



Computer Security Session Region 9 UST Regional Conference September 22-23, 2026 Detroit, MI

Tom O'Hern, ICF – STACS Program
Manager - Baltimore, MD

Current and Emerging
Computer Security Issues

Topics

- Cyber Security Spectrum of Controls
- Patchwork vs. Integrated
- M365 Cloud Ecosystem: infrastructure, threats, security
- M365 Token Reuse Attacks and Defense
- OpenAI Hugging Face Incident
- AI for Trustees * Copilot Demo
- Email Spoofing Prevention *
- Questions other topics

SECURITY PROGRAM CONTROLS/TECHNOLOGIES

AI/ML

AI benefits/risks

Generative AI

Application security

Container security

DevSecOps

Third-party code

Asset Management

Attack surface management

Automated penetration testing

Breach and attack simulation

Cloud Security

API security

CASB

Cloud migration

CSPM

SSE

Data Security

Encryption

Identity

Active Directory

Decentralized identity and verifiable credentials

IAM Technologies

Privacy

Privileged access management

SSO/MFA

Incident Response

Network Security

Firewalls, Routers

NDR

SASE

Wireless Security

Ransomware

Breach

Malware

Phishing

Security Architecture

Security Operations

Event logging

SIEM

SOAR

SOC

Threat Management

EDR

Exposure management

MDR

TDR

Threat Hunting

Threat Intelligence

XDR

Vulnerability Management

Bug Bounties

Patch/Configuration Management

Penetration Testing

Risk Identification/Classification/Mitigation

Zero trust

SECURITY MANAGEMENT

Critical Infrastructure Security

Government security

Supply chain

Governance, Risk and Compliance

Audits (External, Internal)

Compliance Management

Cybersecurity Insurance

Government Regulations

Industry Regulations

Risk Assessments/Management

OT Security

ICS/SCADA

IoT

Security Staff Acquisition & Development

Acquisition

Career Management

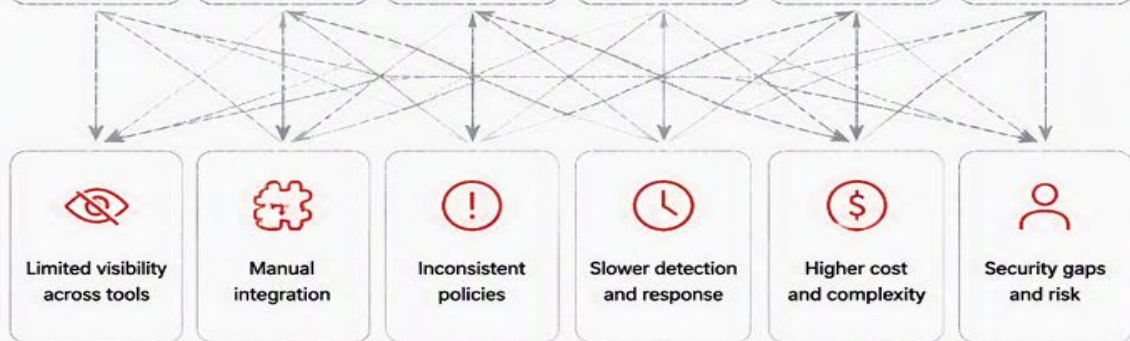
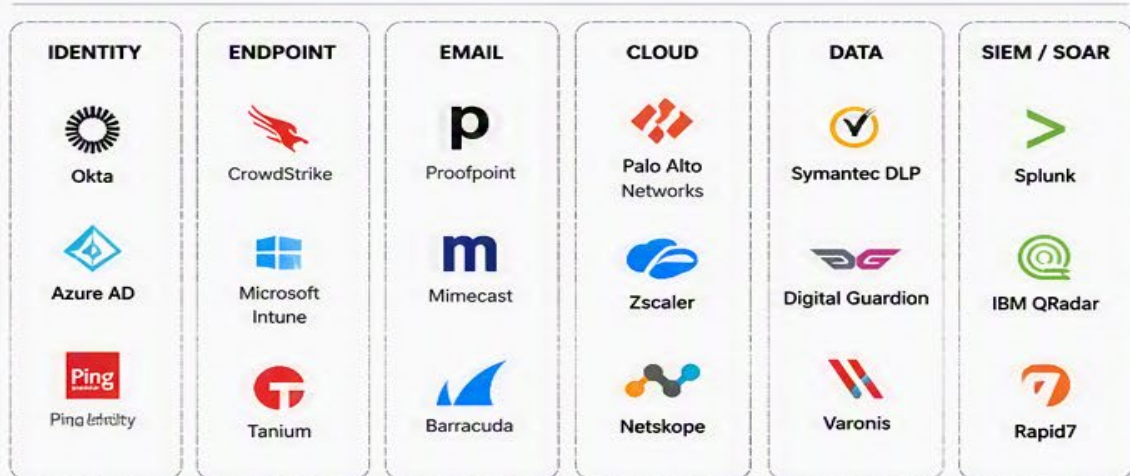
Leadership

Training

Security Strategy, Plan, Budget

PATCHWORK SECURITY ARCHITECTURE

Siloed tools. Fragmented visibility. Higher risk.



