expel

Same playbook, different year

What attackers still get away with—and what to do about it

A snapshot of Expel's **2026 Annual Threat Report**. For the full version, visit **expel.com/2026atr**.

Welcome to the executive snapshot of our Expel 2026 Annual Threat Report

Greg Notch
CSO, Expel

If there's one thing 2025 made clear, it's that speed matters more than ever—and I don't just mean how fast threat actors move.

The gap between detecting a threat and actually doing something about it is where breaches happen. We saw it play out across our customer base all year: Many intrusions succeeded simply because the "basics"—like multifactor authentication (MFA) or proper configurations—weren't fully optimized.

This year's report digs into the data behind nearly 1 million alerts. You'll see how identity remains the primary attack surface, and which endpoint and cloud threats continue to evolve. But beyond the numbers, you'll find practical insights from our analysts who handled these threats in real time. What worked. What didn't. What you can do about it.

We're sharing this because cybersecurity is a team effort. The more we learn from each other's experiences, the harder we make it for adversaries. We hope this report helps you head into 2026 with clearer direction and fewer unknowns.

One year. A million alerts. Here's what we found.

To defend yourself against a determined adversary, you have to know their weapons and targets. Expel's position on the cybersecurity front lines gives us a unique vantage point into the threats and attacks our customers face. The data we gather helps us deepen our insight, refine our tools and methods, and provide better protection in a constantly changing threat environment.

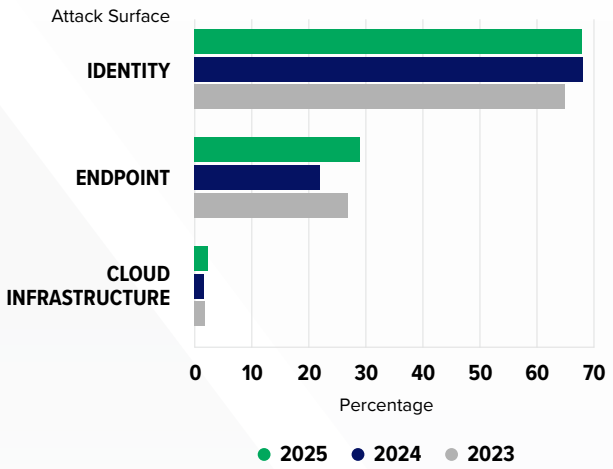
Each year, the Expel Annual Threat Report provides in-depth findings based on our work defending customers. This brief will reveal the most-important trends and developments from the 2026 report so you can better align your budgets, strategies, and tactics with the threats you face today.

Early detection—fast response

In 2025, our security operations center (SOC) triaged nearly 1 million alerts generated in our customers' environments across every major attack surface. And we investigated tens of thousands of incidents. Most of these incidents fall into three categories:

- **Identity-based attacks** using stolen user credentials and authentication tokens
- **Endpoint attacks** like malware, hands-on hacking, and server-side vulnerability exploitation
- **Cloud infrastructure attacks** targeting technologies including Amazon Web Services (AWS), Amazon Elastic Kubernetes Services (EKS), Google Kubernetes Engine (GKE), and Google Cloud

EXPEL SOC INCIDENTS, 2023-2025



Identity-based incidents continue to outpace other attack surfaces, but a growing share target endpoints and cloud infrastructure.

Wherever attackers strike, early detection and fast response are equally essential to stop threats before damage can spread. The detections we write help us shut down nearly two-thirds of observed incidents early in the kill chain, enabling us to more effectively contain threats before attackers can achieve their objectives.

Our early detection capability is complemented by the speed of our auto remediation features, which enable our SOC to achieve a current mean time to respond (MTTR) for high and critical incidents with auto remediation of just 13 minutes.

Go deeper with the full Annual Threat Report: **expel.com/2026atr**.

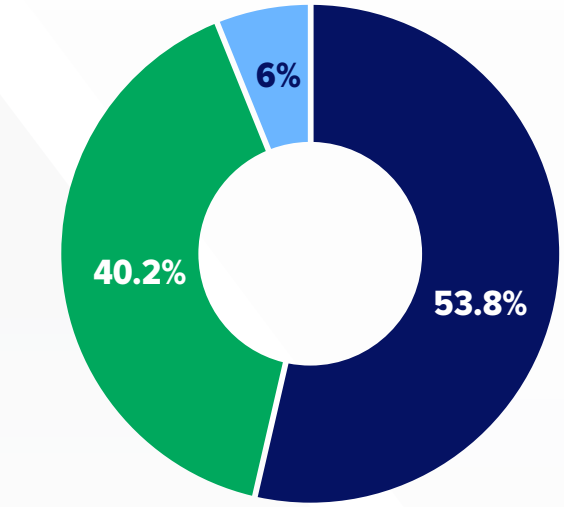
IDENTITY

Attackers don’t break in. They log in.

