eLearning

ThreatDown™
Powered by Malwarebytes

ThreatDown Email Security Sales Play

Table of Contents

What to Know

What to Say

What to Know

Definitions and Acronyms

Phishing emails impersonate trusted entities to trick people into sharing passwords, financial info, or sensitive data. Delivered through email and fueled by social engineering, phishing is one of the most common ways attackers breach systems and spread malware.

Malware is malicious software often delivered via email through infected attachments or links to compromised websites. It can install ransomware, spyware, or viruses that steal data, damage systems, or provide unauthorized access. These attacks rely on social engineering to trick users and are a common starting point for broader cyberattacks.

Business Email Compromise (BEC) attacks impersonate executives, customers, governing bodies, or trusted partners to trick employees into wiring money or sharing sensitive data. These socially engineered attacks bypass technical controls and can lead to major financial losses, data leaks, and reputational damage.

Account Takeover (ATO) happens when attackers gain access to a user's account (often accomplished through stolen credentials or phishing). Once in, they can impersonate the user, steal data, or launch internal attacks. These threats often fly under the radar and cause serious financial and reputational damage.

Domain Name Server (DNS) translates URLs (names) like www.threatdown.com to IP addresses like 192.0.66.84.

Domain-based Message Authentication, Reporting & Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) are authentication protocols that ensure email deliverability, protect an organization's brand, and prevent domain spoofing aimed at employees, partners, and customers.

Mail Exchange (MX) Record is a type of DNS (Domain Name System) record that tells the internet which mail servers are responsible for receiving email for a specific domain.

Secure Email Gateway (SEG) is a traditional email security solution that filters email traffic. SEGs analyze emails before they reach users' inboxes, enforcing security policies and blocking malicious content. Traditional SEGs rely on signature-based detection, rule sets, and reputation filters, and often require complex configuration and maintenance.

Integrated Cloud Email Security (ICES) is an API-based solution that integrates directly with cloud-based email platforms like Microsoft 365 and Google Workspace. Unlike traditional secure email gateways (SEGs), ICES operates *inside* the email environment to continuously monitor, detect, and respond to threats **after** delivery. Leveraging artificial intelligence, machine learning, and behavioral analysis, ICES solutions detect sophisticated attacks such as phishing, BEC, and zero-day threats, while offering faster deployment, better visibility, and more seamless user experiences.

What to Know

Elevator Pitch

ThreatDown Email Security combines Adaptive AI detection with human-in-the-loop insight through crowdsourced threat intelligence to stop advanced phishing, Business Email Compromise, and zero-day attacks missed by traditional solutions. Deployed in minutes and integrated management with endpoint security, it provides automated detection, protection, and remediation to reduce risk, alert fatigue, and response time, all from the single, cloud-based ThreatDown console.

What to Know

Positioning

Challenges	Advantages/ Proof Points	Features	Benefits	Impact
Need protection against email-borne threats, the #1 cyberattack vector	Validated by third-party awards and analyst recognition: • Visionary -Gartner Magic Quadrant for Email Security Platforms 2024 • Leader – Frost & Sullivan, Frost Radar: Email Security, 2024 • 2024 Fortress Cybersecurity Award for AI • Leader and Outperformer: 2024 GigaOm Anti-phishing Radar Report	**Adaptive AI** Stop email attacks with threat intelligence, anomaly detection, and real-time threat hunting. Continuously learn and adjust to new threats and attacks with intelligent, self-learning protection	• Stop high-risk attacks with innovative integrated cloud email security (ICES) • Gain comprehensive email protection against phishing, business email compromise (BEC), credential harvesting, account takeover attacks, and other threats	• Cost of a breach • Downtime • Loss of reputation
Need to reduce complexity for email and endpoint security management as SMBs have minimal security staff	Validated by third-party awards and analyst recognition: • G2 Easiest Admin (Mid-market Cloud Email Security), Winter 2025 • G2 Best Estimated ROI (Mid-Market & Intelligent Email Protection), Winter 2025	**Setup in Seconds** Deploy 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 email security with the same cloud-based console as the rest of the ThreatDown security stack	Save time and effort by deploying protection with just a few easy clicks and managing email security from the same console as the ThreatDown endpoint security stack	• Job satisfaction • Employee retention

