

REZONATE

Winning the Identity War:

How to Protect Your Organization's Most Critical Asset



Contents

Introduction	03
The Challenges of Identity Security	04
Navigating the cloud	05
Gaining visibility	07
Defending against identity attacks	08
Staying compliant	10
Core Vulnerabilities in Modern Enterprises	13
Supply chains	14
Social engineering	15
Authentication mechanisms	16
Ransomware	18
Unmanaged and misconfigured identities	19
Non-human identities	20
The identity attack flow	21
Fighting Back	24
What's required?	25
The five pillars of identity security	27
How to Improve Your Security Posture with Rezonate	31
Conduct a risk assessment	33
Centralize your security	34
Automate!	35
Build ITDR into everything you do	36
Identity security hygiene best practices (checklist)	39
Next Steps	40
Appendix	42

Introduction

As organizations move beyond traditional networks to embrace cloud-based infrastructures, SaaS applications, and hybrid working environments, digital identities have been given unprecedented levels of power. They're a single source of truth, letting employees, third parties, and machines all freely navigate cloud infrastructure from different devices and endpoints around the world. This is great news for organizations in search of flexibility and efficiency – not so much for security teams.

Attackers today are targeting user credentials, compromising valid accounts to gain immediate access to the heart of public and private cloud networks. They're preying on the fact that it's harder than ever for organizations to know where their identities are, what they're doing, or whether they're even legitimate.

The cloud is not a padded playground. It's a vast and complex environment that's home to a growing number of vulnerabilities and threat actors. Yet, when organizations charge forward with cloud migration armed only with traditional identity and access management (IAM) tools, they lose crucial visibility and control over their digital identities – and this is when attackers strike.

The time is now for IAM and security teams to wipe clean and reduce the identity attack surface. Protecting your organization from data breaches means modernizing your defenses to keep pace with the rising tide of identity-based attacks. The way can be rocky – it involves taking responsibility for an increasing disparity of identities across on-premises and cloud platforms, wrapping your IAM processes with holistic visibility, observability and actionability – all while remaining compliant with today's cyberinsurance requirements, and strict cybersecurity and data protection regulations.

But you're not alone. We've created this ebook to give hope to CISOs, IT, cybersecurity, and IAM teams looking to take control of their identity attack surface and proactively strengthen their identity security posture. Through a series of resources, best practices, and real-world case studies, we'll reveal the identity-based challenges plaguing organizations today, address the drawbacks of traditional IAM/IGA solutions, and take a deep dive into what's required to scale identity-centric security across all your IaaS, SaaS, and identity provider (IdP) platforms.

And with that, we'll show you how the [Rezonate platform](#) offers a unified, risk-driven, and context-aware approach to protecting all identities across your organization's network that helps you achieve a much faster time-to-value.

The Challenges of Identity Security

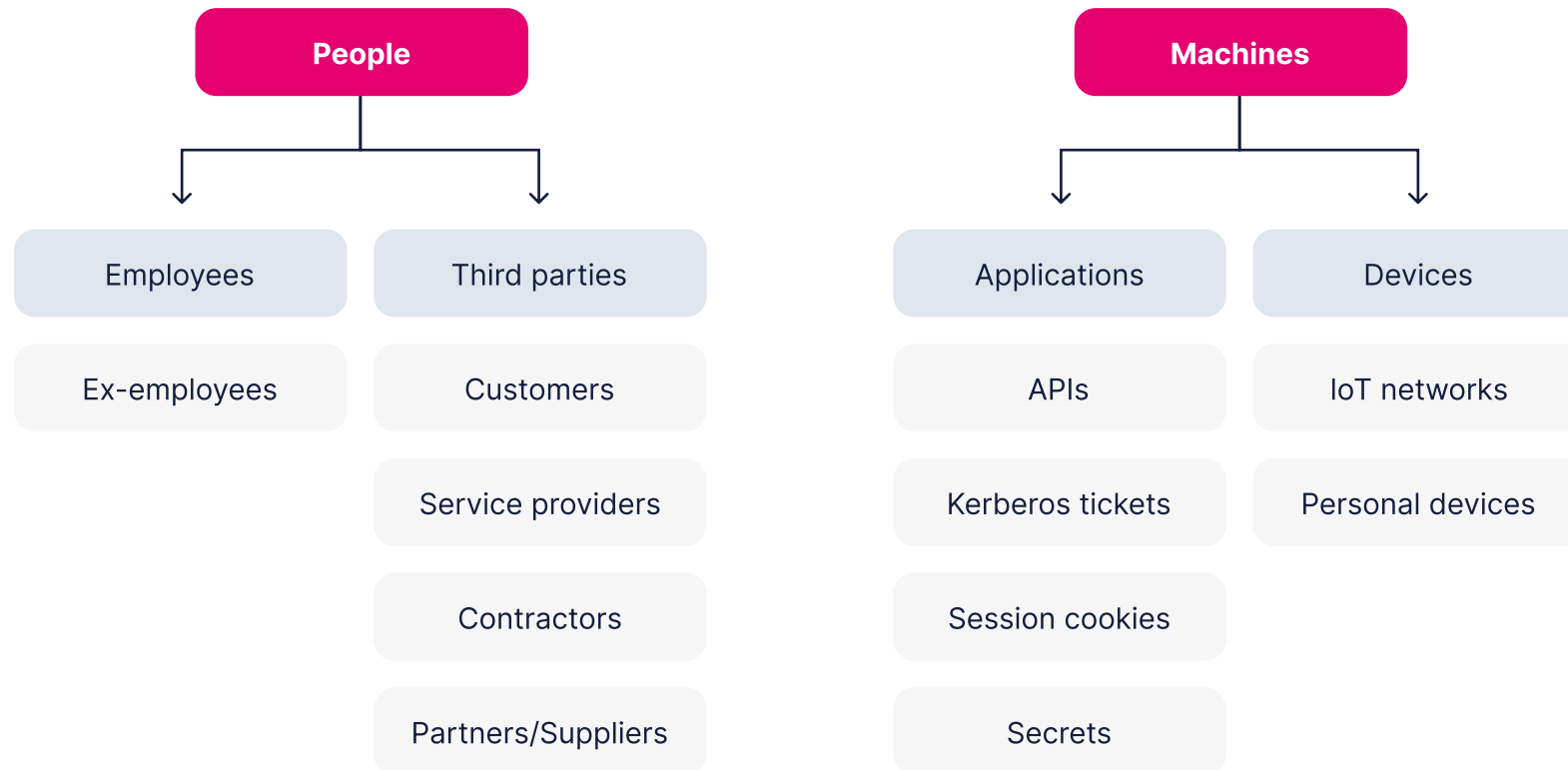


The Challenges of Identity Security

A cloud-first approach offers unprecedented speed and flexibility for organizations looking to scale and streamline their operations. But tread lightly – there are some pitfalls along the way that can expose digital identities to attack while landing your organization with hefty penalties for violating data security regulations and compliance requirements.

Human and Non-Human Identity Scale

As more organizations adopt cloud and hybrid on-premises networks, more digital identities are being created to navigate them, including:



“More” is perhaps an understatement – the number of accounts to manage is surging. In 2019, half of enterprises said they’d seen their identities increase more than five-fold in the previous decade.¹ In 2021, 80% of organizations said they’d seen them more than double², and 98% are still seeing consistent growth.³ 55% of CISOs, meanwhile, say that their identities have increased due to cloud and SaaS adoption. Hybrid working practices have also increased the number of endpoints and mobile devices being used to authenticate users around the world, as well as third-party identities (including partners, suppliers, and affiliates) working within corporate cloud networks.