In just over half of the identity-based security incidents we saw in 2025, access was denied. Attackers had tried to log in using valid credentials, but existing security controls blocked them based on factors such as login location or device used. In cases like these, security teams should investigate the account used and take steps to prevent further abuse in the event the attacker has found a way around relevant security policies.

Even with security controls stopping the majority of illicit login attempts, attackers frequently managed to gain access. A few cases led immediately to malicious activity, such as registering a new multifactor authentication (MFA) device or accessing data. But such outcomes were relatively rare. However, the absence of immediate abuse shouldn’t be taken as an all-clear. A seemingly benign illicit login can be part of a sophisticated phishing technique known as an adversary-in-the-middle (AiTM) attack. This maintains an active session for the attacker to use and control later. To prevent further exploitation, the security team must act quickly to revoke the session and reset the credentials.

VALID CREDENTIAL USE IN H2 2025



A successful login using stolen credentials is an urgent threat, whether or not malicious activity has followed.

Learn about the growing role of phishing-as-a-service (PhaaS) in identity-based attacks in the full Annual Threat Report: **expel.com/2026atr**.

FIELD NOTES

James Shank
Director, Threat Operations

IDENTITY

A solved problem?

In many pursuits, the problems that arise in the operational day-to-day aren't new and aren't unsolved problems. They are normal, routine, or ordinary problems. Most problems aren't new discoveries—they're gaps.

For the last several years, identity-related compromises have been one of three top contenders for initial access vectors. Why hasn't it been solved?

The truth is, most of these identity compromise situations do have solutions aligned towards them. The technology itself isn't the gap—the gap is the lack of technology implementation.

Take password exposure, for example. How long have there been strong password storage solutions? Another example: MFA being bypassed through SIM swapping. Where were the passkeys or OAuth 2.0? And another: sign-ins using stolen cookies. What about behavior monitoring, geo-location checking, and device-bound session credentials (DBSC)? (To be fair, DBSC hasn't fully rolled out.)

Technology currently exists to solve these problems and to fill these gaps. However, it's often *not* in place because security has to fight for resources against competing business interests.

Risk mitigation considers impacts and likelihoods—both inside and outside cybersecurity. In reality, most companies are at higher risk of not knowing where their next dollar comes from than they are of falling to an identity compromise. We don't live in an ideal world, where security teams have every tool they need. Hence, our teams must focus on the basics to reduce impacts and must sometimes *compromise* (pun *definitely* intended) and do the best we can with the resources present.

Learn about the latest identity-based attacks and countermeasures in the full Annual Threat Report: **expel.com/2026atr**.

FIELD NOTES

Josh Carter
Manager, SOC Operations

Identity alerts in action—identifying and stopping them

Identity alerts are strong indicators of attackers attempting to gain access to an environment. We know that detecting and stopping these login attempts are critical to preventing further reconnaissance, persistence, lateral movement, and post-exploitation activities from happening. This past year, 68.6% of all incidents reported by the Expel SOC were identity-based. Let's dive deeper into what these incidents were, and how we as a security community can get ahead of the adversary and use our existing tools to stop these attacks from happening.

One of the easiest ways to identify suspicious logins is by either adding approved (or "expected") geographic locations to allow lists or blocklisting unapproved (or "unexpected") geographic locations. If you're an organization that works within a specific geography, this is a pretty easy task to undertake using your existing security tools.

Incidents involving a suspicious location accounted for 12% of identity incidents in 2025. However, it's worth noting that if you are a larger enterprise, hire contractors from outside your geographical region, and/or have employees who travel to other locations, you can open yourself up to lots of false positive alerts. If you're writing your own login detections, make sure to consider factors such as acceptable VPN usage, active sessions, and user agents.

Speaking of user agents, Axios user agents continue to be strong indicators of attacker activity. This past year, 9.5% of incidents were identified simply by a login attempt from an Axios user agent. So if you know that Axios isn't something your organization uses, consider adding conditional access blocks for that user agent.

Of course, known malicious indicators are always great ways to quickly identify attacker activity. Expel's **Threat Intel** and **Threat Hunting** teams work in tandem with the SOC to create new detections based on real-world, in-the-moment attacker behaviors. Last year, Expel identified 2% of incidents with detection rules written by the Threat Intel and Threat Hunting teams. As a security team, we shouldn't wait until we're under attack from the latest and greatest cyber threats. We need to learn from others and share what's happening to understand the tactics and techniques being used in new campaigns *now*.

