Zscaler MDR

Find and stop threats anywhere with Zscaler's human-led, AI-powered MDR.

> "I view them as an extension of my internal team. I communicate with them 24 hours a day, seven days a week. And I feel like they care about our security as much as my internal team does. And that's why I call them my easy button."
>
> **CHIEF INFORMATION SECURITY & PRIVACY OFFICER, PRIVILEGED ASSET MANAGEMENT COMPANY**

Anywhere you run your business, we got you.

Activate world-class security for your endpoints, networks, cloud infrastructure, SaaS applications, identities, and IoT/OT with one vendor-agnostic platform and an on-call team of security experts that has your back 24x7x365. We hunt, research, manage, respond, and remediate threats at scale, allowing you to stay focused on your mission.

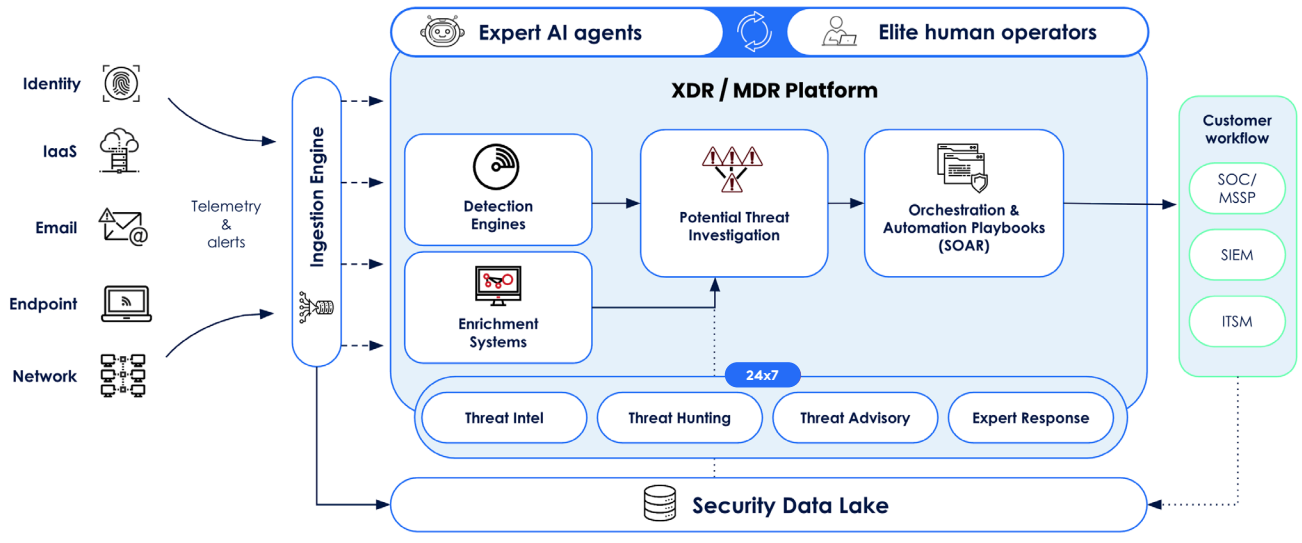
Actionable threat intelligence: Optimize your security program investments with Zscaler MDR. Gain proactive, tactical insights into emerging global threats and collaborate with our analysts. Our continuous analysis of threats across customer environments informs our detection analytics, giving you the collective power of herd immunity.

Unmatched threat detection: Unlike alert-focused solutions, we cast the broadest detection net possible, ingesting both telemetry and security alerts and applying advanced analytics to uncover threats that would otherwise go unnoticed. The result: Red Canary detects five times more confirmed threats than security tools can find on their own.

99%+ noise reduction: Say goodbye to alert fatigue. We've spent over 10 years filtering signals from noise so you don't have to. Our advanced filters and proprietary human+machine approach to high-severity alerts empower your team to focus on what really matters: the security tasks that drive your business forward.

HIGHLIGHTS

- 24/7 monitoring, investigation, and response
- MDR for endpoints, identity, and cloud
- Unlimited access to subject matter experts
- Vendor-and platform-agnostic
- 5x increase in confirmed threats detected
- 10x improvement in MTTR



24x7 expert response

Zscaler MDR goes beyond simply triaging alerts with a full range of response options, including automated, guided, and active remediation. This powerful set of capabilities has resulted in our customers seeing a 10x improvement in mean time to respond (MTTR).

Automated: Our built-in security automation orchestration and response (SOAR) platform provides customizable, easy-to-use playbooks so you can go from alert to action faster. Automated playbooks allow you to quickly notify the right people, contain threats, and begin remediation automatically when confirmed threats are found.

Guided: Zscaler's MDR threat hunting team works side by side with your team, providing real-time guidance during incidents and ongoing coaching. Our write-ups are designed for security operators to take action. Threats are presented in the proper context with all the details needed, including mapping to MITRE ATT&CK®.

Active: Human-led, hands-on-keyboard response acts as an extension of your security team and ensures threats can be mitigated even when your team is unavailable, 24x7x365.

Expert AI agents: Benefit from agentic AI in your security program today

Zscalers MDR's expert AI agents are built from a strong foundation and continuously improved to ensure quality and predictability.

- Imbued with 10+ years of real-world security operations experiences
- Guided by expert-crafted standard operating procedures
- Deployed at scale knowing what great output looks like
- Managed and tuned by elite human operators
- Continuously optimized with feedback and new intelligence

Get herd immunity from prevalent threats across your IT environment

CLOUD
(inc. Control Plane, CNAPP)

- Compromised user credentials
- Misconfigured environments
- Runtime threats
- IAM role abuse
- Data exfiltration

USER
(inc. Identity, Email, SaaS)

- Account compromise
- Unauthorized access
- Business email compromise
- Brute force attacks
- MFA attacks

ENDPOINTS
(inc. Network, OT)

- Credential theft
- Malware
- Ransomware
- Espionage
- Unmanaged devices (IoT)

> "Thanks to this team, we haven't had to fight the fires that other companies do, and it's allowed us to focus on strategic business initiatives."

ROBERT WILLIAMS
CHIEF SECURITY OFFICER, MICROCHIP TECHNOLOGY

Learn more at **zscaler.com**