The result? This explosion in the scale and variety of valid credentials has widened the attack surface. The more identities created, the more targets there are for attackers to exploit.

55%

of IT and security professionals say they’re concerned that managing data in the cloud is more complex than in on-premises environments.⁴

1. Dimensional Research, The State of Identity: How Security Teams are Addressing Risk, 2019.

2. One Identity, 2021 identities and security survey, 2021.

3. Identity Defined Security Alliance, Trends in Securing Digital Identities, 2022.

4. Thales, 2023 Thales Cloud Security Study, 2023.

Paralysis of Choice

This challenge doesn’t just apply to digital identities, but also the identity security solutions required to protect them. When looking to implement a new security tool, security teams must ask:

1. Will it integrate with existing tools and processes?
2. Will it provide value, and when?
3. Will it protect my multi-cloud and SaaS environment?
4. Is it affordable?

Implementing any new identity security tool can be tough, but even more so when it’s poised to change an organization’s high-level identity security strategy. And with so many solutions on the market to choose from, finding the answers to these questions can be overwhelming and lead to poor decisions – or no decisions at all.

Gaining Visibility

Cloud environment intrusions have increased by 75% year on year, and it takes around 120 days for organizations to detect cyberattacks in the cloud⁵. Faced with the sheer scale and complexity of cloud platforms and the sprawl of human and machine identities operating across them, many organizations lack the visibility needed to find out where they're at risk or exposed, who's attacking them, where attacks are taking place, or how to remediate them.

What reduces visibility?



Outdated tools and shadow IAM in cloud and SaaS

The cloud and SaaS apps are home to a diverse range of users, resources, services, and APIs – along with their associated privileges – which are continuously created and deleted, and rapidly scaled up or down on demand. Typical IAM solutions designed for traditional corporate networks (which host fewer, but more reliable identities) can't keep pace with these fast-evolving environments.



Disconnected, silos of tools

In the pressure to modernize their IAM processes, organizations can end up buying separate identity and access management tools from different vendors. In fact, the average enterprise uses 45+ security tools, creating data silos and gaps in visibility.⁵ But this tool sprawl doesn't offer a holistic security strategy that provides end-to-end visibility of digital identities across cloud infrastructure. The siloed approach leads to lack of context and risk understanding from system to system or tool to tool. Many tools do not integrate with each other or scale with cloud platforms. Instead, they can actually reduce visibility – blinding security teams with constant, contextless alerts and contrasting information, and worse, leaving them with blind spots they can't see or manage.



Lack of awareness

IAM is often left out of regular security operations. Nearly 50% of organizations aren't adequately staffed or funded for new IAM projects. Instead, many organizations hold faith in the security theater of traditional identity governance, access management, and XDR solutions, which provide an illusion of safety but expose them to risk and ultimately make it harder for IAM teams to enforce new identity-centric security approaches.⁶

5. CrowdStrike, Global Threat Report, 2024.

6. Schneier, Bruce, Beyond Security Theater, Schneier on Security, 2009.



Poor communication

Traditional IAM processes tend to isolate IT and security teams in silos, preventing them from responding to identity attacks quickly, communicating about potential threats, or properly allocating security resources. This is how identity attacks slip through their defenses undetected.

Defending Against Identity Attacks

Valid credentials are a top target for attackers today, with 80% of breaches now starting with compromised identities.⁷ For the first time ever, the identity attack vector became the most common entry point for cybercriminals in 2023, representing a 71% year over year increase.⁸

Why break in when you can log in?

Cybercriminals are targeting the login box. Rather than hacking systems, they're taking control of identities that grant access to critical resources. With valid credentials, attackers can bypass typical security infrastructure and access controls to breach networks, gain persistence, and operate undetected for months. From there, they move laterally across remote and cloud systems, escalate their privileges, and steal sensitive assets. Identity-based threats move quickly too – the average time for attackers to break out is down to just 62 minutes, from 84 in the previous year.⁹

7. IBM, X-Force Threat Intelligence Index, 2024.

8. IBM, X-Force Threat Intelligence Index, 2024.

9. CrowdStrike, Global Threat Report, 2024.

The identity attack surface is particularly dangerous because once a valid account has been compromised and bad actors are masquerading as legitimate users, it can be very difficult for security teams to identify suspicious activity.

Without the tools to provide end-to-end visibility of identity behavior, security teams may not notice insider threats operating within the vastness of their cloud networks until it's too late.

The cost of data breaches

90%

of businesses had an identity-related incident in 2023, with 68% suffering a direct business impact.¹⁰

Ransomware payments surpassed a record

\$1 billion

in 2023.¹¹

The average cost of a data breach reached an all-time high in 2023 of

\$4.45 million¹²

10. Identity Defined Security Alliance, Trends in Securing Digital Identities, 2023.

11. Chainalysis, The Chainalysis 2024 Crypto Crime Report, 2024.

12. IBM, Cost of a Data Breach Report, 2023.

Staying Compliant

Organizations are responsible for proving compliance with key cybersecurity regulations and frameworks regardless of which cloud or SaaS platforms they're using.

Although well-known regulations such as HIPAA, SOX, CCPA, and GDPR do not specifically cover the cloud, their terms for protecting sensitive data (including digital identities) are growing stricter – with hefty fines and penalties if organizations fail to do so. That's not to mention the risk of reputational damage.

Data security is a top concern for consumers today before deciding to trust a business.¹³ In 2022, 64% of organizations in the Americas were seeing more suppliers and customers ask for proof of compliance with data privacy regulations.¹⁴

However, the scale and complexity of cloud infrastructure makes it easy for organizations to lose visibility and control over their identities, and in many cases, this can translate to non-compliance. 55% of organizations say that data privacy and compliance are challenging in the cloud¹⁵, while 6 in 10 expect the risks of non-compliance to grow in future¹⁶.

As the cloud expands and organizations charge forward with migration without the right tools to cover their blind spots, they're putting themselves at risk. This is why they need to treat identity security in the cloud even more seriously than they would with on-premises networks.

How? By implementing identity-first security solutions that scale with the cloud to continuously perform (and automate) access reviews and audits, spot risk areas, and mitigate vulnerabilities quickly.

13. PYMNTS, Authenticating Identities In The Digital Economy, 2021.

14. KPMG, A triple threat across the Americas: 2022 KPMG Fraud Outlook, 2022.

15. KPMG, A triple threat across the Americas: 2022 KPMG Fraud Outlook, 2022.

16. Thales, 2023 Cloud Security Study, 2023

NIST CSF 2.0 – a sign of the times

Many cybersecurity regulations are increasing their scope. The National Institute of Standards and Technology (NIST), for instance, has revised its Cybersecurity Framework (CSF) for the first time since its creation in 2014 to keep pace with the current threat landscape. The framework now applies to all organizations – not only critical infrastructure – and includes a new core function called Govern which encourages organizations to integrate cybersecurity across all their operations.

