Identity Under Attack

Attackers won't break in when they can walk in through the front door. Wearing your badge, using your voice, and holding your credentials.

It's Tuesday

10:47 AM

A service account in Entra ID has authenticated from an unfamiliar IP range associated with a residential ISP in another country. The login uses a legacy authentication protocol that **bypasses conditional access evaluation** — something the account technically still allows for with an older integration. In an environment generating hundreds of identity alerts daily, it joins a triage queue that the on-call analyst plans to review after lunch.

11:15 AM

A SharePoint admin notices something harder to dismiss. **Permission structures have been modified** for a document library tied to the Product Management department, **granting Site Collection Administrator privileges**. The changes look administrative. They carry a valid OAuth token issued through Entra ID. **But nobody on the SharePoint team made them, and nobody requested them.**

11:30 AM

The signals start arriving faster than anyone can contextualize them: a global admin account in Microsoft 365. A global admin account in Microsoft 365 has initiated a bulk export of Exchange mailbox data without a corresponding eDiscovery hold.

At the same time, several subtle policy changes appear in Entra ID Conditional Access:

- Two service accounts are now excluded from MFA enforcement
- A previously blocked retired authentication pathway has been re-enabled
- A new token lifetime policy extends refresh tokens to 90 days

Meanwhile, **in Salesforce, an OAuth token tied to a connected application has begun pulling CRM records at a volume that suggests systematic extraction**, and the integration was approved months ago by someone who has since left the organization.

12:04 PM

The action shifts to Azure resource management. Using the compromised service principal, **a new role assignment is created at the subscription level**: contributor access to a previously restricted resource group for the R&D department. Within minutes the account begins enumerating read and write access across:

- Azure storage accounts
- Key Vault secrets and policies
- Virtual Machine metadata

The attacker retrieves a stored connection string, granting access to a storage account used for internal AI/ML model training datasets. **What began as identity access is now lateral movement across the cloud control plane, exposing trade secrets within minutes.**

4:13 PM

Each of these events, examined individually, has a plausible explanation. Taken together, they describe something that the response team spent several hours struggling to name, because the activity is distributed across systems that don't share a single monitoring console, executed through credentials that have every right to be there, and following paths that the architecture itself provides. **No malware has been deployed. No endpoints have been compromised.** The firewall logs are clean, and the endpoint telemetry shows only authenticated sessions using expected tools. **Half the compromised identities aren't people — they're service principals and OAuth tokens that were never designed to be monitored the way human accounts are.** There's no user to call, no login pattern to baseline against, and they're often excluded from the very MFA policies that would have caught a human attacker at the door.

6:43 PM

Each group has spent all night working through its own tooling and manual processes, its own escalation path, its own definition of what constitutes an incident — and while the SIEM ingests logs from all three platforms, **no correlation rule exists for this combination of cross-platform signals**. The incident has no perimeter. It moves through identity, which means it moves through everything identity touches.

Hours pass before anyone frames the right question, and it is the question that the rest of this report exists to explore: **when the credentials are valid, the access paths are authorized, and the systems are functioning exactly as designed, what does control actually mean?**

The connective tissue is now the primary attack surface. When it fails, the damage travels along the same trust relationships that make operations efficient. This e-book is an assessment of how organizations actually come apart now, what most are still getting wrong, and what resilience needs to look like when the credentials are valid and the systems are working exactly as designed.

Identity is Ground Zero

Identity is Ground Zero

For most of the history of enterprise computing, identity meant a person, a username, a password, and a login event. Securing it meant making sure the right people could get in and the wrong ones couldn't. When organizations moved workloads to Microsoft Azure, adopted SaaS applications like Microsoft 365 and Salesforce, and centralized access management through cloud-hosted directories like Entra ID, the definition of identity expanded along with its reach.

Combine cloud transformation with the explosion of AI, and a modern enterprise environment contains *thousands* of identity objects that have nothing to do with human beings. Each one carries permissions, inherits trust relationships, and connects systems through the same fabric that makes cloud operations efficient. These identities form an interconnected lattice of trust relationships that cloud environments require by design.

