OUR SERVICES

Expel for Email Security

Secure every email with full lifecycle coverage

Your challenge

Email is the most common attack vector malicious actors use to gain access to an organization. The rise of phishing-as-a-service (PhaaS) platforms and generative AI have increased both the frequency and volume of these attacks, and email security solutions have responded by sending your team more alerts than ever before. Whether malicious, or a "grey area" alert, security teams are bearing the brunt of the manual work required to analyze the potential impact and completely remediate the threat. If you need a trusted security partner to maximize the ROI of your email security or deliver leading detection and response for this attack surface, Expel can help.

How we help

Expel simplifies your ability to protect your organization and data from the growing volume of email based attacks. By combining a unique detection strategy that cuts through the noise and correlates data across your environment, we can detect threats earlier in the attack life cycle, scope who and what may have fallen victim, and automatically contain and remediate the threat.

Expel fortifies your defenses and uncovers attacks sooner by ingesting and correlating telemetry from across your environment including email security solutions, SaaS productivity apps, and endpoint data. Our commitment to building a comprehensive MDR ecosystem ensures unparalleled visibility and rapid threat elimination. Helping your team shift left in the attack cycle limits attackers' ability to move laterally within your environment and minimizes the extent of potential compromise. Our analysts take the burden of continuous detection and response off your plate, boosting your team and technology's effectiveness.

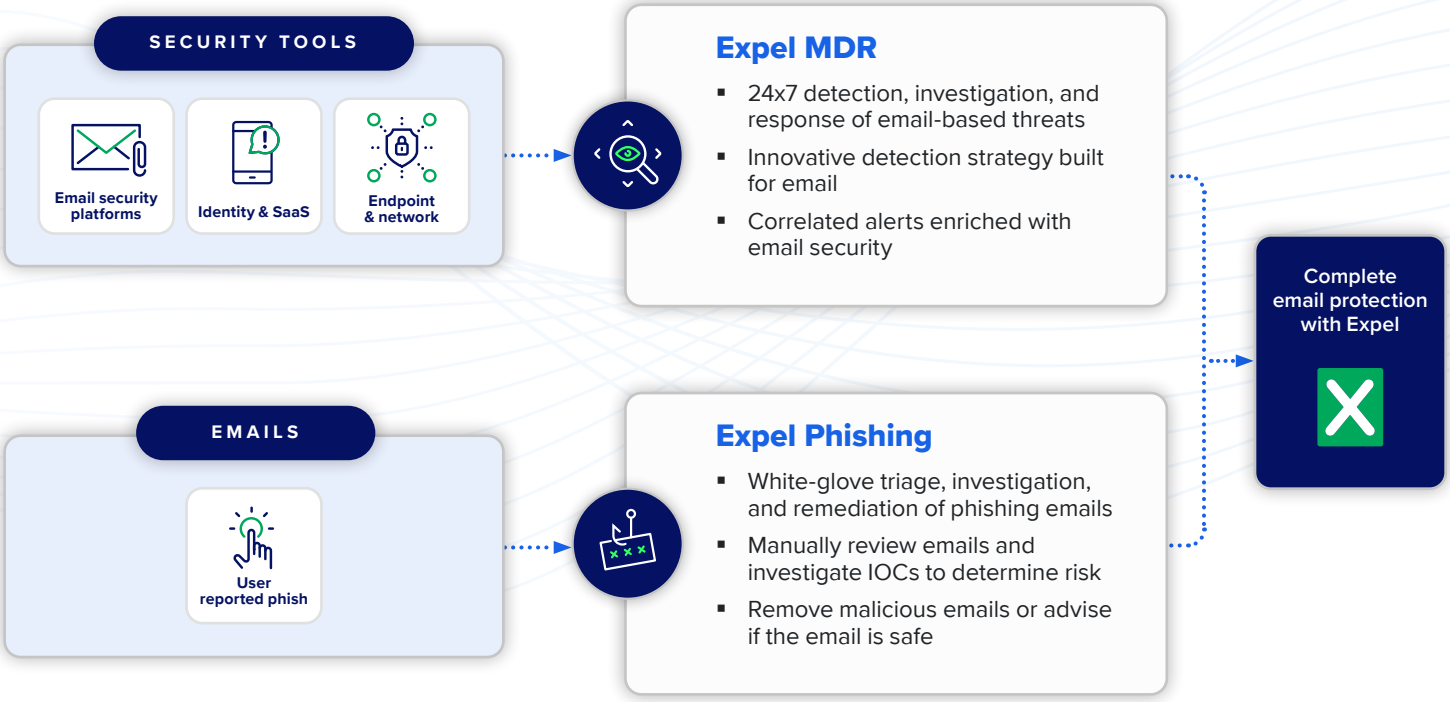
Email security use cases

- **Business email compromise and social engineering**
  Defend against sophisticated threat actors leveraging generative AI tools to craft increasingly convincing fraudulent emails.
- **Credential compromise**
  Find application layer changes and suspicious user activity to prevent lateral movement across your environment.
- **Phishing protection**
  Detect phishing attempts and prevent infiltration of message or limit environmental impact.
- **Enhanced investigation and response**
  Limit exposure when threats penetrate defenses—whether through credential compromise, executed malware, or other techniques—to minimize organizational risk.

Expel for Email Security

Expel provides MDR coverage for email security platforms and a managed phishing solution for user-submitted emails, delivering complete email security.

- **Implement a 'shift left'** security strategy to detect and prevent threats during the initial phases of the cyber kill chain.
- **Enhance the ROI** of email security platforms with unique detection strategy and resilience recommendations.
- **Minimize the blast radius** of email attacks by correlating email data with endpoint, identity, and SaaS alerting to identify IOCs and remediate threats.
- **Investigate phishing emails** by performing analysis of email content, attachments, links, and more, to identify and remove malicious emails.
- **Reduce strain on internal teams** by having Expel's experts handle the 24x7 monitoring and investigation, while reducing the endless noise.



Don't settle for less, work with the leader in MDR.

24x7 email protection

Expel provides full lifecycle, around-the-clock email protection from initial send/receipt to completed investigation.

Accelerate risk reduction

Expel cuts through the noise to quickly detect and eliminate email threats before they impact your organization.

Maximize your investment

An innovative detection strategy and resilience recommendations unlock the full potential of your email security technologies.

Gartner Peer Insights™

4.7/5 Stars
Gartner Peer Insights

Forrester WAVE LEADER 2025
Managed Detection And Response Services

4.8/5 Stars
on G2 Peer Review

Learn more at expel.com