There are two main takeaways here:

1. Cybersecurity and compliance should be everyone's concern across the organization
2. The best cybersecurity posture is holistic



Key regulations and frameworks with identity security requirements

Regulations

- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- California Consumer Privacy Act (CCPA)
- Service Organization Controls 2 (SOC 2)



Frameworks

- NIST CSF 2.0
- NIST 800-53
- NIST 800-171
- ISO 27001
- Cloud Security Alliance Cloud Controls Matrix
- Google, AWS, Microsoft – IAM best practices

Common requirements include

- ✓ Establish secure authentication features (including MFA)
- ✓ Rotate access keys and secure access policies
- ✓ Perform regular audits
- ✓ Secure digital identities and resources
- ✓ Continuously monitor networks for threats
- ✓ Identify and mitigate security risks
- ✓ Grant least privilege
- ✓ Establish strong internal controls and segment networks
- ✓ Prepare incident response plans
- ✓ Encrypt sensitive information
- ✓ Provide employees with security awareness training



Core Vulnerabilities in Modern Enterprises



Core Vulnerabilities in Modern Enterprises

An exposed cloud platform is a goldmine of sensitive data and resources for attackers. Here are several common weak spots that they can exploit to gain access.



Supply Chain Risk

Supply chain attacks have emerged as a significant vulnerability in the modern enterprise landscape. Bad actors inject malicious code into third-party software such as repositories, dependencies, applications, or even hardware components, which is then distributed to customers. This strategy allows attackers to compromise a wide range of targets simultaneously.

According to recent statistics, supply chain attacks have surged dramatically, with a 600% increase reported over the past year.¹⁷ This rise underscores the critical need for robust supply chain risk management and enhanced security measures across all levels of an organization's supply chain.

CASE STUDY



GitHub (2024)

Threat actors compromised multiple GitHub repositories by delivering malware within a popular Python package – an attack which, notably, affected Top.gg, a platform that provides bots for Discord's chat service.





Remote Work

The normalization of hybrid and remote working practices means that fewer employees are directly tied to their corporate network – they can authenticate and access applications from different countries and devices, including unprotected personal or mobile devices. This expanded attack surface extends beyond the control of company cybersecurity teams, increasing the risk of unauthorized access and data breaches.



Social Engineering

Social engineering attacks, which exploit human psychology to trick individuals into revealing sensitive information, account for 74% of all breaches.¹⁷ Techniques like phishing use fake emails, phone calls, website links, and voice messages to spoof users and harvest credentials.

CASE STUDY



MGM Resorts (2023)

Attackers from the threat groups ALPHV and Scattered Spider impersonated an MGM employee, calling IT service desk employees and tricking them into resetting the user's MFA factors. This allowed them to escalate their privileges, deploy ransomware, and steal sensitive data. The attack caused widespread disruption and likely cost the casino giant north of \$100 million.¹⁷

17. Zeba Siddiqui, Casino giant MGM expects \$100 million hit from hack that led to data breach, Reuters, 2023.

Authentication Mechanisms

Attackers target authentication processes that lack secure mechanisms such as multi-factor authentication (MFA) with brute force methods or by abusing stolen credentials purchased from the dark web. They can then cache these credentials after authentication to give them faster access to compromised accounts in future.



Password spraying

A brute force attack where attackers try a set of stolen passwords against multiple accounts to gain access without triggering lockouts.



Credential stuffing

An automated attack where stolen username and password combinations – usually obtained from online data dumps – are repeatedly entered into website authentication forms to try and gain unauthorized access to accounts.



MFA attacks

MFA is not failsafe. Though MFA forms an effective defense against attackers by separating them from the login box with knowledge, possession, or physical factors, there are still ways to intercept these factors and bypass it, including:

- **SIM swapping** – an attacker impersonates a user and convinces their mobile carrier to switch the victim's phone number to their own SIM card, allowing the attacker to intercept one-time SMS codes.
- **Prompt bombing** – using stolen credentials, an attacker repeatedly sends MFA requests to a victim hoping they'll accidentally approve one or do so out of frustration.
- **Adversary in the middle (AITM/MITM)** – attackers create false applications, networks, or websites that trick users out of their authenticated session cookies, which let them bypass MFA.
- **Help desk reset** – attackers trick help desk employees into resetting the MFA factors of legitimate employee accounts, allowing them to gain access.
- **Registration** – attackers register a new device to the victim's MFA account using stolen credentials to gain persistence.

Organizations need to understand these risks and employ identity threat detection and response (ITDR) tools and processes to detect and respond to such attacks in real time, ensuring robust protection against compromised identities.



**Microsoft
(2023)**

CASE STUDY

The Russia-affiliated threat group Midnight Blizzard used a password-spraying attack to compromise corporate emails and more starting with non-human identities first accessing a Microsoft test account that didn't have MFA enabled. Midnight Blizzard then compromised and duplicated a legacy test OAuth application connected to Microsoft's corporate environment, leveraging its privileges to access the Microsoft 365 stack and steal data from senior-level accounts. The attackers may have even stolen source code.



**Okta
(2024)**

CASE STUDY

In October 2023, Okta notified its customers about unauthorized access to Okta's support system. The threat actor got hold of Okta's customer HTTP archives (HAR), uploaded by customers, as part of open support cases. Active Okta session cookies were extracted from the compromised HAR files to gain unauthorized access to Okta's customer environments. The access to Okta's support system gained via a compromised Okta employee's laptop, enabled the attackers to gain access to the Okta tenants of 1Password, BeyondTrust, and others that we might not know about.



Ransomware

Ransomware has become a significant vulnerability for modern enterprises as attackers deploy malicious software that blocks access to critical data, such as personally identifiable information (PII), protected health information (PHI), or financial records. This malware effectively cripples an organization's operations, rendering essential systems and data inaccessible. Attackers then demand a ransom payment in exchange for restoring access, creating a severe operational and financial dilemma for the victim.

The impact of ransomware extends beyond the immediate loss of data access; it can disrupt business continuity, damage reputations, and lead to significant financial losses, either through the ransom itself or the cost of recovery and mitigation efforts. As such, robust security measures and incident response plans are essential to defend against and recover from ransomware attacks.

CASE STUDY



Change Healthcare (2024)

An attacker used stolen credentials to access one of Change Healthcare's remote Citrix portals which wasn't protected by multi-factor authentication. The attacker lay undetected in the system for nine days, stealing patients' PHI and PII, before deploying ransomware which shut down Change Healthcare's claims and prescription processes. The company paid a ransom of \$22 million to restore services.¹⁸ The attack, which affected a third of Americans, likely had a financial impact of over \$1 billion for the full year.¹⁹

18. Murphy, Tom, Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says, AP, 2024.

19. Capoot, Ashley, Cyberattack on UnitedHealth firm forces doctors to dig into personal savings to stay afloat, CNBC, 2024.



Unmanaged and misconfigured identities

Dormant or redundant accounts, often belonging to ex-employees, present another core vulnerability in the modern enterprise. These unmanaged and misconfigured identities are prime targets for attackers because the legitimate owners are unlikely to receive notifications of suspicious activity, and these accounts frequently retain privileged access permissions.

Legacy accounts may also lack up-to-date protections such as MFA, making it easy for attackers to gain initial access. Misconfigured accounts with excessive privileges can cause significant damage if exploited, either by malicious actors or through accidental misuse by employees.