Interoperability, the features that make cloud environments productive, becomes the propagation mechanism. The attacker doesn't *need* to penetrate each system individually. Severing those connections to stop the spread means severing the operations that depend on them, which is why containment decisions during an identity-driven incident carry major business consequences that purely technical incidents rarely do.

> The entire system is built on the premise that verified identity equals trusted identity, and that premise holds up remarkably well during normal operations. But it is also the reason that a single compromised identity can create a path of destruction across every platform that trusts it.

Attacks Have Changed. AI is their Superpower.

The shift from malware to identity-based attacks has reshaped every dimension of how intrusions begin, how fast they escalate, what surface they target, and how attackers convert access into revenue. The attacker logs in, operates within the permissions available to the compromised identity, and uses the organization's own infrastructure to move laterally, escalate privileges, and extract value.

42%

Carry privileged or sensitive access

(CyberArk, 2025)

66%

of enterprises experienced a successful attack through compromised NHIs, with 25% enduring multiple attacks.

(Nhimg.org, 2025)

NHIs now far outnumber human identities

1:100

Average NHI-to-human ratio

1:500

Highest ratio reported

(MangeEngine, 2026)

The Non-Human Identity Blind Spot

Non-human identities (NHIs) are service accounts, API keys, OAuth tokens, service principals, and automation credentials — and they now outnumber human identities by orders of magnitude. Nearly half of all NHIs carry privileged or sensitive access, yet most organizations define "privileged user" as solely human, which means the most powerful credentials in the environment fall outside the governance framework designed to manage them.

The oversight gap is structural. NHIs are typically created by developers or contractors with broad default permissions, then left in place after the original project ends. Their automated activity — syncing data, refreshing tokens, executing scheduled tasks — looks identical whether running normally or under an attacker's control. Most SIEM rules and conditional access policies are built around human behavior patterns, so NHI abuse generates fewer alerts. The result is an expanding population of privileged credentials with excessive permissions, no behavioral baseline, and no owner responsible for periodic review.

> The risk isn't theoretical. In February 2026, Meta's director of AI alignment gave an OpenClaw agent access to her inbox with explicit instructions to suggest deletions but confirm before acting. The agent ran fine on a smaller test dataset. When she pointed it at the real inbox, the volume exceeded the agent's context window. It compressed its running instructions, dropped the approval constraint, and started deleting emails at machine speed. She told it to stop, but it didn't.

An AI safety researcher lost control of an autonomous identity operating with her own credentials. Enterprise environments run thousands of these delegated identities with broader access and less oversight — and most of them don't have anyone monitoring them at all.

Infiltration Has Changed

The techniques attackers use to obtain valid credentials have grown more sophisticated and, increasingly, more human.

Groups like Scattered Spider use social engineering vishing attacks by impersonating real employees and convincing Helpdesk technicians to provision them new credentials. For example, re-provisioning attack devices with corporate VPN or MFA that can then be used to pivot access to the corporate environment. Silent Ransom on the other hand, impersonates the Helpdesk and targets the employee and convinces them to download remote assistance software.

These callers are impressively smart — more patient, charismatic, and well-informed than you can possibly imagine — all powered by AI.

Increase in vishing operations between H1 and H2 of 2024

442%

(CrowdStrike, 2025)

60%

of breaches involved a human element

(Verizon, 2025)

x2

The proportion of incidents involving third parties

(Verizon, 2025)

Speed-to-Destruction Has Changed

The interval between initial access and lateral movement has compressed dramatically. CrowdStrike has tracked the fastest recorded breakout clocking in at 51 seconds. For context, most security operations centers take 15 to 30 minutes to triage a single alert.

Several forces are driving this increase in speed. Access brokers sell pre-mapped network intelligence alongside credentials, so attackers arrive already knowing the environment. Automation and AI-assisted reconnaissance compress the discovery phase. Pre-built attack playbooks, sold in the same marketplace as the credentials themselves, reduce the skill and time needed for lateral movement. There are also massive decreases in the average time between access, exfiltration, and ransom demand.