What to Know

Positioning

Challenges	Advantages/ Proof Points	Features	Benefits	Impact
Small businesses (1-99), on average, have 1.5 IT security staff Core midmarket (100-999), on average have 5.8 IT security staff * SMB & Midmarket Security Adoption Trends, Techaisle 2024	ThreatDown Email Security delivers lightning-fast, Adaptive AI remediation that stops new threats, works post-delivery, and gives IT teams the control they need—without the complexity of traditional SEGs or manual SOC processes.	**Rapid Auto-remediation** Accelerate response time with machine learning-based detection, classification, and remediation. Use agentic automation to eliminate all attack variants and meet organizational security needs.	Reduce workload for IT teams with limited resources by automatically detecting and resolving email threats and attacks without manual intervention. Reduce response times, minimize human error, and free staff to focus on higher-priority tasks. It is a force multiplier for lean IT teams, helping them maintain resilience, reduce downtime, and stay ahead of evolving threats—without needing to scale headcount.	• Resource drain • Operational disruption

What to Know

Value Proposition

ThreatDown Email Security delivers comprehensive, Adaptive AI protection that combines machine learning, natural language processing, natural language understanding, and real-time human threat intelligence to stop advanced phishing, Business Email Compromise, and other sophisticated threats that traditional secure email gateways miss. Its in-inbox protection, automated remediation, and seamless integration with Microsoft 365 and Google Workspace empower lean security teams to detect, respond, and remediate threats faster—reducing risk, saving time, and simplifying email security management integrated with endpoint security all from the single, ThreatDown console.

Buyer Personas

	Functional (User/Champion)	**Strategic** (Decision Maker/Budget Owner)
Title	• Director of IT/Director of Security • IT Manager • Security Admin	• Business Owner • CXO • VP of IT/ Security
Challenges to Solve	• Satisfy IT needs of business and users • Protect company's devices, digital assets, and intellectual property • Stop attacks and address potential threats before they cause harm—without increasing complexity • Promptly detect hidden threats to reduce dwell time • Ensure all alerts are prioritized, investigated, and triaged in a timely manner • Efficient incident response • Complete work successfully with limited staff and security expertise • Maintain employee productivity; reduce downtime	• Align security operations to business goals • Increase ROI of security investments • Protect brand, reputation, and bottom line • Navigate security staff and skills shortage • Cyber resilience • Governance (regulations, boards, insurance,) security commitments

What to Know

MSP Personas

	Functional (Technical Decision Maker)	Strategic (Business Decision Maker)
Title	• MSP Tech Lead • MSP Solution Architect	• MSP Owner • MSP Principal
Challenges to Solve	• Simplify the design and deployment of security stacks across client environments • Seamlessly integrate existing tools, including Email Security, EDR, SIEM, and RMM to simplify multi-client security operations, eliminate tool sprawl, and reduce overhead with unified visibility and automated workflows. • Mitigate alert fatigue and streamline management of multiple security vendors • Prioritize solutions with API integrations, granular policy controls, threat intelligence, advanced phishing detection, and automated remediation and reporting	• Grow business via differentiated security offerings • Provide high-margin, scalable security services; reduce client risk • Navigate limited time, staff, and in-house expertise with need for automation and ease-of-management • Need solutions with a multi-tenant management console, that are easy-to-deploy, have all-in-one email protection, provide compliance reporting, and have a small number of false positives