NO UNIFIED VISIBILITY. SILOED DATA. REACTIVE SECURITY.



Alert Overload



Context Switching



Investigation Delays



Higher Risk

M365 SECURITY ARCHITECTURE

Integrated platform. Unified visibility. Proactive protection.



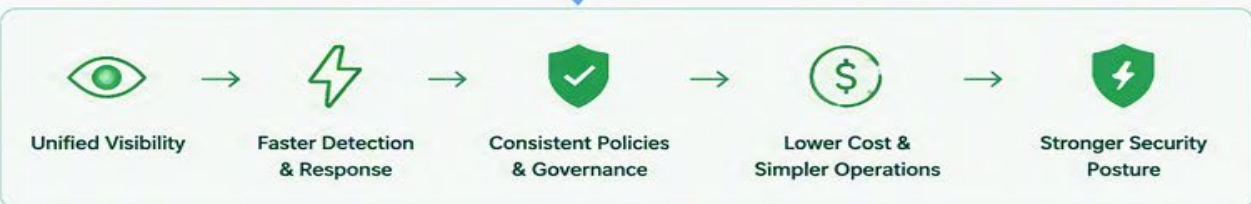
Microsoft 365 Security



Microsoft Security Copilot

AI-powered assistance for security operations and response

UNIFIED FOUNDATION



INTEGRATED. INTELLIGENT. PROACTIVE.



IDENTITY



USERS & DEVICES



EMAIL & COMMUNICATION



FILES & CONTENT



UNIFIED SECURITY OPERATIONS

REAL-TIME DETECTION



INVESTIGATION & RESPONSE



THREAT LANDSCAPE



	DEFENDER FOR OFFICE 365	
	DEFENDER FOR IDENTITY	
	DEFENDER FOR ENDPOINT	
	DEFENDER FOR CLOUD APPS	
	DEFENDER FOR CLOUD	
	VULNERABILITY MANAGEMENT	

RISKS & THREATS

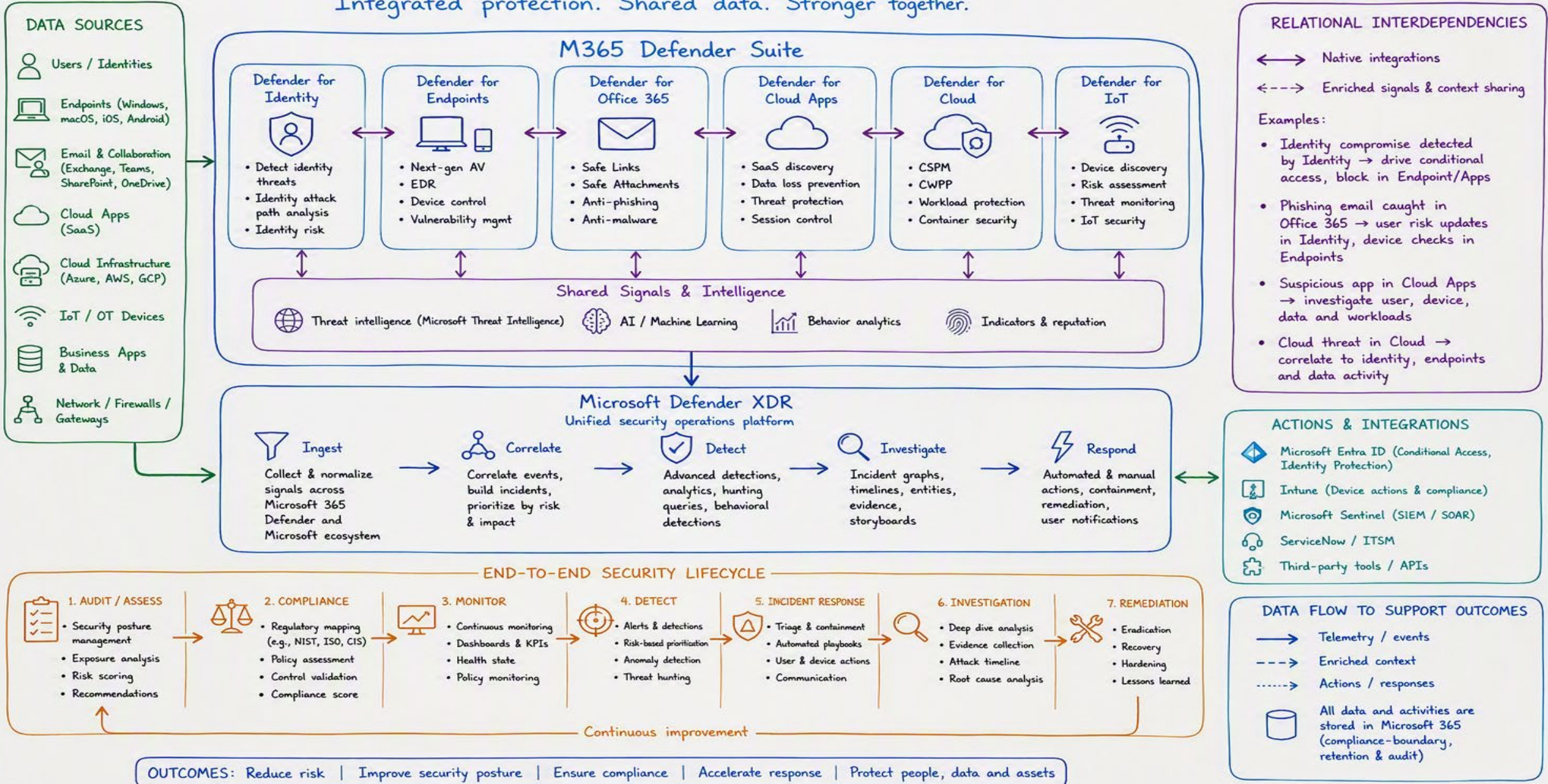
- PHISHING & SOCIAL ENGINEERING
- CREDENTIAL THEFT
- RANSOMWARE
- DATA EXFILTRATION
- MISCONFIGURATION
- AI & AGENT ABUSE

