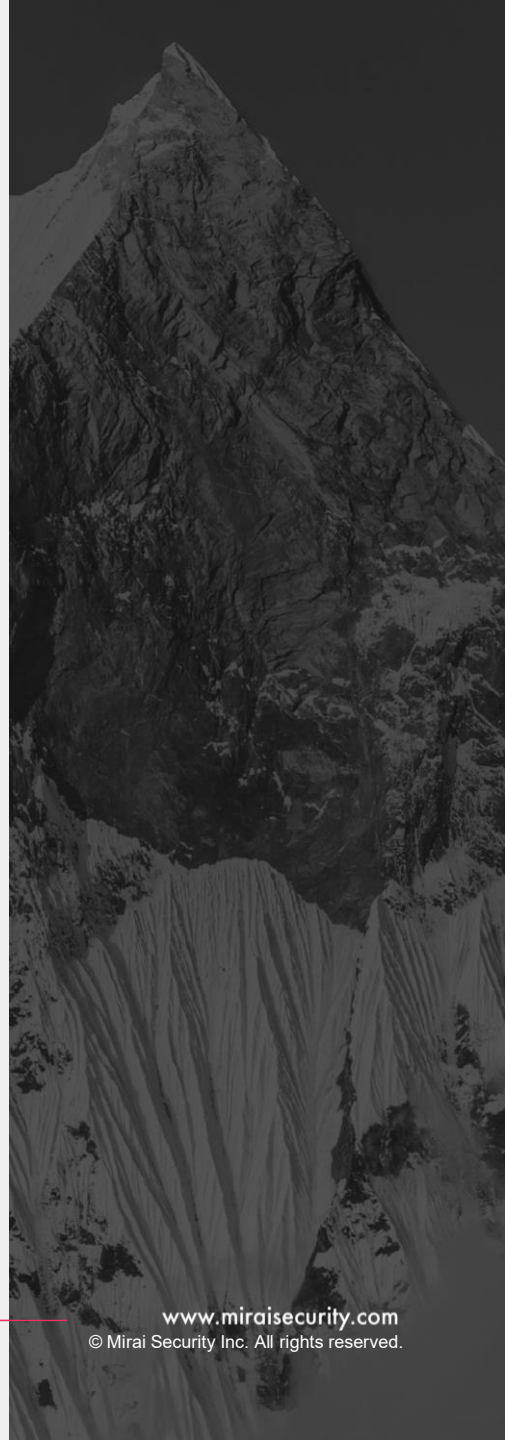
- Free tenants have zero visibility into these log types and not even 7 days. This is not a retention gap. It is a complete blind spot.
- Token-based persistence is how attackers maintain access after a password reset lives entirely in non-interactive logs. Free tenants cannot see it at all.



MIRAI

Unified Audit Logs

What It Shows	Forensic Meaning
Inbox rules created or modified	Classic BEC indicator. Attacker hides sent emails, forwards to external address
Mailbox permissions changed	Attacker granted themselves or an accomplice full access to another mailbox
Files accessed, downloaded, shared	Scope of data exfiltration, which files, when, by whom
Anonymous or external sharing links created	Data made accessible outside the organization without ongoing credential access
Admin role assignments	Privilege escalation attacker granted themselves admin to maintain control
Audit logging toggled off	Sophisticated attacker covering tracks this event itself is only logged if auditing was already enabled
MFA method registered	Attacker registered their own device to maintain MFA-authenticated access
MailItemsAccessed (E5 / Audit Premium only)	Proves exactly which emails were read not just that the mailbox was accessed
Copilot interactions: who, when, where, what was accessed	Confirms if Copilot was used as an attack channel and which external domains it contacted



Unified Audit Logs

Everything that happens inside M365, in one place.

