Less cloud identity stress

Discover how Expel MDR for AWS reduces the stress of securing identity and access management (IAM)—and lowers risk in your cloud environments.

Table of contents

CLOUD CHALLENGE

Just another day in the life

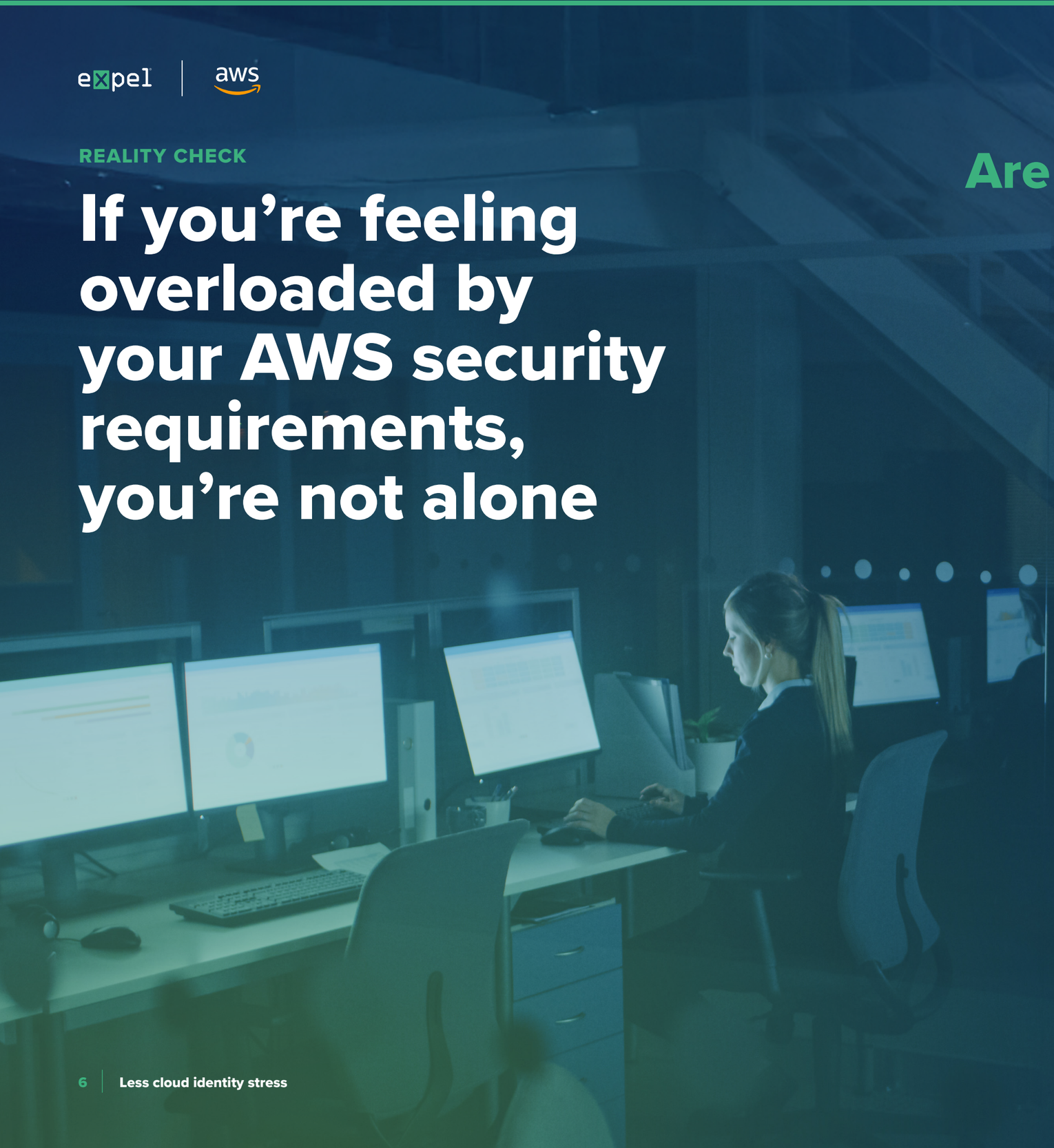
As your cloud footprint expands and security demands mount, your teams must have the expertise to distinguish between business as usual, versus a threat to business. At the heart of protecting your environment sits identity and access management (IAM).

