Modern Email Security That's Smarter, Stronger, and Layered

Today's email threats are faster, smarter, and harder to catch. Midmarket organizations now face enterprise-grade risks: phishing, business email compromise (BEC), AI-driven impersonation, deepfakes, QR-code scams, and the tactics evolve daily.

To stay ahead, teams need more than one line of defense. They need email security that works before, during, and after delivery.

VIPRE Total Email Protection (TEP) brings together two proven solutions, VIPRE Email Security - Advanced Threat Protection (ATP), a market leading Secure Email Gateway (SEG) and VIPRE Integrated Email Security (IES), an Integrated Cloud Email Security (ICES) solution into a single, cost effective product offering. This layered defense model combines high-volume filtering at the perimeter with adaptive, AI-driven detection that works inside the inbox.

It's built for midmarket teams that want enterprise-grade protection without complexity. With native Microsoft 365 integration, hands-free deployment, and automation-ready response, TEP stops modern threats wherever and whenever they strike.

Trusted, Adaptive, and Proven

20M+
Endpoints Protected

10M+
Inboxes Secured

25+
Years Experience

How It Works: Layered Email Defense

Pre-Delivery Defense (VIPRE ATP):
Stops the majority of spam, phishing, and malware before messages reach the inbox. VIPRE/ATP handles high-volume threat filtering at the perimeter, with policy-based controls for encryption, routing, and DLP enforcement.

Post-Delivery Detection (VIPRE IES):
Detects the threats that get through: advanced phishing, BEC, AI-generated impersonation, and internal attacks. IES scans emails inside the inbox and across internal traffic, removing malicious messages post-delivery and reducing dwell time.

Together:
You get defense-in-depth that adapts to evolving tactics. Like securing both the doors and the rooms inside, VIPRE's combined approach helps you catch more and recover faster.

Layered Protection at Every Stage of the Attack Lifecycle

VIPRE ATP Benefits	VIPRE IES Benefits	Combined Product Advantages
Handles high volumes of threats at the perimeter (80% or more)	Post-delivery protection	Extended reach of sandboxing technology to internal emails
Provides pre-delivery filtering	Detects nuanced, sophisticated attacks that bypass perimeter defenses	Protection against threats that trigger later in the cyber kill chain
Advanced policy controls for email routing and management	Offers context-rich visibility for end-users and investigators	Defense against compromised internal accounts
Enforces DLP policies and enables encryption	Scans internal email traffic for threats	End-to-end visibility and control—from the perimeter to internal communications

Core Features in Detail

Real-Time Threat Detection

VIPRE ATP provides robust perimeter protection, blocking spam, viruses, phishing, and malware before emails reach the inbox.

VIPRE IES extends protection post-delivery, detecting targeted, evasive threats that slip through traditional security nets.

Together, they provide layered protection across inbound, outbound, and internal email traffic.

- Blocks phishing, spear phishing, BEC, malware attachments, malicious links, and QR-code scams
- Detects AI-generated impersonation, invoice fraud, brand spoofing, and deepfake URLs
- Leverages threat intelligence from billions of emails for real-time updates
- Signature-based detection (VIPRE ATP) complements AI-driven, behavioral analysis (IES)
- Covers inbound, outbound, and lateral movement within email environments

Semantic and Behavioral Analysis (VIPRE IES)

IES goes beyond surface-level scanning to detect the intent behind an email, even when there are no malicious attachments or links.

- Analyzes message tone, context, and behavior
- Detects socially engineered threats and insider risks
- Strengthens detection of polymorphic, sand box-aware, and AI-generated attacks
- Monitors internal traffic for signs of compromised accounts

Intent-Aware AI (VIPRE IES)

IES uses adaptive machine learning to continuously evolve threat detection capabilities.

- Flags suspicious behavior, even without known indicators
- Learns new tactics as attackers evolve
- Provides explainable, transparent alerts to build trust in automation

Policy Control & Email Governance (VIPRE ATP)
VIPRE ATP provides granular control over email traffic, capabilities not available in IES alone.

- Advanced email routing, message disclaimers, and large message handling
- Outbound scanning and TLS enforcement
- Data Loss Prevention (DLP) and enforced encryption policies
- Ideal for regulated environments and hybrid cloud/ on-prem setups

Sandboxing & URL Protection
VIPRE ATP and IES both include sandboxing and link protection, but in different stages of the attack lifecycle.