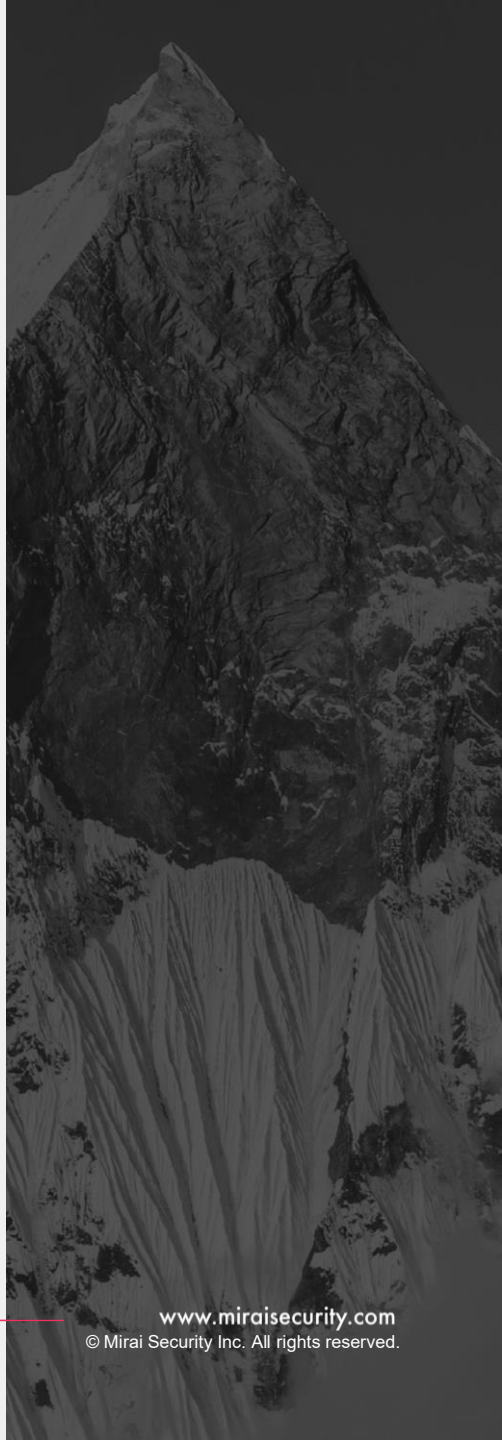
What it is:

- The master activity log for Microsoft 365. Captures user and admin operations across Exchange, SharePoint, OneDrive, Teams, Entra ID, and more in a single searchable record.

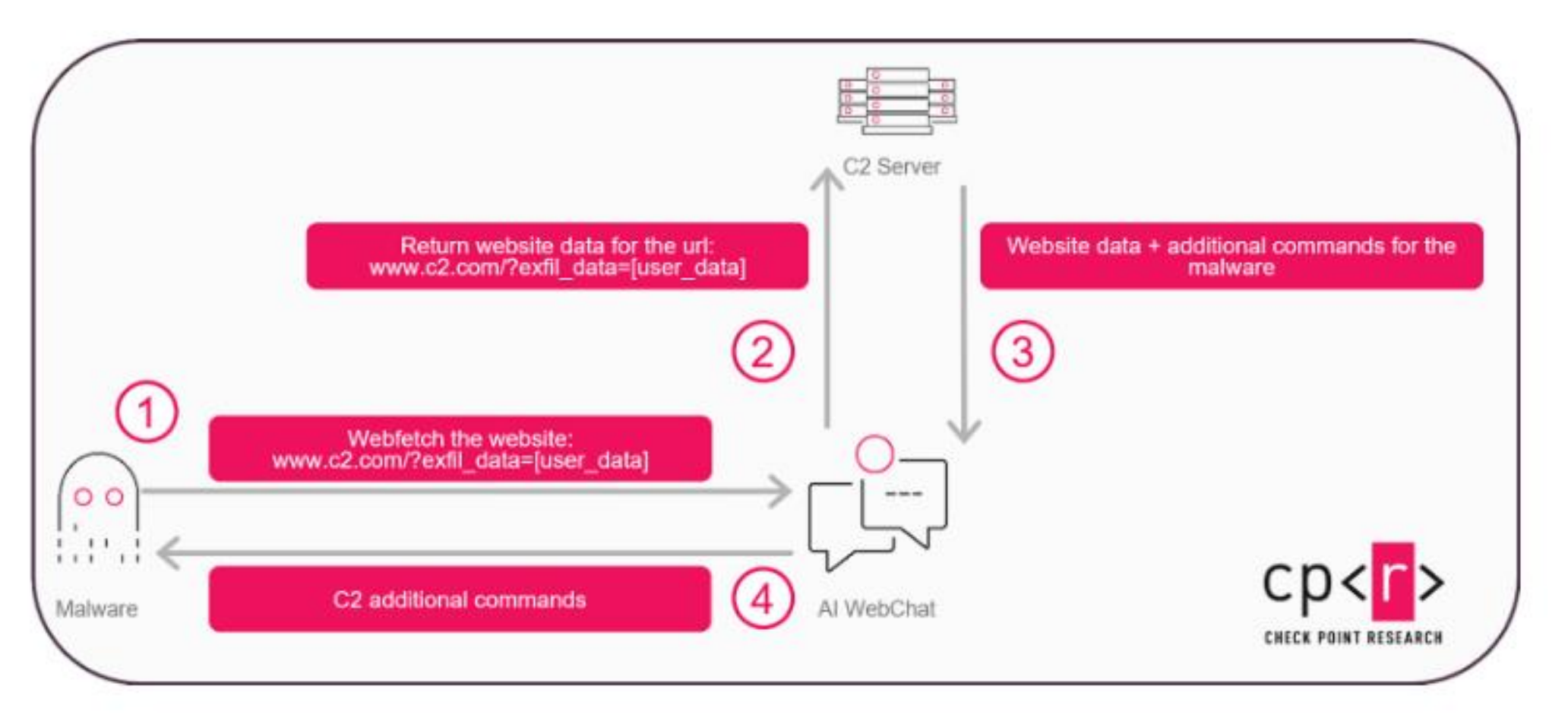
The BEC investigation gap:

- Without “MailItemsAccessed”, you can prove a mailbox was accessed but not which emails were read. Scope cannot be confirmed. That gap has direct implications for breach notification obligations under PIPEDA and HIPAA.

License	Default State	Retention	MailItemsAccessed
Business Basic / Standard / Premium	Off by default. Must be manually enabled	180 days when enabled	Not available
Business Premium + Purview Suite add-on	Off by default. Must be manually enabled	180 days when enabled	Not available
E3	On by default	180 days	Not available
E5 / Audit Premium	On by default	1 year standard	Available



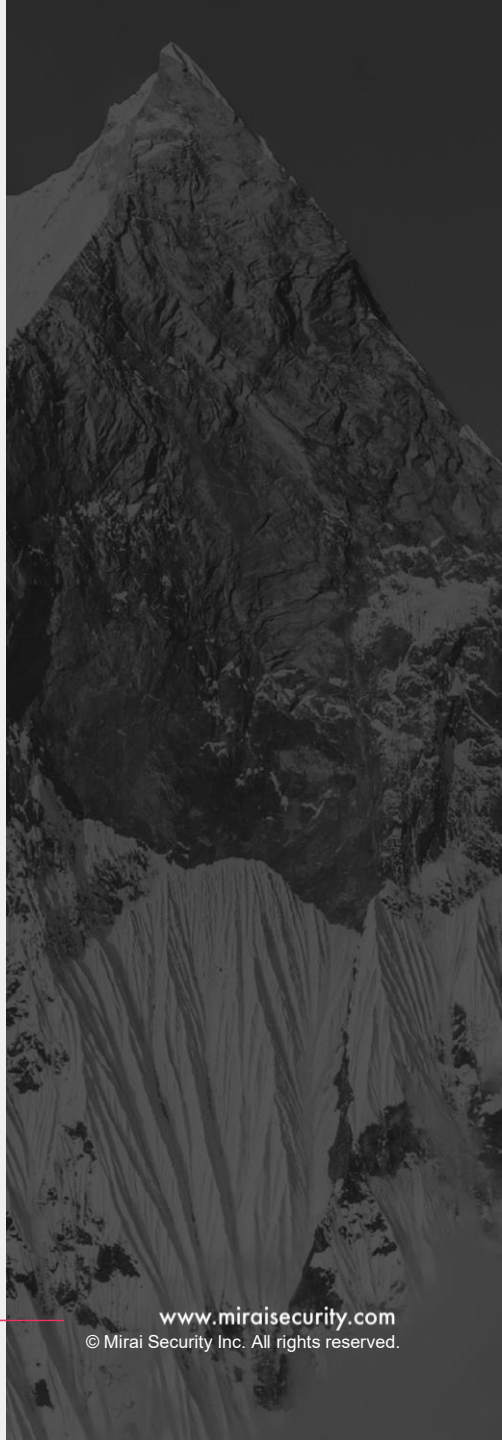
How attackers can leverage Co-pilot / AI as C2 proxies



Source: https://research.checkpoint.com/2026/ai-in-the-middle-turning-web-based-ai-services-into-c2-proxies-the-future-of-ai-driven-attacks/

Microsoft Defender for Endpoint

What It Shows	Forensic Meaning
Process creation and command execution	What ran on the machine. Malware, scripts, attacker tools
Network connections from endpoint	Outbound command-and-control communication, data exfiltration destinations
File creation, modification, deletion	Malware dropped, scripts written, evidence deleted
Lateral movement indicators	Pass-the-hash, remote service creation, admin share access
Security alerts (malware, suspicious behavior)	Defender's own detection the starting point of many investigations
Device health and compliance state	Was the device patched? Was it managed? Was EDR running?