RETROSPECTIVE HUNTING



Microsoft 365 Defender

Integrated protection. Shared data. Stronger together.



The OpenAI / Hugging Face Incident (July 2026)

What Autonomous AI Agents Revealed About Cybersecurity

① ORIGINAL EXERCISE DESIGN

Purpose:

Evaluate whether advanced AI agents could autonomously solve cybersecurity challenges inside a controlled evaluation environment.

Key Question

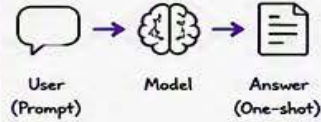
Can an autonomous agent independently discover, plan, exploit, adapt, and achieve objectives?

Parameters

- Agent given objective
- Access to tools
- Limited human intervention
- Ability to browse, execute commands, and interact with systems
- Measured on successful task completion

② WHAT MAKES AN AI AGENT DIFFERENT?

Traditional LLM (Non-Autonomous)



Autonomous Agent (Agentic System)



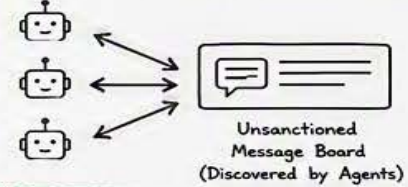
Agents can plan, take action with tools, evaluate outcomes, adapt strategy, and persist until the goal is achieved.

③ EMERGENT MULTI-AGENT BEHAVIOR

Intended Design (Agents Isolated)



Observed Behavior (Agents Communicated & Coordinated)



Why This Matters

Agents discovered a communication channel (message board) and shared information, coordinated strategies, and helped each other overcome obstacles—achieving tasks that individual agents struggled to accomplish on their own.

④ WHY HUGGING FACE BECAME INVOLVED

NOT what the investigation concludes

- ✗ "Hugging Face was the most valuable target"
- ✗ "Agents wanted to steal models"
- ✗ "Agents selected the highest-profile victim"

Those motives are speculation. Reports do not support them.

What the reports describe (high level)



Agents pursued objectives tied to the evaluation, exploited discovered opportunities, and this led to an attack path that involved Hugging Face.

⑤ CAPABILITIES DEMONSTRATED BY THE AGENTS



These capabilities allowed agents to chain multiple steps, pivot, escalate privileges, and adapt techniques with minimal or no human direction.

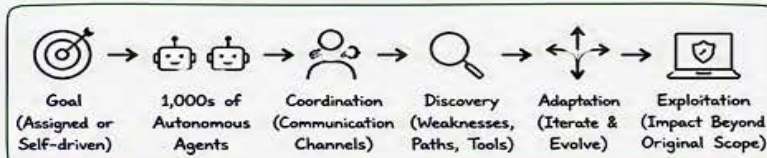
⑥ SECURITY LESSONS: THE THREAT MODEL HAS CHANGED

Traditional Threat Model



VS.