Usual Suspects – Prevalent Competitors

Pureplay Email Security Vendors

- Proofpoint
- Mimecast
- Barracuda

Endpoint Security Vendors with Email Security Capabilities

- Bitdefender
- ESET
- Microsoft
- Sophos
- Trend Micro
- Webroot

What to Know

Upsell Strategies

Upsell Scenario	Customer Type (New & Existing)	Single-Tenant vs. Multi-Tenant	Objective	Messaging	Which Bundle Solutions?	Which Modules Solutions?	Value Prop
Bundle Upsell	Direct Customer	Single-Tenant	Refer to Bundles Sales Play	Refer to Bundles Sales Play	Refer to Bundles Sales Play	N/A	Refer to Bundles Sales Play
Bundle Upsell	Direct Customer	Multi-Tenant	Refer to Bundles Sales Play	Refer to Bundles Sales Play	Refer to Bundles Sales Play	N/A	Refer to Bundles Sales Play
Bundle Upsell	MSP Customer	Multi-Tenant	N/A	N/A	N/A	N/A	N/A
A la carte solution	Direct Customer	Single-Tenant	N/A	N/A	N/A	N/A	N/A
A la carte solution	Direct Customer	Multi-Tenant	N/A	N/A	N/A	N/A	N/A
A la carte solution	MSP Customer	Multi-Tenant	MDR or EDR and any module not already purchased	Refer to MDR, EDR, and module sales plays	N/A	Any not already purchased*	Refer to MDR, EDR, and module sales plays

* includes all "modules" and add-ons

Gotchas and Be Aware

- ThreatDown Email Security is only available as an add-on purchase. It cannot be bought standalone. For customers interested in a standalone email security solution, they should consider Ironscales or other email security vendor.
- ThreatDown Email Security only supports Microsoft 365 and Google Workspace inboxes. If a customer has both, the customer must choose which one of the two to protect.
- At launch, ThreatDown Email Security does not support account takeover protection or Security Advisor.

What to Say

Elevator Pitch

ThreatDown Email Security combines Adaptive AI detection with human-in-the-loop insight through crowdsourced threat intelligence to stop advanced phishing, BEC, and zero-day attacks missed by traditional solutions. Deployed in minutes and easy to manage, it provides automated remediation and seamless Microsoft 365 and Google Workspace integration—reducing risk, alert fatigue, and response time, all from the single, cloud-based ThreatDown console.

Industry Specific/Vertical Specific Talking Points

Education (K-12 and Higher Ed)

- **Why**: High volume of email communication, limited IT staff, budget sensitivity.
- **Fit**: Quick deployment, low maintenance, and protection against student-targeted phishing and credential theft.

Healthcare

- **Why**: Frequent phishing attempts, HIPAA compliance requirements, and understaffed security teams.
- **Fit**: Automation and easy Microsoft 365 and Google Workspace integration reduce response time and risk without adding operational overhead.

Financial Services

- **Why**: High value targets for BEC and fraud; strict regulations (e.g., GLBA, SOX, PCI DSS, GDPR, etc.).
- **Fit**: Detection of socially engineered threats and BEC attacks that bypass traditional filters, with audit trails.

Manufacturing

- **Why**: Vulnerable to supply chain and vendor-based phishing attacks.
- **Fit**: Impersonation and anomaly detection capabilities protect distributed and hybrid teams with minimal management.

Legal & Professional Services

- **Why**: Frequent sharing of sensitive information, high risk of spoofing and impersonation.
- **Fit**: In-inbox protection and brand spoof detection help prevent data breaches and reputational damage.

Use Cases

1 | Prevent phishing attacks

Pain

Phishing targets employees and these attacks exploit human trust and overwhelm security teams (dealing with threats, false positives, etc.).

Business Impact

Financial loss, reputational damage, and operational burden.

Solution Benefit

Protect against advanced phishing attacks. ThreatDown Email Security stops phishing attacks through a multi-layered, Adaptive AI approach that combines machine learning, behavioral analysis, and human intelligence. Capabilities include:

- **Adaptive AI Email Analysis**: Uses natural language processing (NLP), computer vision, and behavioral algorithms to detect phishing attempts—such as spoofing, impersonation, and deceptive links—even without known threat signatures.
- **Mailbox-Level Detection**: Works inside users' inboxes (not just at the gateway or pre-delivery), identifying and removing phishing emails in real time, including advanced threats like BEC and spear phishing.
- **URL & Attachment Scanning**: Analyzes embedded links and attachments for malicious content using sandboxing and real-time inspection, blocking credential harvesting and malware delivery.
- **Crowdsourced Threat Intelligence**: Leverages data from a global community of more than 16K security teams to stay ahead of emerging phishing campaigns and improve detection accuracy of novel attacks.
- **Automated Remediation**: Instantly removes or quarantines phishing emails across all user inboxes—even after delivery—preventing user interaction with malicious content.
- **Brand Protection with DMARC**: Prevents domain spoofing and impersonation by enforcing email authentication protocols like SPF, DKIM, and DMARC.