CASE STUDY



Verizon (2023)

An insider threat at Verizon leaked the personal information of more than 63,000 people (mostly Verizon employees), including names, addresses, Social Security numbers, gender, union affiliations, dates of birth, and compensation information. The leak, which Verizon says was an accident, wasn't discovered for three months.²⁰

20. Kaur, Gagandeep, Verizon employee compromises personal data of 63,000 colleagues, CSO, 2024.



Non-human (NHIs) or machine identities

Managing non-human identities (NHIs) has emerged as a critical challenge in the modern enterprise due to the exponential growth in their number and complexity. With technological advancements such as cloud computing, DevOps, robotic process automation (RPA), the Internet of Things (IoT), and new generation AI, NHIs have become integral to seamless operations. These identities, which include API keys, service accounts, and machine credentials, now outnumber human identities by an average of 40 to 1.

This proliferation has significantly expanded the identity attack surface, making NHIs prime targets for adversaries who can exploit them to gain unauthorized access to sensitive systems and data.

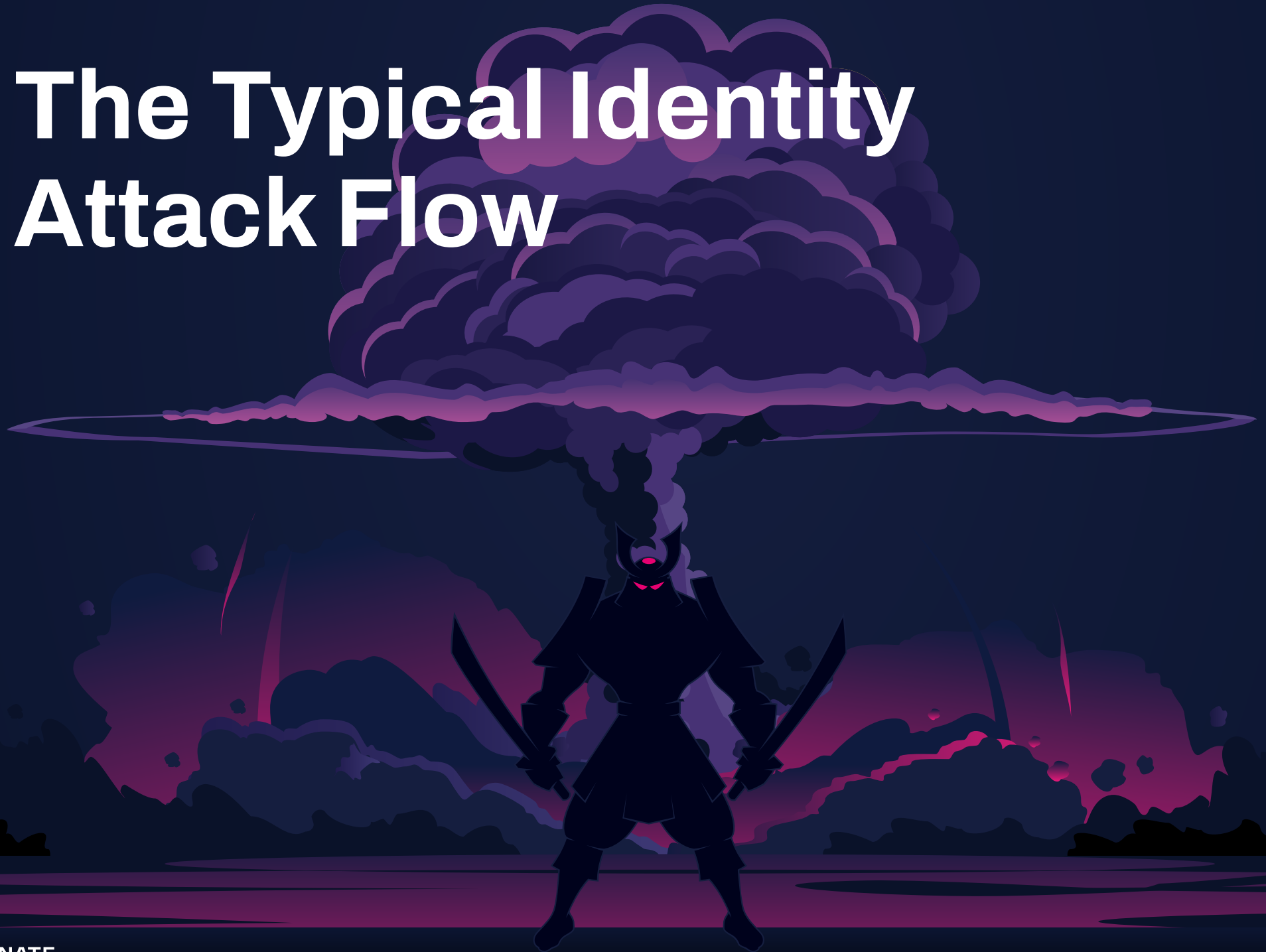
The significance of NHIs extends beyond security. Effective NHI management is vital for maintaining operational integrity, ensuring compliance, and optimizing the efficiency of an organization's digital and data endeavors. Compromised NHIs can silently facilitate intrusions, allowing attackers to navigate undetected through critical operations.

Addressing NHIs as first-class citizens in security and compliance strategies is essential. This involves answering crucial questions about access rights, origin of access, and methods for measuring posture and risk associated with NHIs. Ensuring that there are clear processes and tools for threat detection and response, alongside robust compliance measures, is crucial.

As businesses strive to build with confidence, reducing exposure time, minimizing audit findings, and maintaining operational functionality are paramount outcomes driven by effective NHI management.