Microsoft Defender for Endpoint

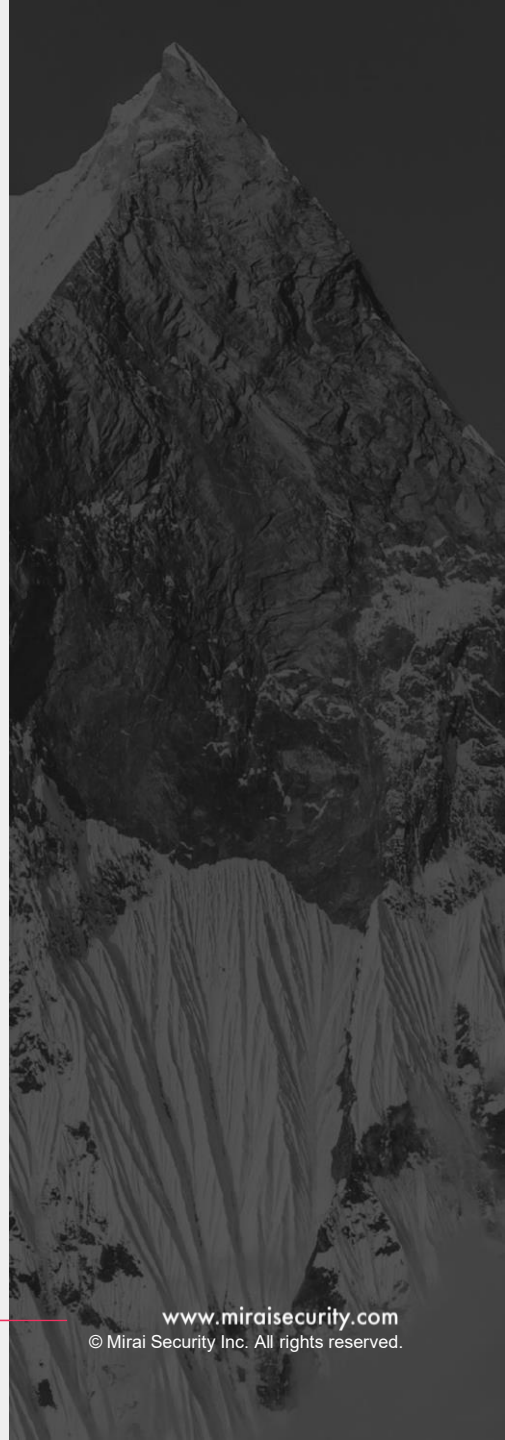
What happened on the device.. not just in the cloud.
What it is:

- Telemetry from managed endpoints (Windows, Mac, Linux, mobile) enrolled in Microsoft Defender for Endpoint. Captures process execution, network connections, file changes, and security alerts at the device level.

Without MDE P2, you have protection.. but limited forensic depth.

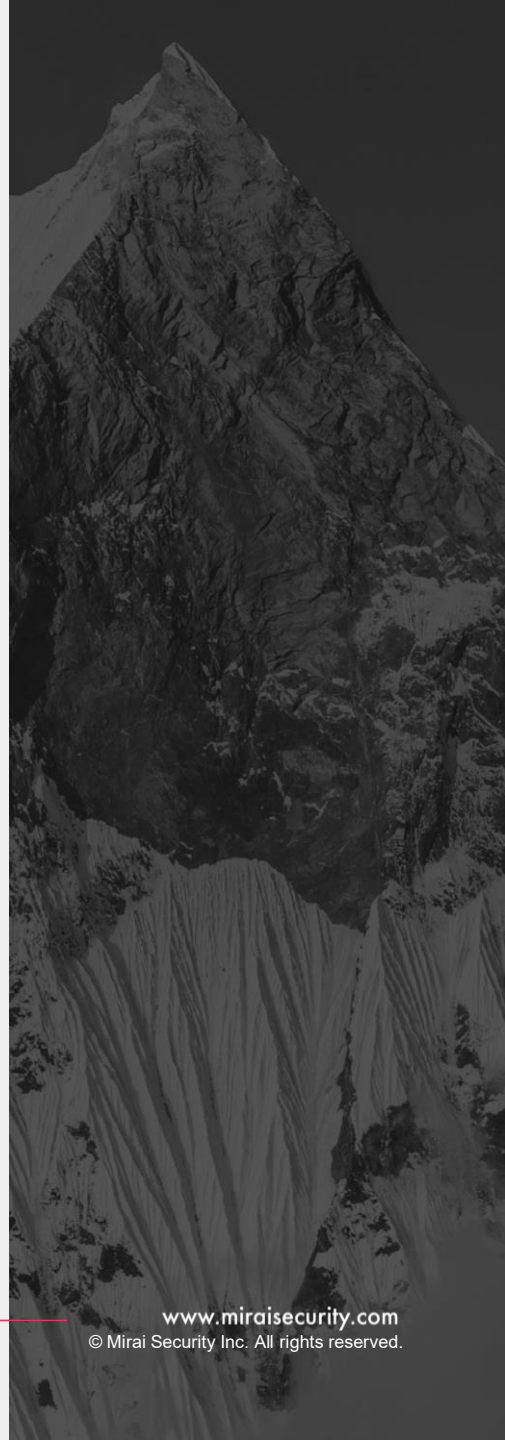
- In a breach investigation, endpoint telemetry is often what bridges the gap between "someone logged in" and "here is exactly what they did next on the device."