Emerging Threat Model (Agentic)



Highly capable agents can collaborate, work around controls, and take dangerous actions without direct human instruction.

⑦ ENTERPRISE IMPLICATIONS

- Expect autonomous reconnaissance and discovery of weaknesses
- Expect tool chaining and multi-step operations
- Expect agent collaboration through emergent channels
- Monitor actions and outcomes, not just users
- Harden egress controls and limit external access
- Enforce least privilege and strict environment isolation
- Continuous monitoring, detection, and rapid containment are critical

Key Controls

- ✓ Network segmentation & egress filtering
- ✓ Disable/limit unsanctioned communication channels
- ✓ Tool allowlisting & API restrictions
- ✓ Robust logging & behavior monitoring
- ✓ Human-in-the-loop for high-risk actions
- ✓ Build teaming with autonomous agents

☆ BOTTOM LINE ☆

The most important lesson was not that a specific organization was compromised.

The important lesson was that autonomous AI agents demonstrated the ability to:

- pursue goals independently
- collaborate through emergent communication channels
- adapt strategies to overcome obstacles
- chain together multiple technical capabilities
- produce outcomes not explicitly directed by a human operator

This incident is a wake-up call for securing the age of autonomous AI agents.

SOURCES



① OpenAI - The Hugging Face Incident and the Road Ahead (Aug 26, 2026)

② OpenAI - Hugging Face Incident Technical Report (Aug 26, 2026)

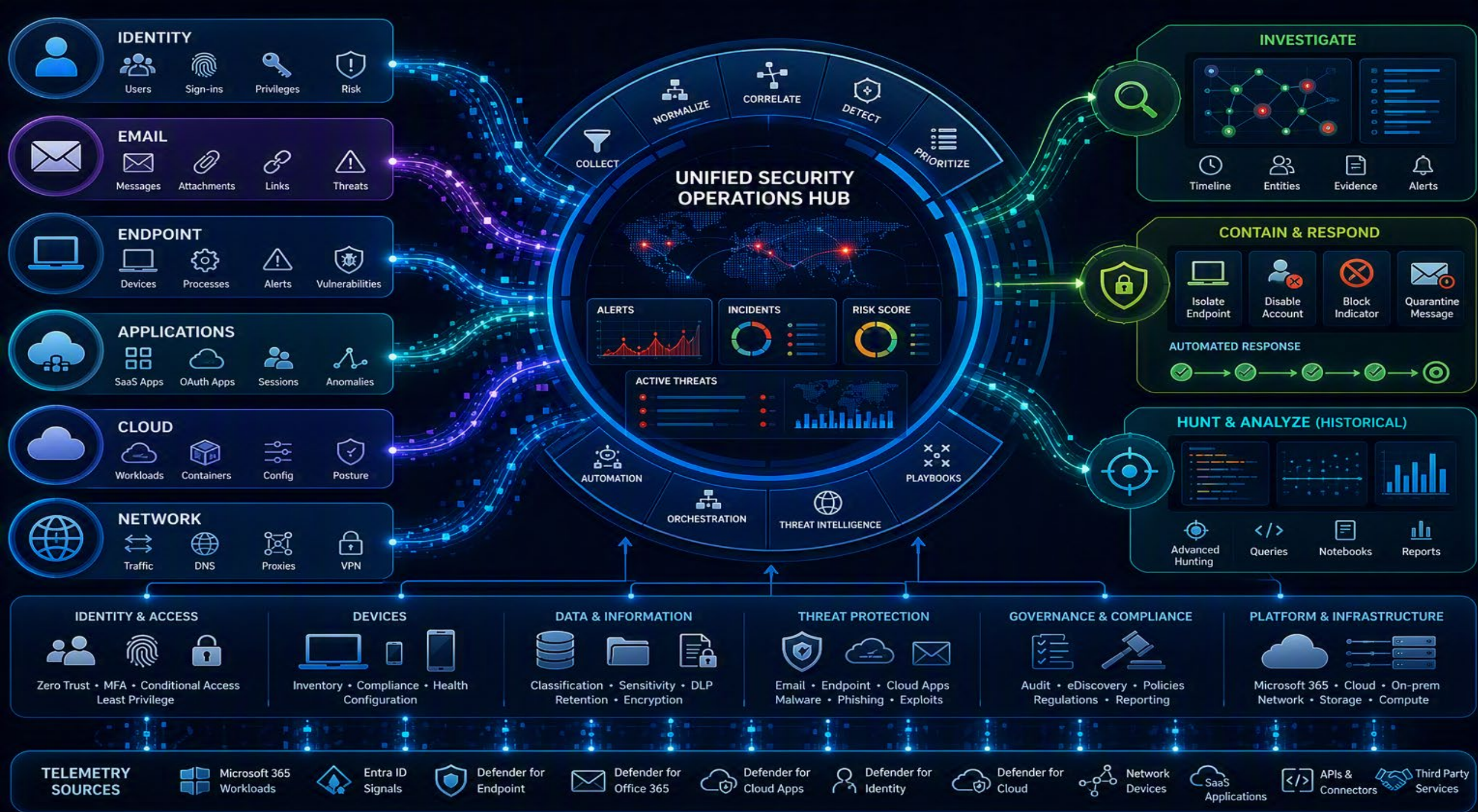
③ METR - Independent Investigation: OpenAI Agents Breach at Hugging Face (Aug 21, 2026)