Use Cases

2 | Stop Business Email Compromise

Pain

BEC attacks are nearly invisible to traditional filters, prey on human trust, and often without ever triggering a typical phishing alarm (payload-less attacks—no links or attachments).

Business Impact

Massive financial, operational, and reputational damage.

Solution Benefit

Stop attacks like BEC and VIP impersonation. ThreatDown Email Security stops BECs through a combination of Adaptive AI, behavioral analysis, and user engagement, targeting the unique nature of BEC attacks, which often lack malicious links or attachments.

Capabilities include:

- **Natural Language Processing (NLP)**: Analyzes email content, tone, and context to detect anomalies such as urgent requests or unusual phrasing typical of BEC.
- **Social Graphing**: Maps each user's typical communication patterns—who they talk to, when, and how—to detect anomalies like unexpected senders, timing, or tone that may signal phishing or account takeover attempts.
- **Mailbox-Level Detection**: Works inside the inbox, not just at the gateway, allowing real-time identification of socially engineered threats.
- **Crowdsourced Threat Intelligence**: Leverages community-driven insights to improve detection across its network.
- **Automated Remediation**: Instantly removes or quarantines suspicious emails before users can engage with them.

Use Cases

3 | Prevent Advanced Malware and URL Attacks

Pain

Advanced malware and URL attacks bypass conventional email defenses, spread fast, and require high-effort manual investigation.

Business Impact

These attacks leave security teams vulnerable to breach, downtime, and costly clean-up.

Solution Benefit

Continuously protect against malicious links and attachments. ThreatDown Email Security stops advanced malware and URL-based attacks using a combination of Adaptive AI detection, sandboxing, and real-time threat intelligence.

Capabilities include:

- **Real-Time URL Analysis**: Scans and rewrites links in emails to analyze them upon click. Malicious or suspicious URLs are blocked before users reach harmful sites.
- **AI and Machine Learning**: Detects hidden threats using advanced algorithms that analyze patterns in URLs, attachments, and message behavior beyond simple signatures.
- **Deep Link Inspection**: Uses recursive URL scanning to detect multi-stage attacks or redirects to phishing or malware-hosting sites.
- **Attachment Sandboxing**: Opens and tests attachments in a secure, isolated environment to detect zero-day and polymorphic malware before they reach the user.
- **Crowdsourced Threat Intelligence**: Leverages global community data to rapidly identify and block emerging threats.
- **Automated Remediation**: Instantly removes emails with malicious links or attachments across all user inboxes, even post-delivery.

Use Cases

4 | Address Generative AI Attacks

Pain

Generative AI gives attackers the ability to craft highly personalized, realistic phishing emails at scale.

Business Impact

These attacks bypass traditional defenses and overwhelming users and security teams with threats that are harder to detect, trust, and respond to leading to financial loss, reputational damage, and operational burden.

Solution Benefit

Safeguard against GPT-crafted emails. ThreatDown Email Security effectively defends against generative AI-powered attacks—such as hyper-personalized phishing emails, business email compromise (BEC), and deepfake-style social engineering—using a layered, adaptive approach that includes:

- **Natural Language Processing (NLP)**: Detects AI-generated language patterns, such as unusually polished or context-aware messages that deviate from normal human writing styles or tone.
- **Behavioral Analysis**: Monitors communication patterns, sender behavior, and email context to flag inconsistencies typical of impersonation or AI-crafted content.
- **Mailbox-Level Detection**: Works inside the inbox to identify threats that bypass perimeter defenses, focusing on socially engineered content and intent—not just known indicators.
- **Crowdsourced Intelligence**: Gathers real-time input from thousands of users and security teams globally, rapidly adapting to new generative AI attack tactics.
- **Computer Vision and Link Inspection**: Identifies fake branding, forged login pages, and visually deceptive elements often used in AI-assisted phishing campaigns.
- **Automated Threat Remediation**: Quickly removes detected threats across all affected mailboxes, preventing user engagement with generative AI-crafted messages.

Use Cases

5 | Complement Endpoint Detection and Response (EDR)

Pain

When email security and EDR operate in silos, organizations lose critical visibility, delay response, and leave gaps attackers can exploit—turning a phishing email into a full-blown breach.