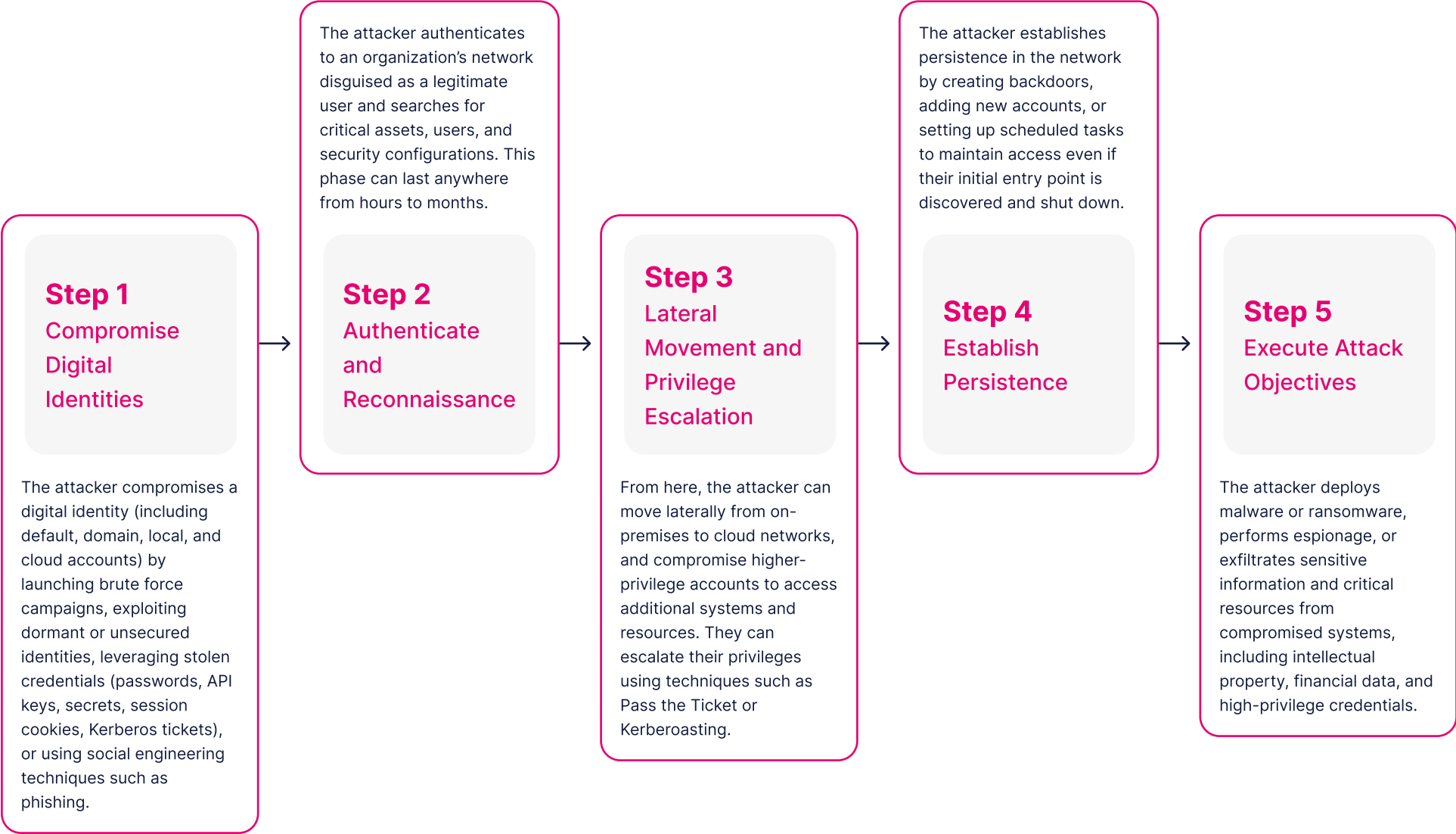


The Typical Identity Attack Flow

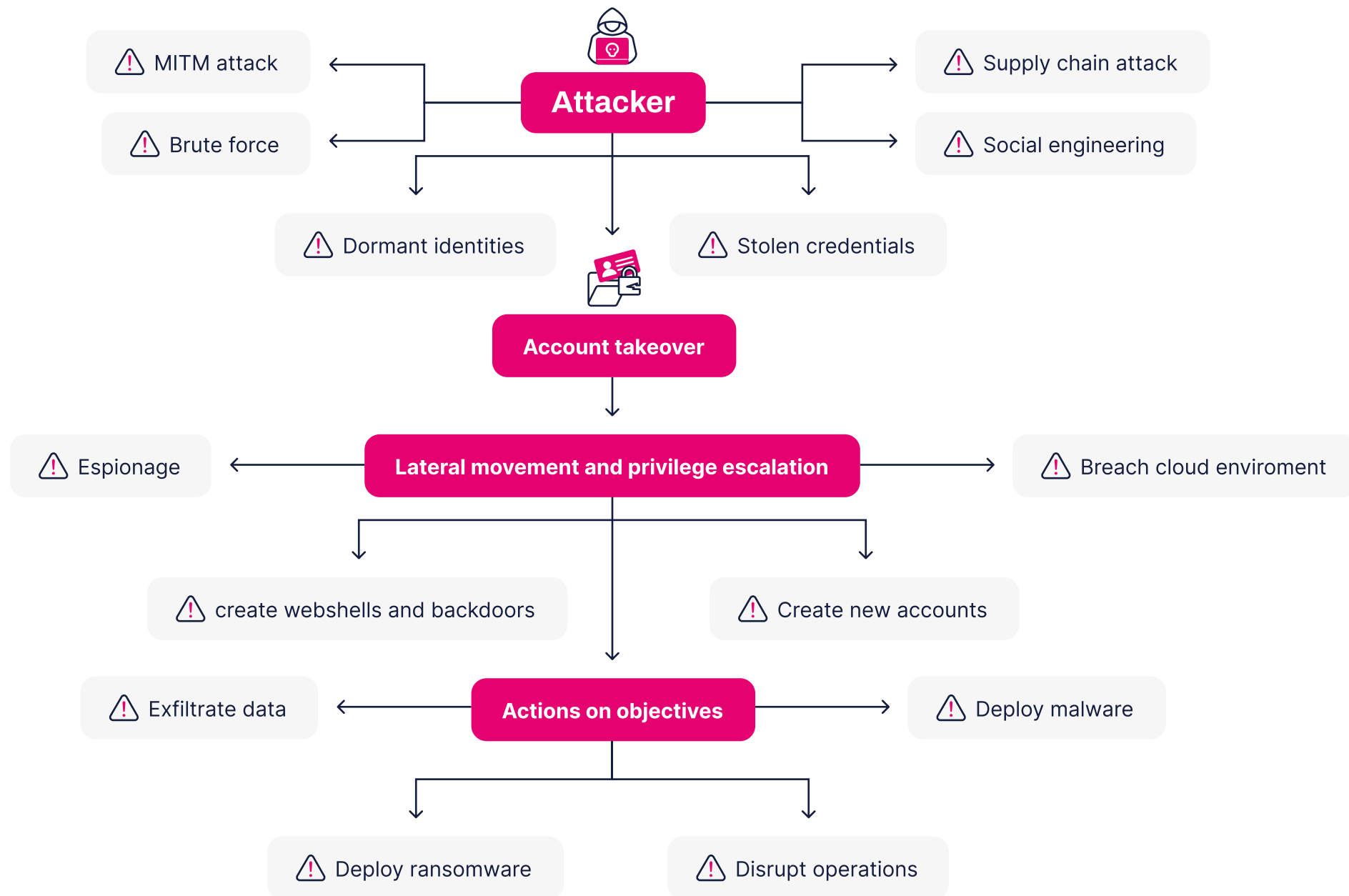


The Typical Identity Attack Flow

5 Steps



A Closer Look: An Identity Attack Flow



Fighting Back



Fighting Back

The cloud and its trust relationships are entirely different from the world of on-premises networks. But this doesn't make it unmanageable. With the right tools, strategies, and teamwork, the cloud can be made into a highly secure environment.

By implementing strong identity security practices, organizations can ensure that only authorized entities – both human and non-human – have access to critical systems and data. This includes enforcing multi-factor authentication, regularly auditing and revoking unnecessary permissions, and continuously monitoring for suspicious activities.

Ensuring the integrity of non-human identities, such as service accounts and API keys, is essential to prevent attackers from exploiting these entry points. Robust identity security measures can help contain the spread of malicious code introduced through supply chain vulnerabilities, maintaining the overall security posture of the organization.

A comprehensive approach to identity management must include regular audits and timely deactivation of dormant accounts, along with strict configuration controls to minimize the risk of exploitation.

What's Required?

Whether you're concerned about third party risk, supply chain attacks, remote workforce risks, social engineering hacks, ransomware, or non-human identities, modern identity security can provide greater protection for the entire identity attack surface.

To fight back against attackers, your organization needs to improve three things – visibility, speed, and control.

Visibility

If you can't see your identities, they're vulnerable. Cloud infrastructure is vast; it's complex, but with continuous, end-to-end visibility of all the human and machine identities across all of your cloud and on-premises networks, you can eliminate your blind spots. Good visibility can reveal whether your identities are logging in from an unknown device or location, operating with the wrong permissions, or accessing unfamiliar network resources – all key indicators of attack. Visibility helps you to:

- Understand context and risk profiles
- Proactively discover misconfigurations, over-privileged identities, toxic access combinations, dormant accounts, missing security controls (i.e., MFA), and more
- Measure and mitigate your identity blast radius

Speed

With visibility over your identity infrastructure, you can see threats coming. But how quickly can you detect and mitigate these threats before they cause serious damage to your system? Identity-based threats move quickly and so must you.

