expel

OUR SERVICES

Cloud Security

Air-cover for the cloud: unlock better security outcomes with Expel MDR

Expel: tailored cloud security, 24x7

As more companies move to the cloud, their security challenges grow. The fast-changing threat landscape—and a shortage of skilled cloud security pros—makes managing security even harder. That's where Expel steps in. We deliver fast, context-rich threat detection across your cloud environment, from the control plane to SaaS apps. Expel offers detection and response strategies specific to AWS, GCP, and Azure, in addition to containerized workloads running in Kubernetes engines. Cloud coverage also includes apps such as Okta, G Suite, and O365 to protect you from data loss and alert you to unusual behaviors, compromised accounts, and privileged access abuse.

With AI-powered alerts and 24x7 support, we quickly detect incidents that evade traditional security tools while giving you real-time visibility. Our tailored detections, resilience recommendations, and proactive threat hunting capabilities ensure your cloud security is always one step ahead.

Transformative results across real customers

125+
integrations from Cloud to IAM

20
minute MTTR on high/critical incidents

87%
MTTR reduction with AI-assisted auto-remediation

Complete cloud coverage

CLOUD CONTROL PLANE	WORKLOADS, CONTAINERS, KUBERNETES	NETWORK	SAAS AND IDENTITY
aws	CROWDSTRIKE	paloalto NETWORKS	Microsoft 365
Microsoft Azure	LACEWORK	zscaler	okta
Google Cloud	PRISMA	FORTINET	snowflake
WIZ		netskope	workday.
▪ Data loss ▪ Compromised credentials ▪ Application attacks ▪ Abnormal API use	▪ Lateral movement ▪ Signs of persistence ▪ Command and control ▪ Privilege escalation	▪ Malicious destination ▪ Malware traffic ▪ Suspicious ports ▪ Suspicious traffic patterns	▪ Data loss ▪ Unusual user behavior ▪ Compromised accounts ▪ Privileged access abuse

How we're different

Expel's tech-agnostic platform enables you to retain your existing tools while quickly unlocking value through custom detections and automations that reduce false positives and accelerate incident detection.

Transparency in everything we do

Stay fully informed on our analysts' observations and audit our decisions in real time.

- **Deep investigations:** our analysts go beyond simply closing alerts, providing you full visibility into their process. They investigate the origin of cloud threats and assess whether other areas are compromised, ensuring comprehensive and transparent security coverage every step of the way.
- **Visibility into your defenses:** we offer clear insights into your MITRE ATT&CK coverage and feedback on your highest-fidelity tools to ensure full transparency into your security defenses.
- **Collaboration and rule transparency:** we openly share our detection logic with you, fostering collaboration to enhance our service for your organization and all Expel customers.

Cloud detections with breadth and depth

Our competitors hyper-focus on EDR—we specialize in the cloud, crafting high-fidelity, custom detections.

- **Unmatched cloud expertise:** offering the most expansive and relevant cloud workload coverage, Expel provides the broadest and deepest detection capabilities tailored specifically for cloud environments.
- **High-fidelity, custom detections:** many MDR solutions are just now investing in boosting cloud detections, but our detection engineers have 8+ years of cloud specific experience. They continuously tune and create custom detections, ensuring detections are relevant and effective across all your cloud services, reducing false positives and improving response times.
- **Advanced detection engineering:** our team of engineers use insights from our entire customer base to customize and tune new detections to your specific needs. We leverage integrations across your environment to augment detection in the cloud.

The flexibility to BYO tech

No need to rip and replace, we have a technology-agnostic platform to meet you where you are.

- **Seamless technology integration:** Expel integrates with over 125 technologies (and growing) across cloud, Kubernetes, network, identity & SaaS apps, endpoint, and SIEM systems, ingesting signals from your existing tools into the Expel Workbench™ platform.
- **Business-driven outcomes:** gain value fast with onboarding in hours, not days. Expel translates alerts into actions, delivering quality forensics at scale with the right combination of people and technology.

Automate the manual to focus on what matters

Expel swiftly consolidates and enriches alert data from hundreds of sources, automating what would take analysts hours to do manually.

- **Precision in risk detection:** machine learning algorithms at Expel highlight alerts with the highest risk, ensuring that critical threats are identified and prioritized.
- **Instant, comprehensive context:** bots automatically stitch together complete context of the situation and run independent workflows to surface additional insights.
- **Award-winning efficiency:** a recognized leader in the Forrester Wave for Managed Detection and Response 2023, Expel's AI/ML and automation technologies deliver unparalleled SOC efficiency, allowing us to invest more in technology and provide global, industry-specific insights in an easy-to-understand format.

How we secure the cloud, yesterday, today and tomorrow

Yesterday

Proactive threat hunting across historical data

Expel's threat hunting service uncovers advanced attacks that evade traditional detection methods. Using hypothesis-driven investigations across your historical cloud data, we hunt for unusual logins, anomalous user behaviors, and suspicious patterns that indicate undetected risks within your cloud infrastructure. By continuously assessing the impact of emerging threats we help protect your organization from both existing and future vulnerabilities. Integrated with Expel's Managed Detection and Response (MDR), our threat hunting service detects and remediates hard to find attacks, while also identifying misconfigurations and gaps in your cloud defenses for proactive risk mitigation.

Today

Real-time monitoring and reporting

Expel gives you real-time visibility into your security operations by allowing you to monitor investigations alongside our analysts, with full transparency. Thanks to deep integrations with cloud sources, we bring in more telemetry than our competitors, providing unparalleled visibility into your environment. We deliver detailed, real-time reports on what happened, where, when, and why. Acting as an extension of your team, our security experts handle threats on your behalf while keeping you informed every step of the way through Expel Workbench™ and Slack and Teams, ensuring you're always in the loop.

Tomorrow

Build cyber resilience with Expel

Expel continuously analyzes threats across billions of events and provides recommendations on how to increase your security posture, helping your organization stay ahead of the latest threats. We provide resilience insights for 70% of the incidents we manage, and offer tailored guidance on configuring your cloud environment to improve detection accuracy and reduce false positives. In addition, Expel benchmarks your security posture against your industry peers and frameworks like NIST CSF, CIS, and MITRE, ensuring you remain both competitive and compliant. Bonus: we continuously learn from the data we ingest to enhance your technology and share strategies that minimize risk and reduce exposure to future threats.

500+ Detections across cloud integrations

Protect your business with the industry's broadest security coverage.

AWS	MICROSOFT AZURE	GOOGLE CLOUD PLATFORM	WIZ	BOX	KUBERNETES
ORCA SECURITY	LACEWORK	PRISMA	CROWDSTRIKE	DUO	DATADOG
WORKDAY	AMAZON GUARDDUTY	GITHUB	SNOWFLAKE	SALESFORCE	OKTA

Ready to take the next steps with Expel MDR?

The choice is yours: see Expel in action in an on-demand demo or talk to one of our MDR specialists.

Watch a demo →

Contact Sales →

092324