Finally, phishing emails continue to be the primary tools used by attackers to trick users into handing over their credentials. Of incidents last year, 12% were attributed to successful phishing attacks. Employee training continues to be the number one way to fight social engineering techniques. However, adopting additional tools to mitigate phishing attacks will help when a human inevitably makes a mistake.

ENDPOINTS

Malware doesn't always look like malware

While many sensitive files and data have moved to the cloud, servers and user endpoints remain prominent targets—most often, for attacks involving malware.

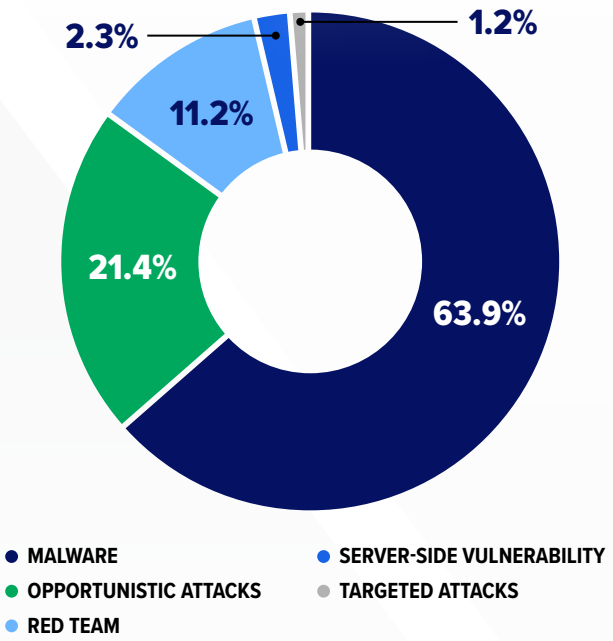
In one piece of good news, law enforcement scored a major victory against Lumma, formerly the overwhelming favorite infostealer of cybercriminals. This led to a steep drop in its use against our customers, but criminals are seeking alternative infostealers, such as Vidar and StealC.

Fake PDF editors continue to be a major problem. Once run by unsuspecting users, they can install backdoors, hijack users' browsers, access stored credentials, execute arbitrary code, intercept sensitive information, and download arbitrary payloads.

The ClickFix tactic accounted for more than one-third of all of 2025's malware-driven incidents. Here, attackers trick the user into executing a malicious script on their own system, often by completing a bogus CAPTCHA or following offered instructions for fixing an issue.

Unlike attacks targeting a particular target or sector, opportunistic attacks take advantage of general weaknesses wherever available, whether through portscanning, remote access tool usage, or actor commands from a compromised asset. These attacks are mostly detected only after the attacker has gained control of the endpoint.

THREATS TO ENDPOINTS



Malware and opportunistic attacks account for the majority of endpoint detections.

Incidents involving server-side vulnerabilities account for a relatively small share of our detections. But they can be quite serious, allowing attackers to compromise systems and gain network access.

Finally, there are incidents that don't involve criminals at all. Here, when we notify the customer, they inform us they were performing "red team" security exercises to test the resilience of their environment.

Learn about 2025's most commonly seen server-side vulnerabilities in the full Annual Threat Report: **expel.com/2026atr**.

FIELD NOTES

Jake Downie
SOC Analyst

PRODUCTIVITY TROJANS

Stop downloading free PDF editors (please)

Please, for the love of SOC analysts like me, make sure your employees stop downloading free PDF editors.

Here's a story. Sue receives a form from her boss that needs to be filled out and sent to a client ASAP. The only issue is that her job doesn't provide licensing for a PDF editor. So she goes looking for a free PDF editor online.

She has so many options. PDFast, PDFSkills, or even SupremePDF. Sue wants only the best, so she clicks on a link to download SupremePDF. The program installs, and she uses it. The software works enough for her to edit the form and ship it off without terribly inconveniencing her or her boss.

What Sue doesn't know is that SupremePDF is just a disguise used by malware to maintain a persistent hold on your system. Some days later, the security team is alerted to an attacker laterally moving on their network and stealing data. Tracking the source leads them right to Sue's machine. She tells them that she didn't click on any phishing links or give scammers access to her computer over the phone, so it couldn't have been her. Sue is informed that the PDF editor she downloaded was secretly malware that allowed the attacker access to her computer, and only used the ability to edit PDFs as camouflage to lull her into a false safety.