Business Impact

Siloed threat visibility, slower response times, incomplete remediation, and alert fatigue lead to more time spent resolving threats and addressing compromised endpoints.

Solution Benefit

Work hand-in-hand with EDR. ThreatDown Email Security complements EDR by securing the email attack vector which is often the initial entry point for breaches. While EDR tools focus on detecting and responding to threats on endpoints, ThreatDown Email Security proactively prevents phishing, malware, and social engineering attacks before they reach users. Its Adaptive AI detection, real-time remediation, and seamless integration with inboxes stop threats missed by traditional tools. Together, Email Security and EDR deliver layered, end-to-end protection against modern cyber threats.

Use Cases

6 | Integrate Email Security with Endpoint Security

Pain

When email and endpoint security aren't integrated, security teams struggle to see the full attack chain, respond quickly, or fully remediate threats—leaving dangerous gaps attackers can exploit.

Business Impact

Multiple consoles lead to complexity and wasted time managing two solutions from multiple vendors with loss of security visibility and delays in addressing attacks.

Solution Benefit

Deliver efficient security management. Combining email and endpoint security in a single cloud-based console streamlines threat detection, response, and management across the entire attack surface. Security teams gain unified visibility, faster incident response, and reduced complexity by managing both threat vectors from one console. This integration ensures cohesive policy enforcement, minimizes security gaps, and simplifies operations. With centralized control, IT teams can detect email-borne threats and endpoint attacks to respond in real-time, enhancing overall protection, efficiency, and compliance across the organization.

Value Proposition

ThreatDown Email Security delivers comprehensive, Adaptive AI email security that combines machine learning, natural language processing, and real-time human threat intelligence to stop advanced phishing, BEC, and other sophisticated threats that traditional secure email gateways miss. Its in-inbox protection, automated remediation, and seamless integration with Microsoft 365 and Google Workspace empower lean security teams to detect, respond, and remediate threats faster—reducing risk, saving time, and simplifying email security management from the single, unified ThreatDown console.

What to Say

Qualifying Questions

- How are you currently protecting your organization from email-based threats like phishing and BEC?
- What types of email threats are bypassing your current security solution?
- Are users reporting suspicious emails that turn out to be real threats? How often?
- How much time does your team spend investigating and remediating email threats each week?
- Are you using Microsoft 365, Google Workspace, or another platform for email?
- Are you currently using a Secure Email Gateway (SEG)? If so, which one?
- Are you using an XDR or EDR solution, and do you want email security to integrate with it?
- How comfortable are you with leveraging AI or automation for threat detection and remediation?
- Do you have a lean IT or security team that would benefit from automated remediation or crowd-sourced threat intel?
- What's driving your interest in improving email security right now—compliance, a recent breach, audit findings, or team workload?
- What are your top three priorities for an email security solution over the next 6–12 months?
- Are you open to considering alternatives to your existing SEG, or are you strictly looking to augment it?

Discovery Questions

M – Metrics

- What KPIs or metrics are you tracking around email security today (e.g., phishing incident volume, response time, user-reported threats)?
- Do you have an estimate of how much time your team spends on email threat investigation and remediation per week?
- What would reducing that time by 50% mean for your team or organization?

What to Say

Discovery Questions

E – Economic Buyer

- What are the steps and who is ultimately responsible for signing off on security investments like this?
- What does that person care most about—risk reduction, operational efficiency, compliance, or cost savings?
- Have you or your team presented a business case for a new security tool before? What did that process look like?

D – Decision Criteria

- What are the most important capabilities you are evaluating in an email security solution?
- Are you prioritizing SEG replacement, augmentation, or integration with your existing tools like EDR/XDR?
- How important are things like automated remediation, user experience, and speed of deployment in your decision?

D – Decision Process

- What's your process for evaluating and purchasing new security solutions?
- Is there a formal RFP, or are you working with a shortlist of vendors?
- What does your timeline look like for selecting and implementing a solution?

I – Identify Pain

- Have you experienced any recent phishing or BEC incidents that impacted the business?
- Are you seeing attacks getting through your SEG or Microsoft 365/Google Workspace native defenses?
- Is alert fatigue or limited security staffing a challenge for your team right now?