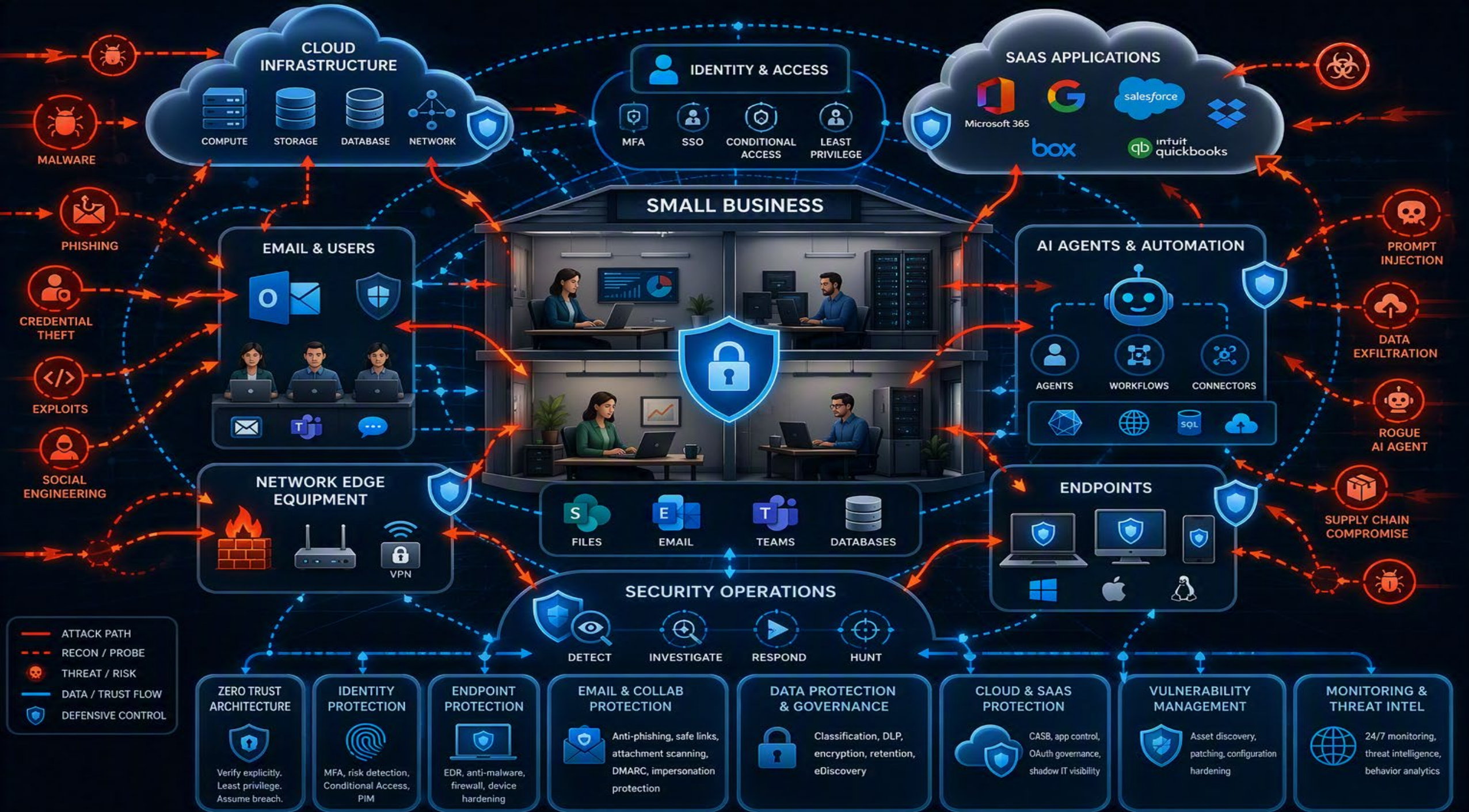
④ Agentic AI for Cybersecurity (Pearson, 2025)