Now, this specific story is fictional; however, this scenario is not uncommon and happens more and more as attackers realize what an effective attack vector this really is.

These "PDF editors" are actually trojans, which use their safe-looking outer shell to establish a foothold on your endpoints. The malware maintains persistence, making sure that the software creates a service that runs on the endpoint, keeping the PDF editor running. We often see these editors then used as a backdoor to run malicious code on the host, commonly abusing encoded PowerShell to download a second payload.

These editors pose a significant risk. When they are initially downloaded, they usually don't raise a "red flag" from an endpoint detection agent, as these files are usually signed and do not *yet* have a record of malicious behavior.

This software family is so appealing to users because PDFs are common in daily work and many companies don't have enough legitimate PDF editor licenses for all employees. Users who only occasionally need to edit a PDF often lack a license and don't want to ask for one. Making matters worse, software like this is also usually shared with coworkers through word of mouth and can commonly infect several machines at once, creating a ticking time bomb for your environment.

TL;DR, if your company's employees don't know that these applications are dangerous, you should let them know. Today.

CLOUD INFRASTRUCTURE

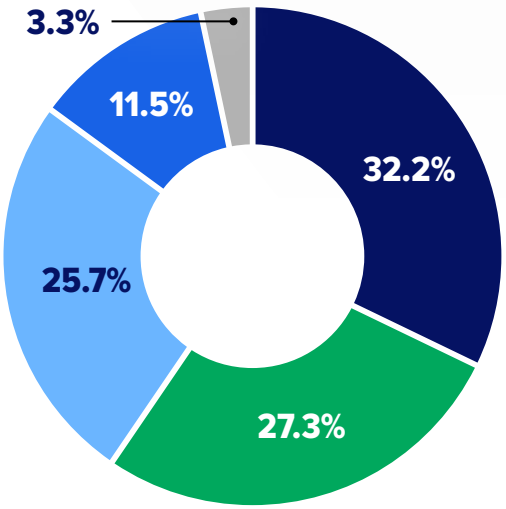
Red teams and red alerts

Red-team testing—a vital element of cybersecurity—accounted for more of our observed cloud infrastructure incidents than any other category. These simulated attacks covered a wide range of cloud technologies, as well as many types of activities, from server-side request forgery (SSRF) to access management breaches. The latter is especially important, helping companies understand risks such as overprivileged accounts and cloud misconfigurations.

Among genuine attacks, exposed cloud secrets were a frequent factor. These included API keys, passwords, encryption keys, and certificates. A majority of these incidents involved TruffleHog, an automated secret scanning tool. Secrets are also commonly exposed through supply chain attacks designed to expose credentials stored in a workflow's logs.

The emergence of the Shai Hulud 2.0 worm at the end of 2025 introduced a new twist by weaponizing the "trust layer" of the software supply chain. The worm scans environment variables and local config files for cloud credentials. Then it uses these to inject malicious GitHub Actions workflows into existing repositories. This provides the attacker with a permanent backdoor in the build pipeline, exfiltrating new secrets every time code is pushed.

THREATS TO CLOUD INFRASTRUCTURE



Misconfigurations and stolen secrets compromise cloud infrastructure.

See how cryptominers are hijacking targeted devices via cloud misconfigurations in the full Annual Threat Report: **expel.com/2026atr**.

Better detections. Faster responses.

Alert fatigue can be a SOC's worst enemy. When security tools produce more notifications than overworked analysts can field, a real threat can easily slip through. This is a common problem with one-size-fits-all detections that prioritize breadth over depth.

We designed Expel's detection framework to counter this issue. While we ingest alerts from hundreds of tools across a wide range of vendors, our additional detection logic enhances signal quality, coverage priorities, and responsiveness by:

- Evaluate potential threats through contextual risk factors.
- Elevate low-severity alerts that we know tend to trigger during an event.
- Combine low-fidelity alerts that, taken together, are prone to indicate nefarious activity.
- Cross-reference events across vendors to identify unusual activity.
- Write our own detections for activities we've witnessed.

