Data Sheet

ThreatDown
Powered by Malwarebytes

ThreatDown Email Security

Real-time Adaptive AI protection and remediation against advanced phishing attacks.

Overview

Phishing remains one of the most critical cybersecurity challenges due to its evolving sophistication and ability to exploit human behavior. Attackers use social engineering, impersonation, and convincing messages to deceive users, making detection difficult. The widespread use of email and messaging platforms increases exposure, while traditional security tools often fail to stop advanced phishing attempts. Combating phishing requires continuous user education, advanced threat detection, and layered security measures to mitigate risks and reduce successful attacks.

With limited resources, organizations need practical and cost-effective solutions that stop phishing attacks, business email compromise, credential harvesting, and other email-borne attacks. ThreatDown Email Security stops phishing attacks through a multi-layered, Adaptive AI approach that combines machine learning, behavioral analysis, and human intelligence. It is managed easily along with ThreatDown's endpoint security solutions; all from the single, cloud-based ThreatDown console.

ThreatDown Email Security Advantages

- ✓ **Adaptive Email Threat Protection:** Prevents email attacks with anomaly detection and crowdsourced threat intelligence (from 16K+ security teams). Continuously learn and adjust to new threats and attacks with intelligent, self-learning protection.
- ✓ **Setup in Seconds:** Deploy and configure easily with just a few clicks for native API integration with cloud-based email providers — no MX record changes, no agents, no separate console.
- ✓ **Unified Endpoint and Email Security Management:** Manage endpoint security and email security together with the same cloud-based ThreatDown console for easy monitoring, detection, and response.
- ✓ **Rapid Auto-remediation:** Accelerate response time with machine learning-based detection, classification, and remediation. Agentic automation eliminates all attack variants to meet organizational security needs.

Industry Accolades and Peer Reviews

The Ironscales technology that powers ThreatDown Email Security is rated highly by third-party customer reviews and independent rating organizations.

Challenges

- **Need security against email-borne threats** - #1 cyberattack vector is email
- **Need to reduce management complexity** - 70% of SMBs are in the process of or planning to consolidate software and vendors[1]
- **Need to address lack of security staff resources** - 1.5 IT security staff on average per small business[2]

Benefits

- **Stop high-risk attacks with integrated cloud email security** - Gain comprehensive email protection against phishing, business email compromise (BEC), credential harvesting, and other threats
- **Save time & effort** - Manage email security from the same console as the ThreatDown endpoint security stack; Deploy protection with setup in seconds stack
- **Automate response** - Empower IT teams with limited resources by automatically detecting and resolving email threats and attacks without manual intervention to reduce response times and minimize human error

Learn More

To learn more about Email Security, please visit threatdown.com/custom-quote/email-security

1.Elevate SMB IT Strategy with These Top 4 Priorities, Goto 2024, 2.SMB & Midmarket Security Adoption Trends, Techaisle 2024

ThreatDown
Powered by Malwarebytes

threatdown.com

sales@threatdown.com