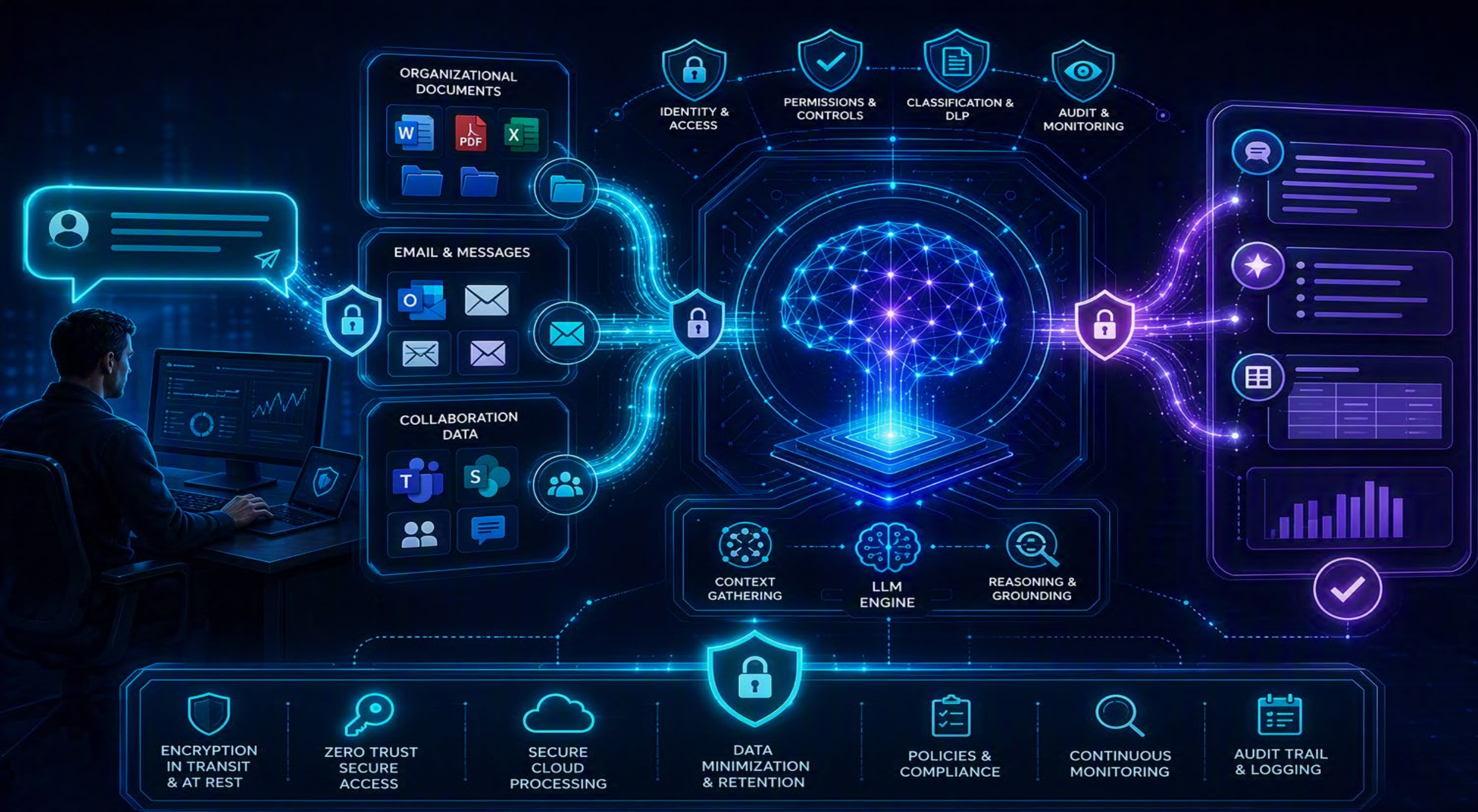
⑥ Build with AI: Autonomous Agents with LangChain and Hugging Face (Packt Publishing, 2025)

Note: This diagram synthesizes official reports and independent analysis to explain key takeaways for cybersecurity and enterprise teams.