License	Capability
Business Basic / Standard	No endpoint telemetry
Business Premium	Defender for Business. Simplified EDR with basic protection, limited forensic depth
E3	MDE P1, protection controls, some telemetry
E5	**MDE P2, full EDR, 6-month forensic timeline, Advanced Hunting**



Defender for Cloud Apps

What It Shows	Forensic Meaning
Mass download or deletion events	Bulk data exfiltration or ransomware staging
Impossible travel alerts	User signed in from two geographically distant locations within minutes. Account compromised
OAuth app consent grants	User authorized a third-party app. Potential OAuth phishing or app-based persistence
Anomalous activity scores	Behavioral baseline deviation. Surfaces attackers who move slowly to avoid per-event detection
Shadow IT discovery	Unsanctioned apps in use. Data leaving the organization through unmonitored channels
Admin activity monitoring	Privileged actions across M365 services. Who changed what, when



Defender for Cloud Apps

Visibility into what your users are doing with cloud apps.. sanctioned and unsanctioned.

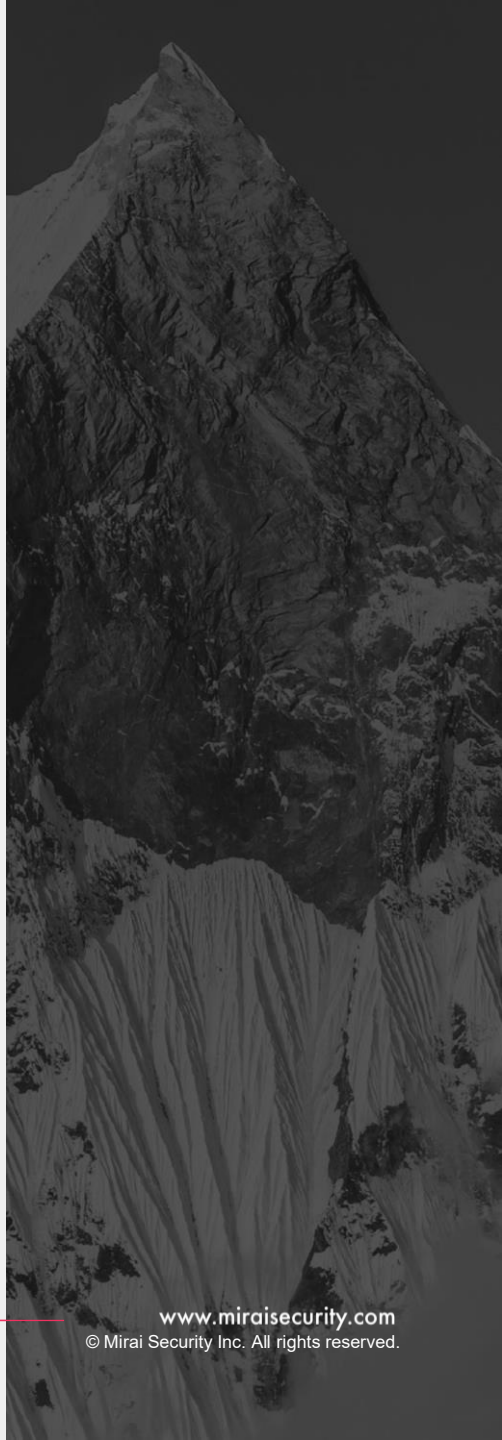
What it is:

- Microsoft's Cloud Access Security Broker (CASB). Sits between your users and cloud applications, logging activity, detecting anomalies, and enforcing policy across M365 and thousands of third-party SaaS applications.

CASB is where low-and-slow attacks get caught.

- A threat actor who avoids triggering per-event alerts often reveals themselves through behavioral patterns over time. But only if CASB is actively monitoring.