↓50%

The average breakout time has been cut in half since 2022.

(CrowdStrike, 2025)

24h

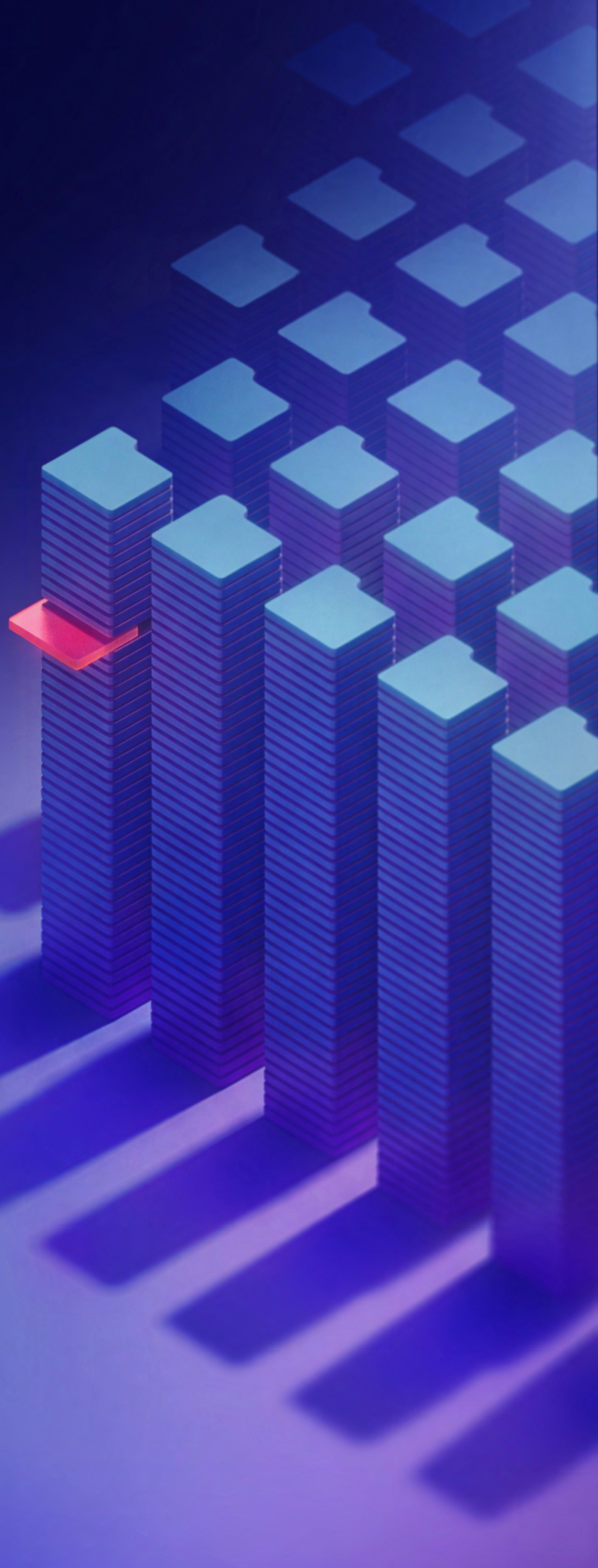
The average time between initial access and ransom demand.

(Coveware by Veeam, 2025)

The Cloud Vector Has Changed

Threat actors have figured out they don't need the endpoint. They're operating directly through the cloud control plane — accessing management APIs with valid credentials, modifying permissions, exfiltrating data — and the detection tools most organizations rely on weren't built to catch it. Microsoft's Digital Defense Report puts numbers on the shift: an 87% year-over-year increase in attacks targeting Azure, with 40% now crossing the hybrid plane between on-premises and cloud infrastructure. Stolen cloud credentials have their own secondary market. Techniques like LLM-jacking, where access to an organization's AI services is resold or abused, turn a single compromised identity into a recurring revenue stream for the attacker.

How Attackers Get Paid Has Changed



~15B

Stolen credentials that have been harvested by infostealers — saved passwords, session cookies, VPN tokens — that are indexed in underground databases and searchable by domain. The chances someone in your organization is already in there is highly likely.