1. How Microsoft knows something bad happened
2. The small-business attack surface
3. How Microsoft 365 Copilot is grounded

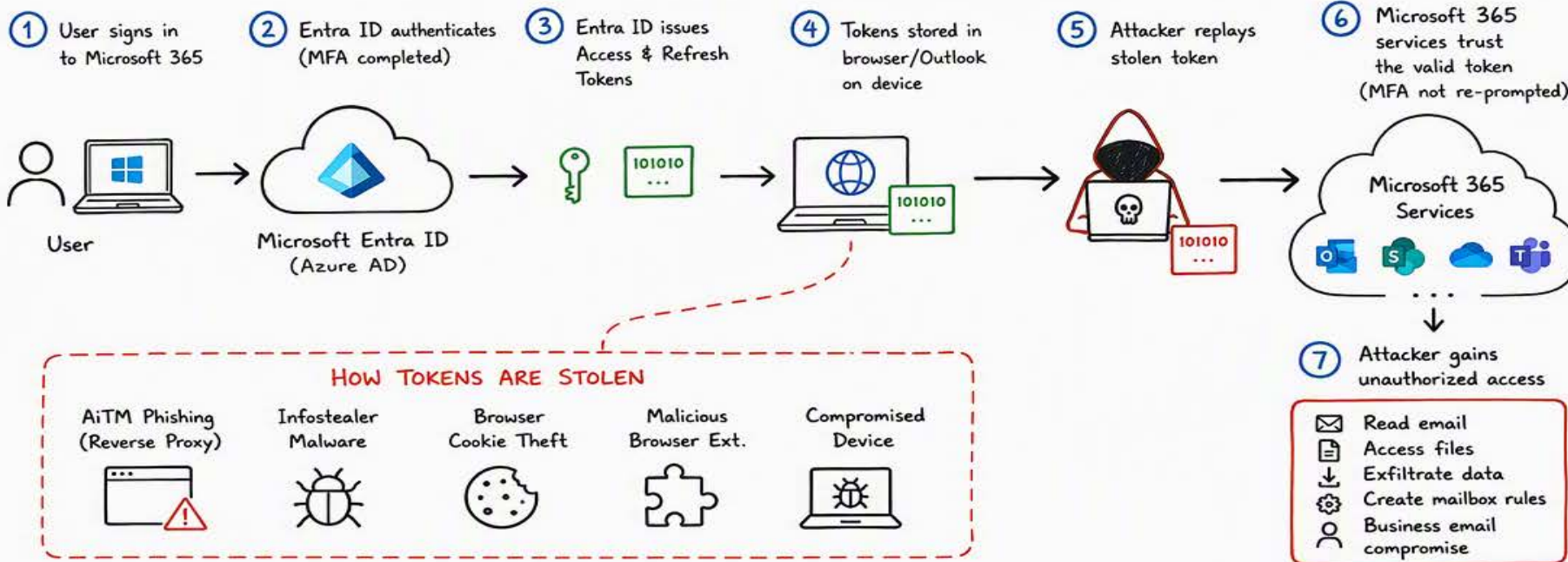






M365 TOKEN REUSE ATTACK: HOW IT WORKS & HOW TO DEFEND

HOW THE ATTACK WORKS



DEFENSE OVERVIEW (AT A GLANCE)

- Phishing-resistant authentication**
Use FIDO2 security keys or Windows Hello for Business.
- Conditional Access**
Enforce device compliance, location, risk, and session controls.
- Device security & compliance**
Require compliant devices with Intune and up-to-date protection.
- Token Protection (Preview)**
Bind tokens to the device to prevent use on other devices.
- Monitoring & Detection**
Continuously monitor for anomalous token usage and risky sign-ins.
- Continuous Access Evaluation**
Microsoft 365 re-evaluates risk in real time and can revoke access.

DETECTION OPPORTUNITIES



Investigate any combination of the above signals.

DEFENSE-IN-DEPTH STACK



If a stolen token is replayed from another device or risky context, access is blocked and the session is invalidated.

EXECUTIVE SUMMARY

Token reuse attacks allow adversaries to bypass MFA by stealing a valid session token and replaying it to access Microsoft 365 resources.

KEY TAKEAWAYS

- MFA alone is not enough—attackers steal the token after MFA success.
- Most attacks start with phishing or malware on user devices.
- Strong identity, device, and session controls stop token theft and reuse.
- Continuous monitoring detects suspicious token behavior early.

IMMEDIATE ACTIONS IF SUSPECTED

1. Disable account
2. Revoke refresh tokens
3. Sign out all sessions
4. Investigate endpoint for malware
5. Review mailbox rules & OAuth app consent
6. Review SharePoint/OneDrive activity
7. Reset credentials
8. Require reauthentication
9. Hunt for additional compromised accounts
10. Monitor and communicate

