Secure Email Threat Defense

Cloud-scale, AI driven email security protection in a singular, simplified platform



© 2025 Cisco and/or its affiliates. All rights reserved.

Moving your organization's email to the cloud provides convenience and scalability, but the growing sophistication of the threat landscape means it also brings an increased risk of advanced threats like account takeovers and business email compromise.

It's critical to deploy a cloud-focused email security platform that fortifies your existing email security investment, is simple to deploy, and fully protects your organization.

Secure Email Threat Defense, a cloud-scale advanced email security layer, harnesses AI powered detections to provide comprehensive protection against advanced email threats, integrated as an API-based supplemental control or with the addition of new pre-delivery inline gateway protection. It provides the most comprehensive protection against damaging and costly email threats that compromise your organization's brand and operations. Email Threat Defense uses advanced threat detection systems leveraging multiple detection engines that simultaneously evaluate different portions of an incoming email to uncover known, emerging, and targeted threats.

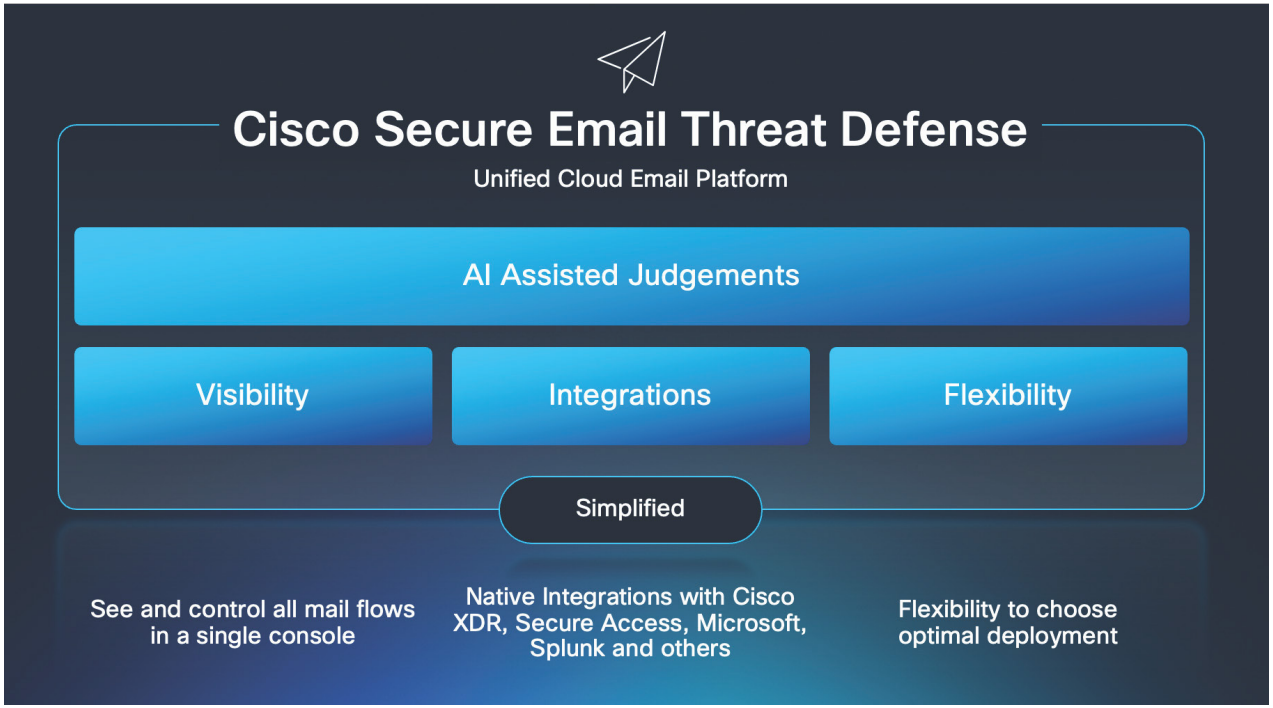
Secure Email Threat Defense Essentials features

- **Identifies malicious techniques:** AI driven technology pinpoints methods used in attacks targeting your organization before they breach your defenses
- **Derives unparalleled context:** Gain deep insights into the specific risks that matter most to your business
- **Provides searchable threat telemetry:** Instantly search and analyze threat data for rapid response
- **Protects your most vulnerable assets:** Categorizes threats to understand which parts of your organization are at highest risk for attack
- **Integrates superior threat intelligence:** Leverages Talos™ intelligence to provide more comprehensive, real-time threat visibility that informs better and faster decision-making
- **Simplifies deployment:** Quick API-based integration requires no changes to existing mail flow or DNS records

Backed by over two decades of email gateway expertise, Secure Email Threat Defense brings the next wave of email security to your organization — it's now a gateway solution!