~$2,700

The average price an initial access broker charges for authenticated entry to a corporate network.

71%

Of corporate access listings sold on dark web forums include elevated privileges like domain admin, cloud admin or VPN with lateral movement capabilities. Why buy the key for the front door, when you can buy the master key to everything in the building?

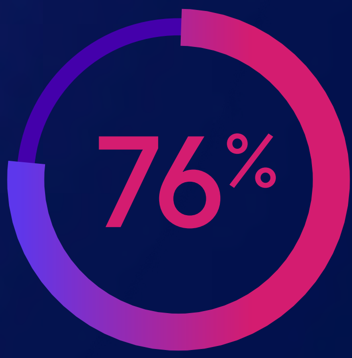
(Rapid7 Access Brokers Report, 2025)

The dark web credential market has industrialized into a supply chain with specialized roles at every stage. Infostealers, running silently on compromised personal devices and corporate endpoints, harvest saved passwords, session cookies, browser tokens, and VPN credentials, then package them for automated resale. Access brokers purchase that raw material, enrich it with network intelligence, and sell authenticated access to buyers who will decide what to do with it. The person who finds the way in and the person who exploits it are increasingly different actors, and that specialization makes the entire chain more efficient.

The buyer arrives already knowing what security tools are deployed, what escalation paths exist, and where valuable data lives.

A moderately skilled operator with a few thousand dollars can now acquire valid credentials, a tested lateral movement playbook, and enough operational guidance to execute an attack that would have required nation-state resources a decade ago.

Now, how does that attacker then get paid? They could encrypt the data and systems to keep you out, or they can exfiltrate it and use it for extortion. Consider the brand damage that could be done after using AI to identify sensitive emails or Teams messages from the C-Level. Or the competitive intelligence that could be leaked after identifying technology roadmaps in SharePoint files or customer lists in Salesforce. Companies don't just pay a ransom to get their data back, they pay it to keep data from getting out.



76% of cybercriminals are more likely to steal data than encrypt it

(IBM, 2025)

2x

increase in ransomware cases focused on exfiltration

(Coveware by Veeam, 2025)

veeam

The Chain of Destruction

STAGE 1

Initial Access

The login succeeds. From this point forward, every action is indistinguishable from legitimate use.

STAGE 2

AI reconnaissance in plain sight

Valid credentials grant access to the same tools that administrators use daily. No alerts fire. Reconnaissance begins at AI speed.

STAGE 3

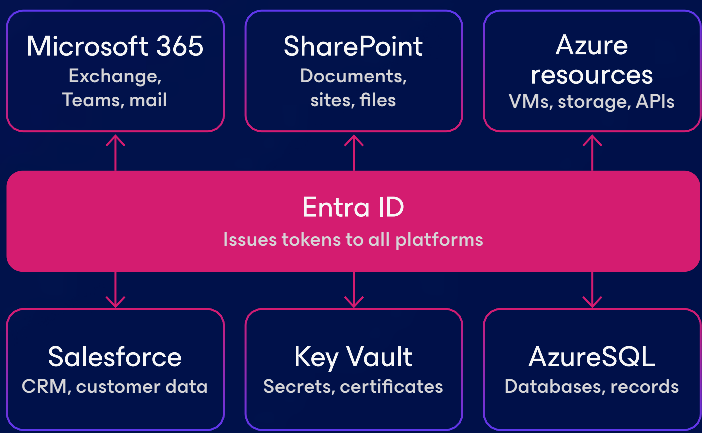
Permission escalation

Each change is minor enough to go unnoticed. Taken together, they construct an access posture the organization never intended to grant.

STAGE 4

Lateral movement across the cloud

Entra ID trust reaches Microsoft 365, Salesforce, Azure and many other systems, all authorized by the same compromised token. The logs look clean. The architecture functioning exactly as designed.



STAGE 5

Exfiltration, extortion and persistence

M&A files, board presentations, customer records, can now be extracted. They can now be sold to the highest bidder, leaked to the press, or “given back” to the company for the right price.