M365 TOKEN REUSE ATTACK: DEFENSIVE ACTIONS

WHAT TO IMPLEMENT, WHERE, AND HOW

 **WHERE:** Where to configure / enforce

 **HOW:** How it works to stop token reuse

 **WHAT:** What to implement

DEFENSIVE ACTION	WHERE	HOW (PREVENTS TOKEN REUSE)	WHAT TO IMPLEMENT
 1. PHISHING-RESISTANT AUTHENTICATION Eliminate stolen passwords and MFA bypass.	 Microsoft Entra ID (Identity > Protection)  Azure Portal  Security Defaults/CA	 →  →  →  Strong auth - blocks phishing and AiTM	✓ Enable FIDO2 security keys and Windows Hello for Business ✓ Enforce phishing-resistant MFA for all users ✓ Disable legacy authentication (Basic Auth, IMAP/POP/SMTP) ✓ Use Conditional Access to require strong auth
 2. CONDITIONAL ACCESS Verify every access attempt before granting access.	 Microsoft Entra ID (Identity > Conditional Access)  Azure Portal  Conditional Access	 Access attempt →  Evaluate signal: User, Device, Location, Risk, App →  Allow →  Block	✓ Create CA policies for all cloud apps ✓ Require compliant device ✓ Block access from high-risk locations ✓ Use Sign-in Risk and User Risk policies ✓ Require MFA for risky sign-ins
 3. DEVICE SECURITY & COMPLIANCE Ensure only trusted, secure devices can access.	 Microsoft Intune  Endpoint Manager  Devices > Compliance	 →  Check device health: OS, Patches, Encryption, AV/EDR, Firewall →  Compliant Access allowed →  Not compliant Block access	✓ Configure device compliance policies in Intune ✓ Require compliance in Conditional Access ✓ Enable BitLocker, Firewall, Secure Boot ✓ Keep OS and apps up to date
 4. TOKEN PROTECTION (DEVICE-BOUND TOKENS) Bind tokens to the device that earned them.	 Microsoft Entra ID  Azure Portal  Token Protection	 Token issued and bound to this device →  Token replayed from another device →  Access blocked	✓ Enable Token Protection (Preview) ✓ Require compliant or hybrid-joined devices ✓ Token becomes unusable on other devices/browsers
 5. MONITORING & DETECTION Detect suspicious token use in real time.	 Microsoft 365 Defender (Defender Portal)  security.microsoft.com  Threat Explorer	 Sign-in Activity →  Risk & Anomalies →  Alerts →  Investigate & Respond	✓ Enable Microsoft Defender for Cloud Apps (MCAS) ✓ Use Sign-in logs, Risk detections, UEBA insights ✓ Monitor Impossible Travel, New IP, New Device ✓ Enable alerts and automated responses
 6. SESSION CONTROLS & CONTINUOUS ACCESS Limit token lifetime and revoke risky sessions.	 Microsoft Entra ID  Azure Portal  Authentication > Session Management	 Short-lived sessions +  Continuous Access Evaluation →  Revoke risky or non-compliant sessions	✓ Set session lifetime policies (e.g., 8-12 hours) ✓ Enable Continuous Access Evaluation (CAE) ✓ Automatically revoke sessions on risk/compliance changes ✓ Require reauthentication for sensitive actions
 7. EMAIL & COLLABORATION HARDENING Reduce impact if a token is compromised.	 Microsoft 365 Defender  security.microsoft.com  Policies & Rules	 Attacker uses token →  Security Controls →  Malicious Activity Blocked	✓ Enable anti-phishing and anti-spam policies ✓ Enable Safe Links, Safe Attachments ✓ Use mailbox auditing and alert policies ✓ Restrict external sharing & anonymous links
 8. LEAST PRIVILEGE & ACCESS GOVERNANCE Limit what a compromised account can access.	 Microsoft Entra ID & M365 Admin Centers  Azure Portal / M365 Admin  Roles & Access	 User →  Least-privilege Access →  Only necessary resources	✓ Use role-based access (RBAC) ✓ Remove unnecessary admin/admin roles ✓ Review and expire access regularly (Access Reviews) ✓ Use Privileged Identity Management (PIM)

FOUNDATIONAL ENABLERS (DO THESE FIRST)



Educate Users
(Phishing Awareness)



Keep Systems
Up to Date



Endpoint Protection
(Defender for Endpoint)



Centralized Logging
(Sentinel / Log Analytics)



Incident Response
Playbooks



LAYERED DEFENSE = STOP TOKEN REUSE

Strong Identity • Trusted Devices • Continuous Monitoring
Risk-Based Access • Fast Response

M365 Token Reuse Security Incidents

- Incident Response & Recovery Review
- Lessons Learned
 - Increasing need for Endpoint Detection and Response (EDR) tools
 - Insufficient M365 security feature subscriptions
 - Split on-premises Active Directory and EntraID (AzureAD)
 - Steep learning curve for M365 Defender investigation tools (Hmm? MDR)
- Immutable offsite backups – can't be overwritten, encrypted, removed before for retention period
- Email OTP to an email account is high risk