This requires you to have the right identity threat detection and response tools in place from the outset to block accounts, muster security teams, investigate threats, and rapidly shut them down.

With identity-centric security that works in real time you can:

- Detect risks and threats in real-time
- Respond to incidents quickly (and automatically)
- Enforce least privilege for zero trust

Control

Speed and visibility let you react to identity threats efficiently. But with control over your identity infrastructure, you can prevent these threats from surfacing to begin with and ensure your organization remains compliant with regulations at all times. The key here is covering your pre- and post-authentication attack surface with strong authentication mechanisms, strict trust relations, and continuous monitoring.

Having proactive control, you can:

- Employ zero trust and manage privileged access
- Monitor and control identity privileges
- Streamline compliance efforts





The Five Pillars of Identity Security

The Five Pillars of Identity Security

Let's break this down into an action plan. At Rezonate, we believe there are five main pillars that ensure a rock-solid identity security posture.

1. Authentication Controls

The login box is the gateway to your network and your first line of defense against attackers. Strong authentication mechanisms are also a key requirement in most cybersecurity regulations and frameworks. But traditional username and password combinations aren't strong enough to protect it anymore – you need to go beyond.

Action plan

Enforce strong MFA methods for human identities, and create a strict network-based authentication policy for your non-human/machine identities. This advice is given time and again, for good reason – many attacks start simply by exploiting identities that lack MFA.

Sometimes all that's needed is a single degree of separation to spot and shut down a breach. Clamp down on weak passwords too by implementing passwordless authentication where possible, rotating passwords regularly, and training users to avoid setting default passwords or reusing them across multiple systems.

2. Identity Hygiene

Given the scale of cloud infrastructure, it's easy for organizations to lose sight of dormant or redundant accounts, such as those belonging to ex-employees, third-parties, and machines that still provide access to their system. But attackers can exploit these identities to gain initial access and escalate their privileges to admin level. Or worse, they can take the fast train there by compromising unprotected identities that already have admin privileges.

Action plan

Don't leave the door open. Be proactive and automate identity security where possible. An identity-centric security solution can provide visibility into the behaviors, privileges, and risk profiles of your identities, as well as help you find and secure dormant or redundant accounts. This way, you can shut down potential attack vectors before threat actors catch the scent.

3. Observability

To detect and respond to identity threats as quickly as possible, as well pass audits and comply with regulations, you need a holistic view over all of your human and non-human identities. This includes the ability to track and monitor what they're doing in real time. And, you need a view to understand the entire blast radius to comprehensively address an attack.

Action plan

Implement a strong identity security solution that continuously monitors all your cloud, SaaS, and IdP platforms. This will enhance visibility over suspicious behaviors related to authentication and authorization processes, while providing actionable insights and analysis from multiple sources of data. Even better – choose a tool that offers automated remediation workflows and alerts features to speed up your identity posture and threat investigation and response efforts.

4. Least privilege

If attackers manage to authenticate, your security measures need to rapidly shift into gear and stop them from moving laterally within your network and escalating their privileges. Accounts that are bloated with excess privileges pose a serious risk to your organization – they can lead attackers directly to the heart of your network.

Action plan

Implement strong session policies and access rights to minimize the risk of unauthorized data exposure or breaches. Employ zero trust within your systems and establish least privilege across all your identities to restrict dangerous activity within your network. This will help prevent attackers from moving laterally and escalating their privileges to reach dangerous levels of influence.

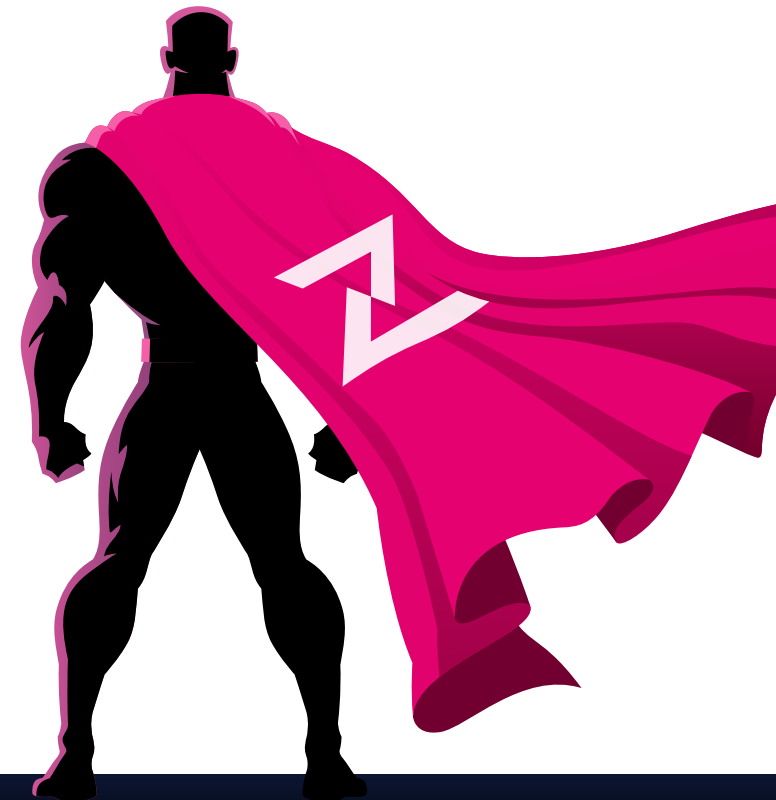
5. Identity security posture

Security starts with people, and so do data breaches. Identify risky behaviors and actions in your organization, including how your identities are being used on a day-to-day basis, as well as how they're being configured and controlled. This will reveal any blind spots or bad practices that may be compromising your identity security posture and help you promote a security-first work culture.

Action plan

An identity-centric security platform that offers a comprehensive view of the entire identity landscape and integrates preventative measures with access analytics and insights, compliance reports, risk assessment help to get an understanding of your current areas of risk. Having access to conduct microcertifications or in-line access reviews. Leverage a solution that offers both guided or automated remediation options prioritized by risk profiles to improve posture significantly, and quickly.

With actionable data, context-based threat information, and a unified view of the identity infrastructure, the right tools enable organizations to establish risk-informed policies and procedures confidently. This clear visibility into identity risks also aids in educating employees on best security practices, including strong password hygiene and awareness of modern phishing and social engineering techniques.