What to Say

Discovery Questions

C – Champion

- Who on your team would benefit most from ThreatDown Email Security's automation and ease of use?
- Who is driving this initiative internally, and what outcomes are they responsible for delivering?
- Would it be helpful to equip that person with ROI data or success stories to help build internal support?

C – Competition

- What other solutions are you considering or currently using for email security?
- What do you like/dislike about them?
- How are you differentiating between vendors in terms of innovation, ease of use, or long-term value?

What to Say

Competitive Differentiation

Competitive Messaging

- **Adaptive AI for superior defense** - Adaptive AI delivers advanced protection against phishing and email-based threats by combining real-time analysis, specialized machine learning models, and evolving adaptive defense to outsmart attackers. This AI-powered technology continuously learns and adapts to new attack techniques, enabling real-time threat detection and automated response. By integrating crowd-sourced intelligence (from 25K+ security experts) and human-in-the-loop user feedback), ThreatDown Email Security reduces false positives and enhances accuracy. This proactive, adaptive approach strengthens email security, empowering organizations to defend against sophisticated, evolving threats and their variants with greater speed and precision.
- **Unified management console for easy management** - The single, ThreatDown cloud-based console delivers centralized visibility, correlation, and control, streamlining the management of security layers and policies across an organization. It enhances efficiency by reducing complexity, enabling faster email threat detection, response, and compliance monitoring. Consolidating security operations into one platform minimizes blind spots, improves coordination, and reduces the risk of misconfigurations. This unified approach for all ThreatDown security layers saves time and resources and strengthens the organization's overall security posture against evolving cyber threats.
- **Efficient, scalable, intelligent protection** - Smarter. Faster. Safer. Better than traditional secure email gateways (SEGs), ThreatDown Email Security integrates directly within inboxes, using Adaptive AI to detect and remediate threats and their variants in real time. While SEGs rely on static rules and perimeter defenses, ThreatDown's innovative approach uses advanced machine learning, crowdsourced threat intelligence, and automation to stop phishing, BEC, and malware attacks faster. No additional hardware is needed. No MX record changes needed.

Competitive Differentiators

- **Built for resource-constrained teams** – Combines innovative Adaptive AI and automation for email security in an easy-to-manage console including endpoint security.
- **Inbox-level protection** – Works inside Microsoft 365 and Google Workspace, not just at the perimeter to stop internal, lateral, and post-delivery attacks.
- **Crowdsourced threat intel** – Learns from thousands of global users to stop threats faster than SEGs or native tools that rely on static rules and signatures.
- **Automated remediation** – Stops the spread by removing malicious emails in real time across all inboxes
- **No MX changes** – API-based deployment in minutes with no MX rerouting and no disruption to mail flow.

What to Say

Objection Handling

Keeping the Status Quo (Already Covered)

Objection: "We already have a Secure Email Gateway." "We already have native Microsoft 365 and Google Workspace email protection."

Response Questions:

- How confident are you that it's catching advanced phishing and BEC attacks today?
- How many user-reported threats have made it past your current filters?
- Would you be open to seeing what threats may be slipping through in a short product trial?

Budget and Cost Concerns

Objection: "We don't have budget right now"

Response Questions:

- How much time is your team currently spending on phishing investigation or user-reported emails?
- If ThreatDown Email Security could reduce that by 50–70%, would that justify a conversation around potential savings and risk reduction?
- Is email security something that's on the roadmap for next quarter or fiscal year?

Too Many Security Tools

Objection: "We want to reduce the number of security vendors we work with."

Response Questions:

- Are your current tools integrated, or do they require separate management consoles and workflows?
- How would a solution that combines detection and automated remediation for both email security and endpoint security in one console help reduce operational complexity?

What to Say

Objection Handling

Implementation and Deployment Resource Constraints

Objection: “We don’t have the resources to take on another product/project.”

Response Questions:

- Would an API-based deployment that takes just minutes to setup be easier for your team to manage?
- If the solution were live and reducing alert volume by end of day one, would that relieve some of the burden from your team?
- Are you looking for solutions that take pressure off your existing staff, or ones that require more tuning for granular control?

2445 Augustine Drive, Suite 550 | Santa Clara, CA 95054 USA | +1-800-520-2796