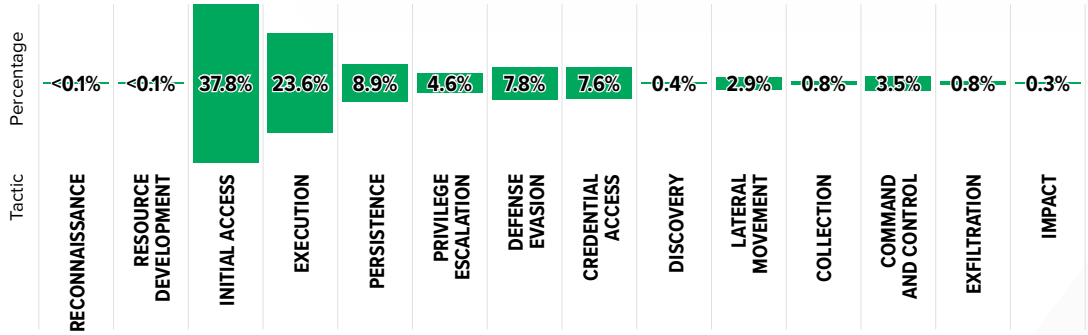
DETECTION SOURCE

Expel's custom and enriched detections deliver more true positives than traditional vendor tool detections.

Moving up the kill chain

The earlier you catch an attack, the greater the possibility you contain it before real damage occurs. A majority of our incident detections in 2025 came during the initial access and early execution phases, before attackers had a chance to exfiltrate sensitive data or deploy ransomware. By combining high-fidelity detections and early-stage threat detection, we help security teams spot and stop real threats faster.

INCIDENT ALERTS BY MITRE ATT&CK TACTIC



Expel detects 62.4% of attacks in the initial access or execution phases.

Get additional cybersecurity insights, recommendations, and predictions from the Expel SOC in the full Annual Threat Report: **expel.com/2026atr**.

Resilience checklist for 2026

Building on the findings of the Expel 2026 Annual Threat Report, these concrete steps can help you better protect your environment in the year ahead.

IDENTITY

- ☐ Strengthen protection for the most-critical and highly privileged accounts through conditional access policies for authentication.
- ☐ Reduce the risk of phishing with policies and tools such as:
  - Secure email gateways
  - Authentication audits and assessments
  - MFA based on the FIDO2 standard
- ☐ Task red teams with auditing your identity security controls to identify weaknesses and reveal the blast radius of a compromised account.
- ☐ **For Expel customers:** Enable account disablement as an auto remediation action to help us quickly contain identity-based incidents.

ENDPOINT

- ☐ Disable the use of the Windows Run hot key (Windows + R), which is used in the majority of ClickFix attacks.
- ☐ Ensure employees have official means for downloading approved applications to prevent fraudulent downloads.
- ☐ Block unwanted applications with whitelisting and Application Control for Windows.
- ☐ Block remote management tools that aren't expected in your environment.
- ☐ **For Expel customers:** Enable the "contain host" auto remediation for a faster response to endpoint incidents.

CLOUD INFRASTRUCTURE

- ☐ When using package managers, such as NPM, control and monitor what happens in this environment by:
  - Disabling lifecycle scripts
  - Implementing version pinning
  - Requiring MFA for the deployment of your own NPM packages
- ☐ Use tools like TruffleHog or GitHub Secret Scanning in CI/CD pipelines to implement proactive secret key security and monitoring.
- ☐ Transition from long-term IAM access keys to IAM roles and OIDC for automated workflows to enforce short-lived credentials.
- ☐ Use a secrets manager to automatically rotate keys every 30 to 90 days. Create a predefined automated script to immediately revoke and rotate any key identified as exposed.
- ☐ Enforce least privilege access policies to ensure all API keys have restricted permissions. Never use `AdministratorAccess` for integration keys.
- ☐ Harden AWS instance metadata service (IMDS) settings and require IMDSv2 for new instances.
- ☐ Guard against cryptomining installations with AWS GuardDuty, Runtime Monitoring, Kubernetes pod security policies, and outbound connection monitoring.
- ☐ **For Expel customers:** Enable the disable access key auto remediation so our SOC can quickly shut down a compromised long-term AWS IAM access key.

Know your enemy

Effective threat defense begins with understanding your adversaries and their tactics. Learn more about the latest cybersecurity trends across identity, endpoint, and cloud in the full Expel 2026 Annual Threat Report: **expel.com/2026atr**

About Expel

Expel is the leading managed detection and response (MDR) provider trusted by some of the world's most recognizable brands to expel their adversaries, minimize risk, and build security resilience. Expel's 24/7/365 coverage spans the widest breadth of attack surfaces, including cloud, with 100% transparency. We combine world-class security practitioners and our AI-driven platform, Expel Workbench™, to ingest billions of events monthly and still achieve a 23-minute critical alert MTTR. Expel augments existing programs to help customers maximize their security investments and focus on building trust—with their customers, partners, and employees. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn**.

03/12/26