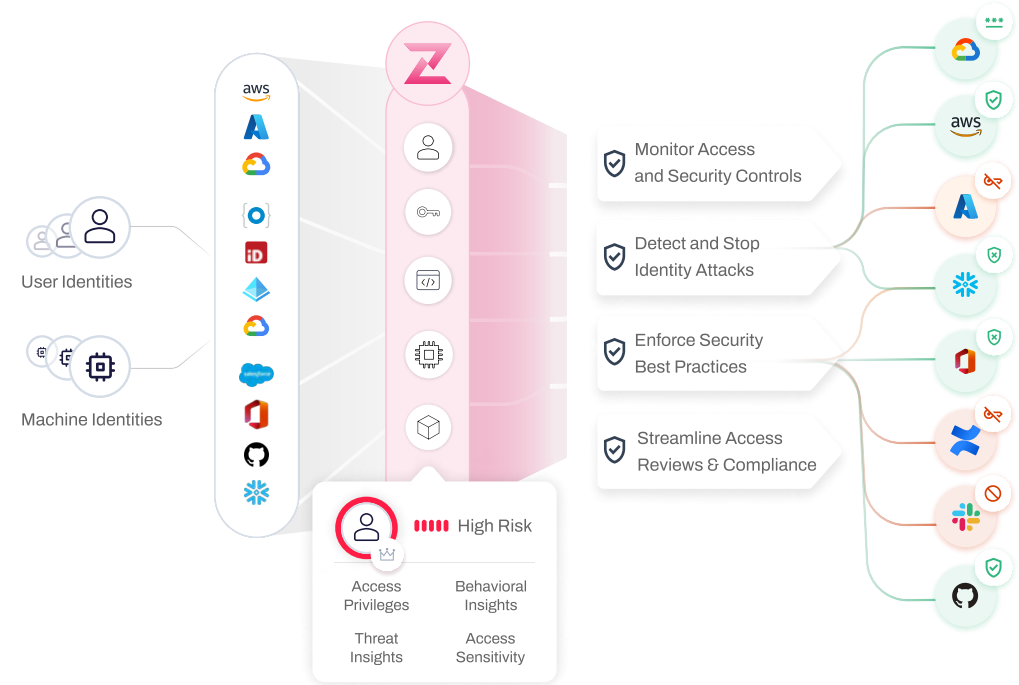


Boost Your Identity Security Posture with Rezonate



Boost Your Identity Security Posture with Rezonate

Rezonate helps organizations visualize and control their identity fabric from one central hub, offering tools and processes designed to detect, prioritize, and respond to identity threats in real time. We help organizations proactively identify their weak spots and tackle them before they become to security risks, leading to faster threat response times, more consistent audit trails, and total compliance across multiple cloud platforms.



Rezonate offers a unique blend of...

Identity security posture management

Continuous and automated monitoring of identity behavior across all cloud, SaaS, and IdP platforms, leveraging MITRE ATT&CK models to quickly mitigate security issues and block potential threats.

Identity threat detection and response

Real-time, risk-driven identity protection that detects and blocks identity attacks coming from outside or within your organization.

Identity and access compliance




Full visibility of your compliance status and risk areas, with suggested remediation actions to ensure you impress auditors every time.

How Rezonate Can Help

1. Risk Assessment

Manually keeping tabs on every human and machine identity across your entire cloud infrastructure would be an impossible task. At Rezonate, we offer a free, interactive risk assessment that gives you a bird’s eye view of your current identity security posture across all your cloud, SaaS, and IdP applications. This is a great first step in hygiene efforts.

Our assessment reveals how well you’re managing and securing your digital identities, helping you prepare for audits, plan investments and security projects, assess the identity security posture of new acquisitions, and sweep new identities and tools before you give them access to your system. It follows five main steps:

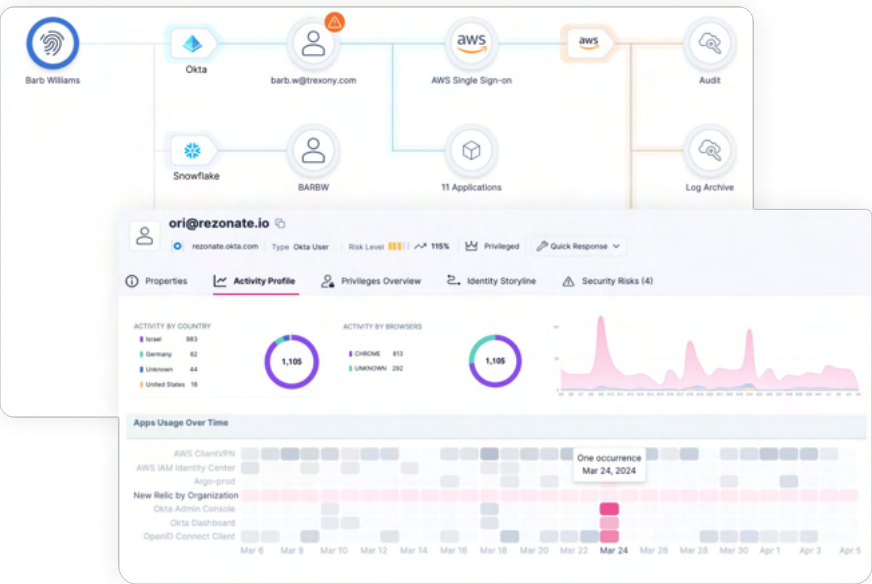
Issue Type	Exposure	Risk Level
>  Dormant Snowflake User	13	 13  0  0  0
>  Okta User Dormant SSO Access	27	 7  2  0  0
>  Dormant Okta Group	5	 5  0  0  0
▼  Dormant Google Workspace User	3	 3  0  0  0
   rezonate.google.com	Nov 30, 2023	                                             

2. Centralize Your Identity Visibility

Rezonate helps organizations manage their entire identity security strategy from one central hub, thanks to features such as:

Visual dashboard

Our platform provides a visual dashboard for real-time, end-to-end visibility across your entire identity infrastructure. From here, you can identify blind spots, set alerts and triggers on changes in configurations, access privileges, and activities, and automatically remediate risk areas before they evolve into data breaches.



Full integration

Rezonate aggregates and correlates identity data from across all your IaaS, SaaS applications and identity provider platforms. This means you can ensure strong multi-factor authentication (MFA) is enforced, spot risks and potential policy violations, prioritize hygiene efforts, detect and mitigate risks, and conduct behavior analysis without having to piece together insights from an array of disparate sources.

Continuous monitoring

Rezonate employs user and entity behavior analytics to continuously monitor human and non-human/machine identities – and their privileges – to spot suspicious or anomalous activity.

Rezonate's Identity Storyline is an innovative authentication and authorization graph that gives context to how your identities are behaving throughout their lifecycle. With an aggregated view, you can see all the granular privileges and activities your identities have across multiple systems to help uncover and reduce the blast radius of a compromised account.

Actionable insights

With detailed and actionable insights, Rezonate makes it easy to review identity privileges and security controls, remediate risk areas, and map to best practices including NIST CSF 2.0 or organizational governance policies.

Interactive reporting

Rezonate provides interactive reporting features that let you sort and filter data, review identity risk levels, activities, and alerts. This makes it easy to assess and improve your security posture, shut down identity threats, and prepare for audits.



3. Automate!

Security teams aren't always on hand to react to threats in real time. That's why automating your identity security with AI-powered tools will help ensure that your back is always covered. This will also help to ensure consistent compliance and remove bottlenecks when it comes to incident planning, response, and remediation.

Rezonate provides organizations with hyper-security automation to plan effective response and remediation strategies against everything from misconfigured accounts to nation-state-grade threats. Our tools ensure rapid threat monitoring and triggering, as well as response and remediation controls. Automation is always an option and can be implemented by each organization where they need it most.

The Rezonate platform automates:

- Real-time anomaly and threat detection, privilege escalation and lateral movement detection
- Response and remediation controls
- Risk reduction
- User access reviews
- Continuous compliance monitoring
- User guidance and playbook prompts

4. Apply ITDR across Your Entire Identity Fabric

Rezonate wraps your traditional IAM controls with ITDR to reveal suspicious identity activity and prevent unmanaged, misconfigured, or exposed identities from being abused by attackers. This way you can see how identities are behaving, what resources they're accessing, and whether they're under threat – or becoming a threat themselves – then respond quickly.