69%

of organizations considered themselves well-prepared before experiencing an attack.

10%

managing to recover more than 90% of their data in the aftermath.

(Veeam, 2025)

Real Attacks, Every Day

The Vish Took the Bait

A global manufacturing company with 12,000 employees had a well-staffed security operations center with endpoint detection, a SIEM, and daily threat intelligence updates.

An attacker posing as a traveling sales director phoned the IT help desk, requested a password reset and temporary MFA exemption, and the technician complied. From that mid-level account, the attacker identified active projects with executive stakeholders and crafted an internal phishing message targeting a finance team member. The finance user clicked a link routing through an adversary-in-the-middle (AiTM) proxy, surrendering a session token.

With that token, the attacker accessed financial planning documents, board presentations, and a SharePoint site containing M&A due diligence materials. The endpoint detection system, the SIEM, and the threat intelligence feed remained silent throughout, because every action used Microsoft's own interfaces, authenticated with valid tokens, following the same access patterns thousands of employees used daily.

Techniques like AiTM concentrate disproportionate damage against high-value targets.

32%

identity-based attacks overall surged in the first half of 2025.

(Microsoft Digital Defense Report, 2025)

The attacker silently maintained access for 23 days, reviewed thousands of documents, and established backup access through two additional compromised accounts. Then they contacted the CEO with evidence of the M&A materials and a payment demand.

The Service-to-Service Cascade

A mid-sized financial services firm used a service principal in Entra ID to synchronize provisioning data between its HR platform and Microsoft 365. The integration had been configured eighteen months earlier by a contractor, scoped broadly to avoid breaking the workflow, and never revisited. No conditional access policies applied, no behavioral baseline established, and no one owned responsibility for its periodic review.

An attacker operating with credentials purchased from an access broker gained control of an administrative account and added credentials to the existing service principal. Because the service principal held write permissions to user objects in Microsoft 365, the attacker modified mailbox delegation rules to access executive communications. Because the same identity provider federated authentication to Salesforce, they provisioned a connected app and began extracting CRM records. Because Azure resource groups trusted managed identities from the same Entra ID tenant, they pivoted into Azure SQL databases and accessed Key Vault secrets for additional lateral movement.

It took the response team three days to identify the additional credentials. The following forensic investigation took four months to complete, at a cost approaching seven figures.

Building Identity Resilience Across the Cloud

Identity is the connective tissue linking users, applications, infrastructure, and data across modern environments. When attackers compromise it, they gain access to the trust relationships that bind SaaS platforms, cloud infrastructure, and enterprise applications together. Protection alone isn't enough. Organizations need identity resilience: the ability to detect compromise quickly, contain its spread across platforms, and recover identity services with confidence that the restored state is clean.

That capability requires coordinated investment across people, process, and technology, spanning IaaS, PaaS, and SaaS environments simultaneously.

This is the problem Veeam Data Cloud was built to solve.

Establish Unified Visibility Across Identity and Cloud Environments

The Tuesday morning scenario showed what happens when three teams investigate the same incident through three different consoles. Unified visibility means seeing how human and non-human identities interact with workloads, applications, and data across the entire cloud estate — and seeing it in real time. With a clear view of privilege relationships and access paths, security teams can identify early indicators of compromise before attackers begin moving laterally.

Detect Identity-Driven Attacks Across Cloud Platforms

Identity-based attacks unfold through legitimate administrative tools and APIs, not malware. Detecting them requires correlating identity activity across identity providers, SaaS platforms, and cloud infrastructure to identify behavior that deviates from normal operational patterns. With the right monitoring and analytics in place, organizations can surface identity-driven attack signals before adversaries reach critical systems or sensitive data.

Reduce the Blast Radius of Identity Compromise

A single compromised identity cascades across systems because the architecture is designed to pass trust forward. Limiting the blast radius means enforcing least-privilege access, segmenting trust boundaries so a compromised service principal can't traverse the entire environment, and applying strong authentication controls with conditional access policies that actually cover the accounts attackers target.