Strong IAM is essential: It scales with your business, protects your data, and ensures only the right people have access to critical systems. It's the foundation for implementing zero trust, defending against threats, and maintaining security across every cloud.

It’s not just about security, it’s about business confidence. By implementing robust IAM you’re safeguarding your operations—and your reputation.

REALITY CHECK

If you're feeling overloaded by your AWS security requirements, you're not alone



Are you...

Confused?

You're managing incredibly complex multi-cloud and hybrid environments, which comes with a slew of new skill requirements, like specialized AWS security knowledge, and the ability to keep up with ever-changing threats.

Anxious?

You have growing concerns about vulnerabilities, the privacy of data, and compliance fulfillment. Worries that "low and slow" attacks like cryptojacking and data exfiltration are operating under all the alert noise are more common than ever.

Fatigued?

You're inundated with alerts across multiple AWS accounts and regions, and there's no capacity to see every alert or prioritize what matters most. Not only do false positives muddle the threat trail (making real-time remediation impossible) security control configurations and updates are giving you the runaround.

Overwhelmed?

Too busy chasing "fires," you're finding it increasingly harder to take a proactive stance or improve MTTX metrics. This bleeds into your ability to build security team expertise, as time is focused on reactive management instead of skill development.

PROBLEM SOLVED

Expel MDR for AWS addresses IAM threats

THREAT #1

Lack of granular tracking and visibility

- Distributed logs and varying interfaces make it increasingly difficult to track IAM activity across multi-cloud environments
- Every cloud provider has unique IAM tools and configurations
- A pass for a security audit may not be possible without demonstrating proper visibility into API calls, or IAM controls and tracking
- Inadequate visibility makes it harder to detect and respond to unusual or inappropriate user actions or unauthorized activities

86%

The amount of cloud infrastructure incidents in 2024 that impacted AWS

How we strengthen AWS IAM

Have no fear, we integrate easily with leading IAM tools and are constantly tuning your detection rules. With monitoring centralized in a single interface, we cross-correlate activity across the tech stack and see gaps quickly.

Automated enrichments use machine learning to add context to your alerts, which means our security analysts can identify risky events, like discovering the original user at the end of role-chaining, and respond even faster.

THREAT #2

Credential (or secrets) exposure

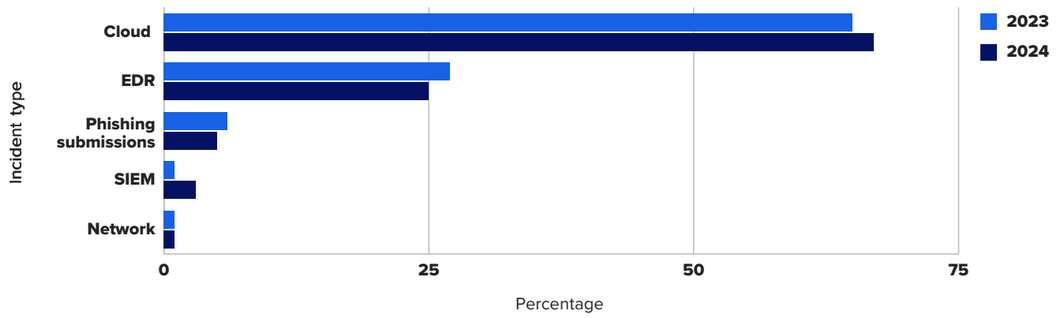
- Hard-coded credentials, exposed API keys, or insufficient rotation policies lead to credential leaks
- Disparate devices and access points add more risk and increase cloud-related incidents
- Threat actors can exploit exposed credentials for unauthorized access