Rezonate's Identity Threat Detection and Response (ITDR) capabilities offer both active and passive responses to identity threats.

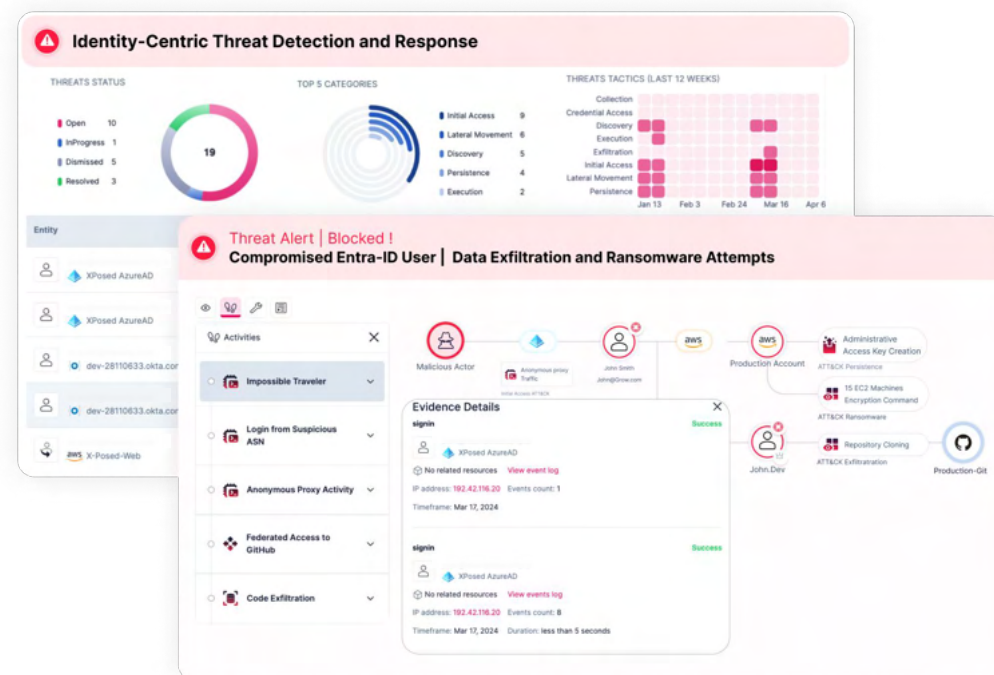
Active response

Rezonate can prompt step up authentication requirements and harden user accounts to mitigate threats in real-time.

Passive response

Rezonate provides guidance, integrates with third-party tools, and utilizes playbooks to inform and streamline the incident response process.

These comprehensive measures ensure swift and effective responses to identity-related security incidents, enhancing overall organizational security.



Typical IAM controls

Identity-centric security with Rezonate

Authentication

- Ensure your identities are covered with multi-factor and passwordless authentication across all cloud, SaaS, and IdP platforms.
- Integrate third-party security tools such as CrowdStrike to secure your endpoints.

Authorization

- Enforce least privilege and zero trust frameworks.
- Utilize machine learning, threat intelligence, and UEBA to track unusual or suspicious user activity across activity logs, cloud services, networks, and endpoints.

Administration

- Improve end-to-end visibility of your identity security infrastructure.
- Give CISOs visibility over your organization's security strengths and weaknesses.
- Receive alerts about potential threats and automatically deploy countermeasures.

Auditing and reporting

- Continuously assess your compliance levels.
- Centralize your identity monitoring, administration, documentation, reporting, and threat detection and response.
- Create better incident response strategies and playbooks for tackling identity threats and minimizing operational downtime.
- Confidently allocate resources and budgets for new security tools and projects.

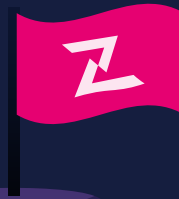


Identity security hygiene best practices

Identity security hygiene best practices

- ✓ Choose one identity-centric security solution to protect your identity fabric and integrate with existing platforms
- ✓ Implement multi-factor and passwordless authentication where possible
- ✓ Conduct a risk assessment with Rezonate
- ✓ Automate your threat detection and response capabilities
- ✓ Educate employees on best identity security practices, including password hygiene, social engineering awareness, and secure remote working
- ✓ Continuously evaluate your progress and set goals for improvement
- ✓ Encourage a zero trust mindset among staff – especially leadership
- ✓ Establish safe reporting methods for insider threats
- ✓ Identify and prioritize your regulatory compliance goals
- ✓ Draw up a plan for quickly and efficiently assigning privileges, segmenting networks, and provisioning/deprovisioning identities
- ✓ Sweep your on-premises and cloud networks for dormant or redundant identities
- ✓ Introduce new third parties and vendors to your network in predefined security phases
- ✓ Build a roadmap for your IGA strategy that takes into account staff, stakeholders, and tools
- ✓ Implement a layer ITDR across your current IAM processes
- ✓ Automate the de-provisioning of inactive identities
- ✓ Remove SMS as an MFA factor to help protect against SIM Swap attacks
- ✓ Standardize your auditing, compliance, and reporting capabilities
- ✓ Apply extra security measures to third-party identities
- ✓ Consistently review privileged accounts and adjust their permissions in line with current job responsibilities

Next Steps



Next Steps

Digital identities are your organization's most critical assets, and attackers know it. By compromising valid credentials, they're able to exploit unmanaged cloud platforms and overburdened security teams, remain undetected for longer, and breach corporate networks from within, disguised as legitimate users.

Unfortunately, many organizations are adrift in the cloud. They don't have the tools to grapple with its scale and complexity, and this means that they can't see their digital identities; they don't understand how their identities are behaving; and they're unable to distinguish friend from foe. Without this crucial level of visibility, organizations are inadvertently exposing their data, systems, and processes while risking costly data breaches, regulatory violations, and reputational damage.

This is why traditional IAM doesn't cut it anymore. Security teams need to embrace a more secure, identity-centric approach. This involves wrapping your identity governance strategy with a protective layer of ITDR and ISPM to continuously map your organization's security posture, identify risk areas, and rapidly remediate threats – all while remaining compliant with today's strict cybersecurity regulations. By making digital identities the centerpiece of your security posture, both pre- and post-authentication, you can detect and respond to incidents before they escalate.

Our platform provides continuous visibility over the permissions, access paths, and activity patterns of your human and non-human identities, helping you identify weak spots and detect, prioritize, and respond to incidents in real time. From risk assessments that provide an eagle eye over your current security posture, to our suite of granular and automated tools designed to centralize your identity visibility, streamline reporting and compliance, and bring all IT, IAM, and security teams together under one umbrella, Rezonate can help turn your organization's most critical asset into its safest one, too.



Get started today!

[Learn more at rezone.io](https://rezone.io)

Appendix

Appendix

List of acronyms

Acronym	Definition
CIEM	Cloud infrastructure entitlement management
IAM	Identity and access management
IdP	Identity provider
IGA	Identity governance and administration
ISPM	Identity security posture management
IT	Information technology

Acronym	Definition
ITDR	Identity threat detection and response
MFA	Multi-factor authentication
PAM	Privileged access management
PHI	Personal health information
PII	Personal identifiable information
SaaS	Software as a service
UEBA	User entity and behavioral analytics
XDR	Extended Detection and Response

REZONATE