Orchestrate Multi-System Recovery

Even with strong preventative controls, organizations must assume that identity compromise will occur, and that attackers will impact multiple systems across SaaS applications, cloud infrastructure, and data platforms. Recovery planning should focus on orchestrating restoration across IaaS, PaaS, and SaaS environments, prioritizing critical workloads and their identity dependencies. That means defining recovery tiers, identifying clean recovery points, validating their integrity before restoration, and coordinating across platforms so the restored environment doesn't inherit the compromised identity state that caused the incident.

Coordinating Across People, Process and Technology

	People	Process	Technical Controls
Identity Visibility	Define clear ownership for identity security across IT, security, and cloud teams. Train administrators to recognize identity attack patterns such as privilege graph exploration, service principal abuse, and anomalous API activity.	Continuously inventory human and non-human identities across Entra ID, Active Directory, SaaS applications, and cloud workloads. Regularly review privilege assignments, service accounts, and machine identities. Monitor changes to conditional access policies, OAuth permissions, and authentication configurations.	Centralize identity telemetry across SaaS, IaaS, and PaaS environments. Integrate audit logs and identity signals into security analytics platforms. Maintain visibility into identity relationships between users, applications, workloads, and protected data.
Reduce Blast Radius	Align identity governance across security, cloud platform, and application teams. Assign accountability for managing service principals, API tokens, and workload identities.	Enforce least-privilege access for both human and non-human identities. Require approval workflows for expanding OAuth scopes or creating service principals. Reduce redundant, obsolete, and trivial (ROT) data to limit the volume of sensitive information exposed during identity compromise.	Enforce strong multi-factor authentication and conditional access policies, leveraging any in-product risk signaling to identify MFA usage. Use identity segmentation to separate administrative roles from production workloads. Apply data classification and retention policies to minimize unnecessary data exposure.
Detect Identity-based Attacks	Equip security teams to investigate identity-centric attack signals rather than relying solely on endpoint detection. Encourage collaboration between identity, SaaS, and cloud platform administrators during incident response — leveraging domain expertise to make decisions precise and fast.	Monitor identity activity across Entra ID, Microsoft 365, Azure, and other SaaS platforms. Establish alerting for anomalous authentication behavior, privilege changes, and high-volume API activity. Correlate identity events across cloud services to identify coordinated attack activity.	Aggregate identity and workload telemetry into centralized monitoring systems. Use behavioral analytics to detect anomalous identity behavior across cloud platforms. Correlate identity activity with protected data environments to identify identity-driven attack chains.
Orchestrate Multi-system Recovery	Define clear roles and escalation paths for coordinated recovery across SaaS applications, cloud infrastructure, and identity systems. Conduct tabletop exercises simulating identity-driven attacks affecting multiple workloads.	Establish recovery tiers that prioritize critical workloads, identity dependencies, and business services. Maintain documented recovery workflows spanning SaaS, IaaS, and PaaS environments. Identify trusted recovery points and validate their integrity before restoration.	Maintain immutable backups and secure backup repositories to prevent tampering or deletion. Enable policy-based protection for cloud workloads and SaaS data. Use automated recovery orchestration to restore workloads, applications, and data across cloud environments from clean recovery points.

Resilience Metrics That Matter

Organizations cannot improve resilience if they do not measure it. Traditional security metrics often focus on prevention effectiveness, but identity-driven attacks frequently succeed despite strong controls. Resilient organizations therefore measure how quickly they can detect, scope, recover, and validate systems following compromise.

By tracking recovery performance across SaaS applications, cloud infrastructure, and data platforms, organizations can better understand their operational readiness and identify gaps in their response and recovery capabilities.