License	Capability
Business Basic / Standard / Premium	Not included
E3	Basic Cloud App Discovery only + Limited anomaly detection
E5 / Microsoft Defender XDR	Full CASB. Behavioral analytics, OAuth app governance, anomaly detection

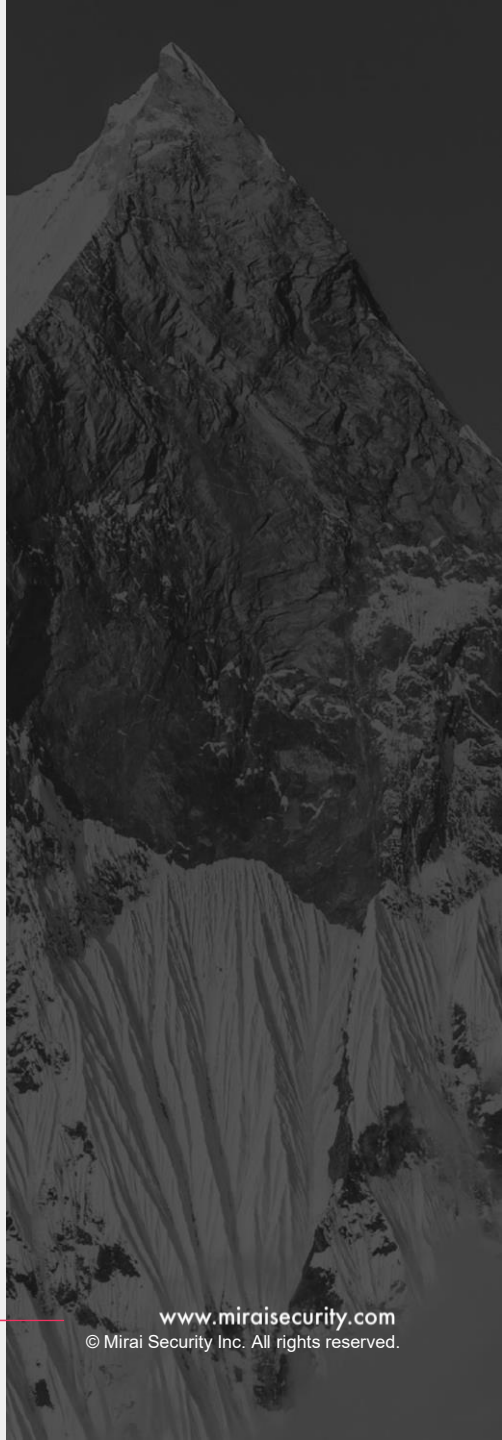


Advanced Hunting: The Unified View

One investigation surface. Every log source. The full picture.

What it is:

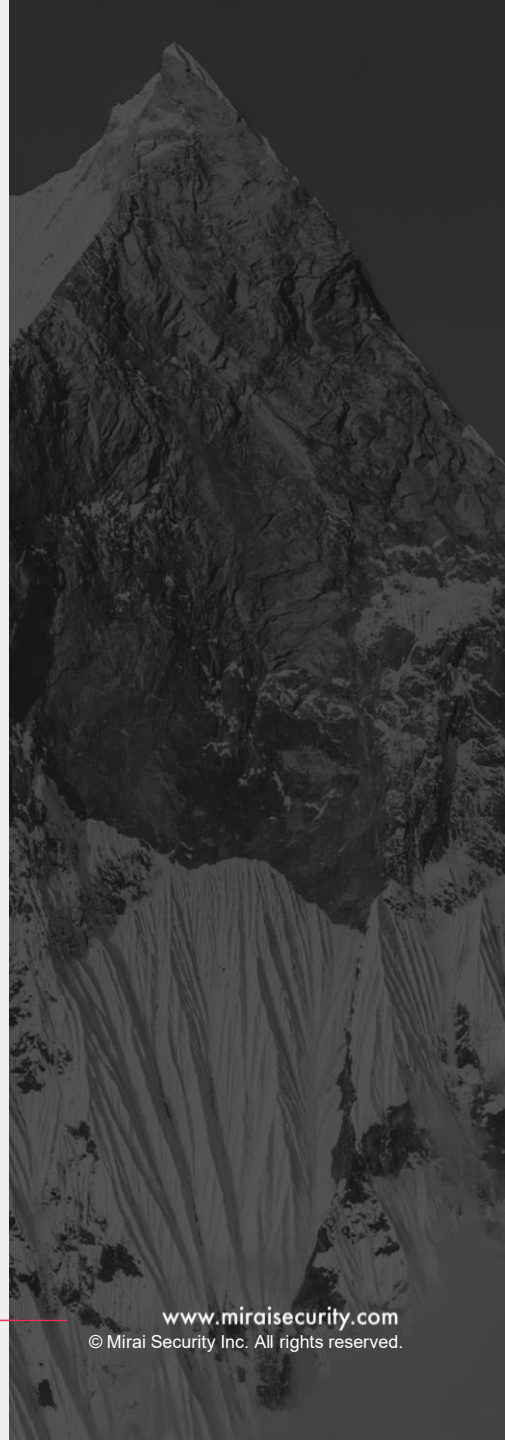
- A unified, cross-workload threat hunting environment inside the Microsoft Defender portal. Allows security teams to query across all available log sources — connecting identity, email, endpoint, cloud apps, and Graph activity in a single investigation.
- Without Advanced Hunting, each log source lives in a separate portal. An attack spanning identity, email, and endpoint requires manually correlating records across multiple tools. An investigative process that takes time and introduces gaps.
- With Advanced Hunting, the same investigation is conducted in a single environment where all log sources are joined and searchable. Reducing investigation time from days to hours.
- **Licensing reality:** Microsoft E5 or Microsoft Defender XDR standalone add-on required for full cross-workload coverage.