How we strengthen AWS IAM

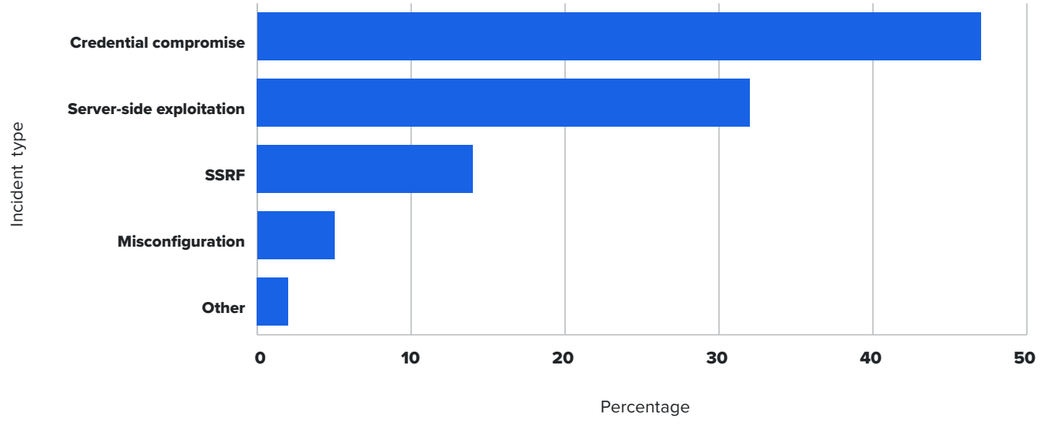
Providing 24x7x365 monitoring, we're up all the time to protect your network.

Our process delivers Resilience Recommendations and Remediation Steps to remove, rotate, and reduce permissions—along with resolving IAM issues. We can also create custom AWS detections around exposed "secrets."

Cloud resources provide the highest number of leads to identify malicious activity



Cloud infrastructure incident types in 2024



THREAT #3

Rising alert volume

- More and more dynamic, ephemeral resources and non-human identities to keep track of
- Added noise from service-to-service communication, including variables disappearing, or scaling up and down quickly
- Increase in users and machines assuming roles to perform actions

How we strengthen AWS IAM

With automated filtering and enrichment of raw logs, we collect insights to reduce false positives, and deliver auto-remediations against threats.

MDR also covers Kubernetes, the standard for managing containerized workloads, to demystify this potential attack surface. That includes filtering out the noise and detailing findings by cluster, severity, and title, so you know exactly what needs your attention.

THREAT #4

Evolving IAM threat vectors

- Attackers are increasingly targeting cloud IAM misconfigurations and vulnerabilities, and it's not stopping anytime soon
- Data and documents continuously travel to and from the cloud, creating more opportunities for ransomware, hyperjacking, and hypervisor infections
- Playing catch up with bad actors to figure out the cause of issues and how to resolve them wastes your valuable time

How we strengthen AWS IAM

We offer hypothesis-based threat hunting services to uncover unusual logins, patterns, user behaviors, and more, addressing undetected risks across environments.

Additionally, Expel Threat Intelligence—a combination of our own research, OSINT, and history with customer networks—helps us assess emerging attacks and ensure protection against new threats.

67%

The amount of incidents targeting cloud for all incidents in 2024, up 2% from 2023

TRANSFORMATION

Level up your IAM and be more...

Confident

Gain clarity through the consolidation and centralization of your operations. We help you make the most of your current tech stack—across cloud and on-prem—by integrating with your existing technologies. Our personalized solutions always fit into your world without disrupting it.

Purpose-built for the cloud

Deep integration with AWS, and expertise in building out detections, means greater confidence in any of your cloud security initiatives—especially the strengthening of your IAM.

Assured

Stay ahead of threats with proactive detection and response. Our team of analysts specializes in AWS security to ensure comprehensive protection of your cloud infrastructure.

Any time, anywhere

Connect with your dedicated Expel SOC team instantly through Slack or Teams, whenever you need us.

Focused

Whether sorting through alerts for suspicious login activity, privileged account misuse, or even policy violations, reduce alert fatigue through data correlation and issue prioritization.

24x7x365 support

Expel's SOC analysts triage alerts on your behalf, and provide you with actionable remediation steps. Our MDR approach seamlessly integrates with your operations, reducing your MTTR to 20 minutes for high-critical alerts with auto-remediation.

Empowered

We seamlessly integrate with your organization, offering complete visibility and flexible collaboration. Our AWS experts complement your in-house staff, providing deep insights without expanding headcount.

More is possible

With enhanced support capabilities at your fingertips, free up your internal resources to focus on what matters most.

IAM secured

With a unified view across AWS environments and the support of managed detection and response, it's never been easier to safeguard IAM—a cornerstone of cloud security.

Schedule a demo →

Source: *Expel Annual Threat Report 2025*