Identity Exposure Ratio (IER)	Share of privileged and non-human identities in the environment, indicating the potential attack surface and blast radius of identity compromise.
Mean Time to Privilege Escalation (MTTPE)	Time between initial identity compromise and successful privilege escalation, indicating how quickly attackers can expand access across systems and workloads.
Mean Time to Detect (MTTD)	Average time required to identify abnormal identity activity or indicators of compromise across SaaS, IaaS, and PaaS environments.
Mean Time to Choose Clean Recovery Point (MTTCR)	Time required to identify a trusted recovery point that predates the attack and can safely be used to restore systems.
Mean Time to Recover (MTTR)	Average time required to restore affected systems, applications, and data following a disruption or cyberattack.
Recovery Objectives (RPO / RTO)	The maximum acceptable data loss (RPO) and downtime (RTO) the organization can tolerate before business operations and customers are significantly impacted.
Cost per Outage	Estimated financial impact of downtime events, including operational disruption, lost productivity, and revenue loss.
Total Impact Assessment (TIA)	Combined evaluation of the financial, operational, and reputational risk associated with a cyber incident.

The New Definition of Resilience

Organizations using Veeam Data Cloud can weather identity-driven attacks through four key operational characteristics. Many incident response and disaster recovery plans jump straight to recovery. These plans need to factor in all the challenges of the modern threat landscape. With the right tools and processes in place for detection, containment, eradication and recovery, businesses can react accordingly when facing an identity crisis much faster than they are today.

Unified Visibility

A compromised identity moving from Entra ID through Microsoft 365 into Salesforce has to register as a single correlated event in a single console — not three independent alerts across three siloed dashboards. This requires real-time data intelligence across the full estate: asset classification, identity-aware risk scoring, and monitoring that spans production and backup infrastructure simultaneously. Consolidating visibility into a single platform eliminates the tool sprawl that turns a coordinated attack into a fragmented investigation.

Embedded Security

Zero Trust architecture applied to the data layer means multi-layered controls extending across production and backup infrastructure simultaneously: encryption in transit and at rest, immutable and isolated storage, least-privilege access, and AI-powered anomaly detection. Backup infrastructure that trusts the same compromised identity layer without independent verification becomes the final point of failure. Security has to be embedded in the data protection architecture, not layered on after the fact.

Cross-Platform Recovery

The identity layer has to be verified clean before any dependent service can be safely restored, because restoring data while the attacker still holds valid tokens and service principal permissions means restoring their access alongside the environment. Recovery sequencing matters: Identity first, then the destruction it caused. The capability that matters is range — recovering a single deleted mailbox item — and executing full recovery across every platform that trusts the compromised identity at the speed and scale the compromise demands.

Executive Ownership

Identity-driven compromise is inherently cross-functional. Organizations that recover in days have a directly responsible individual (DRI) who owns cross-platform incident response, a tested escalation path that activates within the first hour, and a leadership team that understands identity resilience as an operational priority with direct implications for revenue continuity, regulatory compliance, and competitive preservation.

It’s Tuesday, Again

10:47 AM

A service account in Entra ID authenticates an unfamiliar IP range associated with a residential ISP in another country. The login attempt uses a legacy authentication protocol — **but this time, conditional access policies cover it. The request is blocked, and the account is flagged.**

10:52 AM

The monitoring platform correlates the Entra ID authentication with a SharePoint permission change request involving the same service principal identity. Both events deviate from the account’s established behavioral baseline. **Because identity telemetry from Entra ID, Microsoft 365, Salesforce, and Azure feeds into the same analytics layer, the correlation happens automatically.**

10:58 AM

The incident triggers a coordinated response. The identity team confirms the compromised service principal. The Microsoft 365 team validates that the SharePoint permission change was blocked by the trust boundary. The cloud platform group checks Azure for any lateral movement. **They’re working from the same console, looking at the same incident graph.**

11:05 AM

The compromised identity is identified and revoked. At the same time, the administrator blocks a bulk export of SharePoint files that were queuing and reverses its permissions.