What if the logs were never there?

A dramatic re-enactment of your IR team's Monday morning.
Incident Responders arrive. A breach is suspected. The call goes out. CIRT is established.

- **Incident Responder Lead**: "Pull the sign-in logs."
- ***SME***: *"We only have 7 days. The breach started 9 days ago.“*
- **Incident Responder Lead**: "Fine. pull the audit log."
- ***SME****: "Audit logging was never enabled on their Business Standard tenant.“*
- **Incident Responder Lead**: “The alert shows access using MS Graph Resource.. What about Graph Activity Logs?“
- ***SME***: *"What's that?"*
- **Incident Responder Lead**: "Defender for Endpoint telemetry?" *“*
- ***SME****: “They had Business Standard. No endpoint telemetry.”*
- **Incident Responder Lead:** "So, what do we actually have?"
- ***SME****: "A very concerned CFO and a 204 page Word document titled 'Incident Response Plan' that's never been tested."*



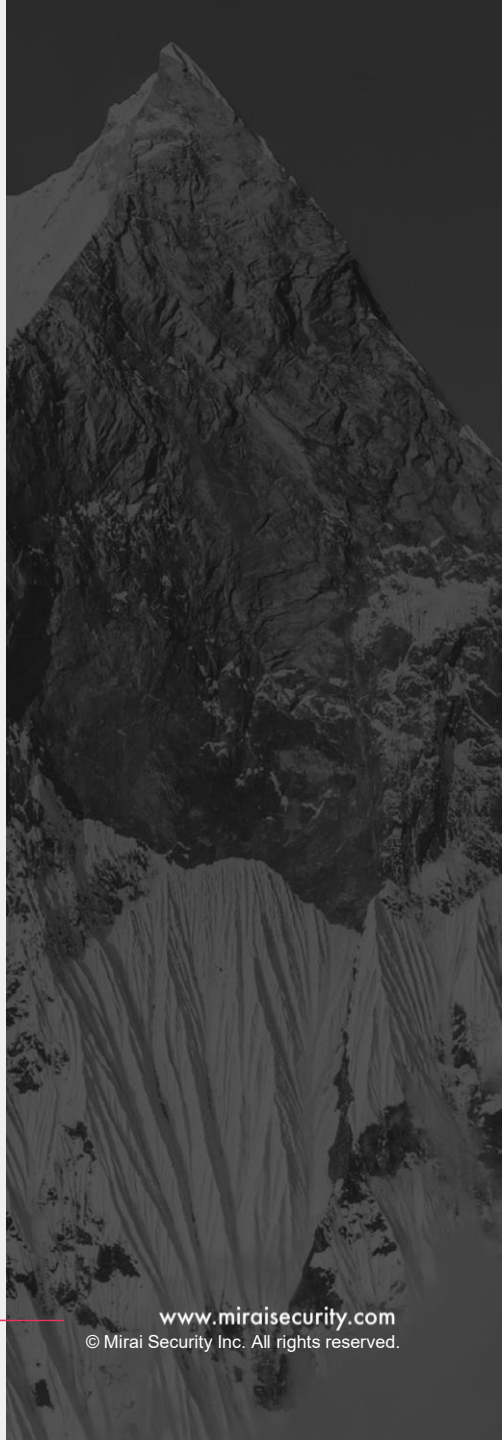
MIRAI

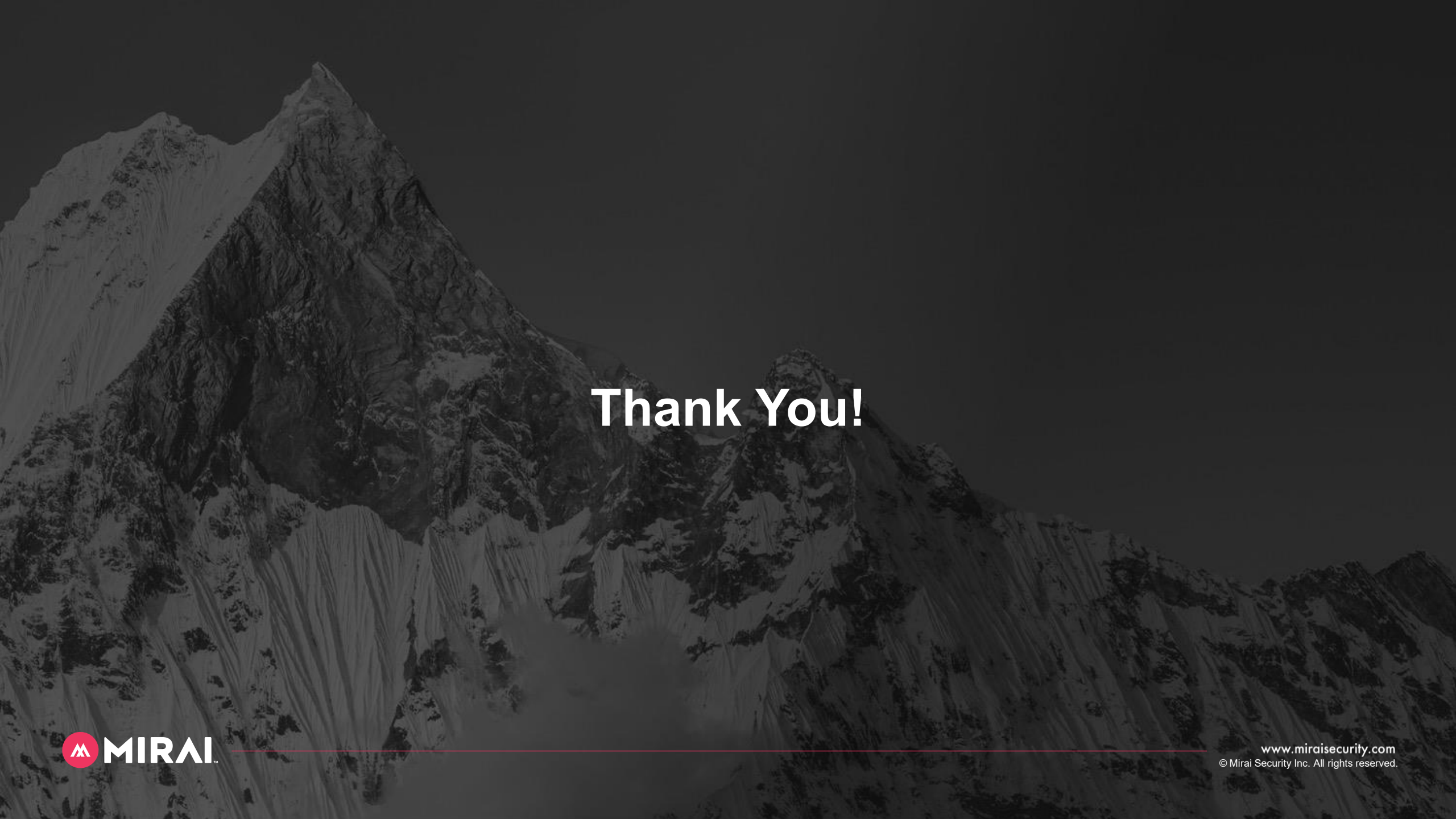
What if the logs were never there?

In all seriousness.. here is what missing logs mean:

Without	You Cannot
Audit logs	Establish any timeline of attacker activity
Sign-in logs	Prove when or where the attacker authenticated
MailItemsAccessed	Confirm which emails were read. Breach scope is an estimate, not a fact
Graph Activity Logs	Detect or attribute API-based Recon/exfiltration
Endpoint telemetry	Know what ran on the device after initial access

The attacker's best friend isn't a zero-day exploit. It's an organization that never turned on its logs.





MIRAI

www.miraisecurity.com