With the Advantage tier, our enhanced Email Threat Defense platform has an even greater focus on customer outcomes by unifying multiple deployment modes into a single, flexible solution offering pre-delivery threat prevention, post-delivery remediation via APIs, and full visibility of email in one streamlined console, available globally.

Until now, Email Threat Defense has been known for its exceptional detection and protection capabilities — backed by proven threat intelligence and advanced analytics. With this new deployment mode, Email Threat Defense can now operate as a standalone email security gateway, providing organizations with even more flexibility in how they defend against evolving email threats.



© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Email Threat Defense Advantage features

In addition to everything included in Email Threat Defense Essentials:

- **Cloud-scale, AI driven gateway capabilities:** Harness cloud-scale AI in our unified platform, eliminating traditional appliance-based limitations and reducing overhead
- **Comprehensive, Pre-delivery Threat Protection:** Proactively stop email threats before they reach the mailbox, ensuring compliance and a safer, protected environment
- **Unified and Flexible Platform:** Gain flexible threat protection through a cohesive interface that unifies inline gateway and API-based deployment modes into a single console
- **Simplified Management and Robust Security:** Streamline maintenance and accelerate your email security journey with cloud-scale AI and seamless platform integration

This enhancement means Email Threat Defense doesn't just rely on what it already does brilliantly — it's now supercharged with additional gateway capabilities. The result is deeper insights, smarter threat detection, and even better protection against phishing, spoofing, and other advanced email-based attacks. Recent third-party testing and analyst reporting celebrate these new levels of efficacy.

Secure Email Threat Defense empowers your organization with the opportunity to modernize your email security into a singular, continuously evolving, advanced platform — driven by cloud-scale AI detections. It eliminates the need to manage appliance resources, which eases product maintenance and reduces the administrative burden on your already busy team. These enhancements and redesigned gateway capabilities are joining with the existing sophisticated detectors within Email Threat Defense in a truly cloud-scale architecture that provides robust security in a simplified way.

A critical component of your extended detection and response strategy

Email Threat Defense is a key component of the User Protection Suite and Breach Protection Suite, and an important part of a strategic XDR strategy. In combination with numerous third-party integration partners and the larger Cisco Security portfolio of products, this provides visibility, efficiency, simplicity, and telemetry that empowers your team to act quickly.

Start a free trial of Email Threat Defense today.

Cisco Secure Email Threat Defense for Government: Class D (High) FedRAMP Certification Achieved

Email Threat Defense has achieved FedRAMP Class D (High) certification, underscoring our ongoing commitment to delivering trusted, government-grade email security for agencies, contractors, and organizations handling regulated or sensitive data. Secure Email Threat Defense, a cloud-scale advanced email security layer, harnesses AI powered detections to provide comprehensive protection against advanced email threats, integrated as an API-based supplemental control or with the addition of new pre-delivery inline gateway protection. Key Benefits of FedRAMP certification include:

- **Proven Compliance:** Meets rigorous FedRAMP security requirements, ensuring alignment with federal mandates.
- **Advanced Threat Protection:** Defends against phishing, malware, business email compromise, and emerging threats with real-time intelligence.
- **Continuous Security Monitoring:** Maintains a high-security posture with ongoing vulnerability assessments and continuous monitoring, not just one-time audits.
- **Streamlined Procurement:** Simplifies acquisition and deployment for public sector, accelerating secure cloud adoption while reducing compliance complexity.
- **Vendor Risk Reduction:** Undergoes third-party assessments for increased transparency and lower risk for agencies and regulated organizations.
- **Operational Efficiency:** Uses the "do once, use many times" FedRAMP model for cost savings and faster implementation across multiple agencies.
- **Robust Incident Response:** Features strong incident detection, response protocols, and audit-ready security telemetry for rapid investigation and resilience.
- **Seamless Integration:** Works natively with Microsoft Office 365 and other platforms for comprehensive, adaptable email protection.