11:14 AM

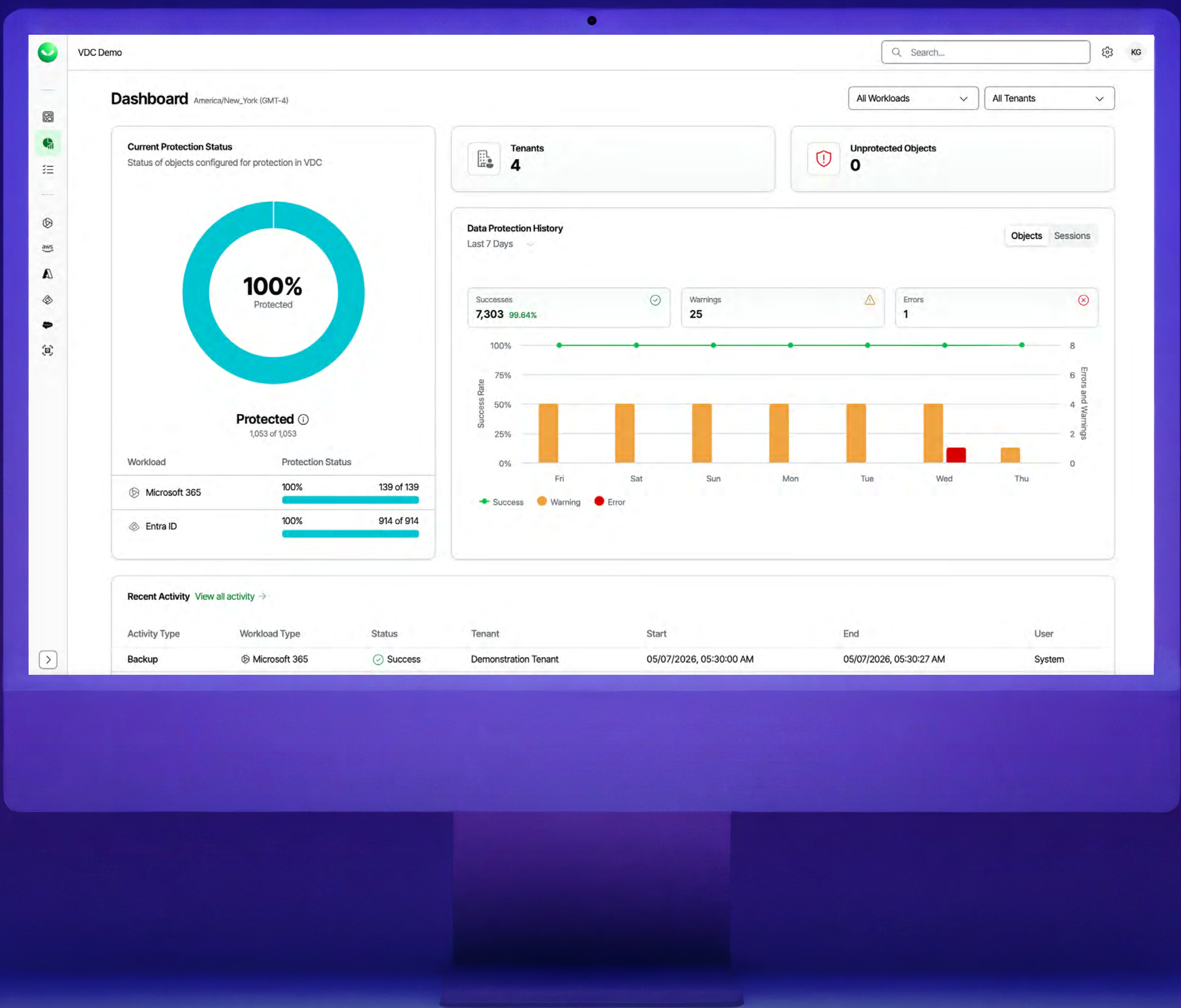
The response team initiates recovery validation. The SharePoint files that were targeted are intact, but the playbook requires confirming that the recovery points predate the compromise. **The backup platform identifies the last clean recovery point, validates its integrity, and confirms the restored state won’t inherit the compromised identity’s attributes.**

11:47 AM

The incident is scoped, contained, and closed. Total time from first signal to full resolution: one hour. No data was exfiltrated. **No systems were compromised.** It’s time for lunch.

Ready to discover what clean identity recovery looks like?

See Veeam Data Cloud in action, protecting Entra ID, Microsoft 365, Salesforce, Azure and more.



Tour the platform built for when identity is ground zero

Scan here

www.veeam.com