- VIPRE ATP rewrites and sandboxes attachments and links before delivery
- IES inspects post-delivery behavior and lateral movement using the same sandbox engine
- This extends visibility and stops threats that activate later or originate from compromised internal accounts

Microsoft 365 Native Integration (VIPRE IES)
As IES integrates via an API, there is no need to reroute email or change MX records.

- Scans mail in real-time, directly within Microsoft 365
- Enables post-delivery remediation and automation
- Maintains native email flow for performance and reliability

Post-Delivery Remediation (VIPRE IES)
VIPRE IES acts after an email is delivered, detecting and removing threats that traditional SEG solutions may miss.

- Removes threats from inboxes instantly, even after delivery
- Automates response workflows to prevent lateral spread
- Reduces dwell time, supports audit logging, and preserves continuity

Email Continuity & Replay (VIPRE ATP)
VIPRE ATP ensures communication continues during outages and accidental deletion.

- Always-on email continuity during Microsoft 365 downtime
- 90-day email replay to resend or retrieve messages
- Minimizes disruption, supports compliance and legal hold requirements

Centralized Management (Both)
VIPRE IES and ATP are managed via intuitive dashboards tailored for lean IT teams.

- Role-based access control
- Integrated alerting and guided workflows
- Rapid deployment with smart defaults
- Unified visibility into threats, routing, and compliance

Why Combine VIPRE ATP, and VIPRE IES?

Because modern email threats aren't one-dimensional.
VIPRE's Total Email Protection merges the strength of perimeter filtering (VIPRE ATP) with the intelligence of post-delivery analysis (VIPRE IES), creating a layered, adaptive, and comprehensive email security posture.

As entities move more workloads to the cloud, Integrated Cloud Email Security (ICES) is the future of email security. Cloud-native and adaptive, it was built to protect the hybrid, AI-driven threat reality. Harnessing the strengths of VIPRE's ATP, and IES, it offers a powerful, layered defense where legacy resilience meets modern agility. You don't have to choose one; you can have the best of all worlds, now and in the future.

VIPRE Total Email Protection

One Platform. Multiple Layers of Defense

Perimeter filtering and inbox detection work better together. With VIPRE ATP handling the volume and VIPRE IES catching what's left, TEP reduces risk across every stage of an email attack.

Built for Midmarket Security Teams

Smart automation, intuitive controls, and native Microsoft 365 integration mean faster setup and lower overhead. No rerouting. No complexity. Just stronger protection with less effort.

Protection That Evolves With the Threat

Attackers adapt. So does VIPRE. The platform learns continuously from real-world data and adjusts to new phishing and impersonation tactics in real time.

Compliance Without Compromise

For organizations with compliance requirements, VIPRE ATP provides granular control over encryption, routing, and DLP policies, while VIPRE IES delivers visibility and detection that meet audit expectations.

Support for Hybrid Environments

TEP supports staged transitions to the cloud. Whether you're fully on Microsoft 365 or running hybrid, you can deploy VIPRE ATP and VIPRE IES in parallel, without disrupting email flow.

What You Get

- Real-time phishing and BEC protection
- Sandboxing and exploit defense
- Business continuity and 90-day email replay
- DNS/browser-based link isolation
- Encryption and data loss prevention (DLP)
- Native Microsoft 365 integration
- Policy and outbound routing control
- AI and signature-based detection
- 24/7 protection and expert support

Bottom Line

VIPRE Total Email Protection is more than a platform, it's a strategy. By combining VIPRE ATP with VIPRE IES, you get a smarter, stronger, more adaptive way to defend against modern threats.

Best-in-class email security, before and after the inbox. Seamless. Scalable. Built for Microsoft 365.

Want to see it in action?

CLICK HERE

About VIPRE

VIPRE is a leading provider of internet security solutions purpose-built to protect businesses, solution providers, and home users from costly and malicious cyber threats.

Our award-winning software portfolio includes comprehensive endpoint, email and web security, plus threat intelligence for real-time malware analysis, delivering unmatched protection against today's most aggressive online threats.

VIPRE Portfolio: Email Security | Endpoint (EDR & MDR) | SAT | SafeSend

Part of Ziff Davis Group: CNET | IGN | Humble | Mashable | MOZ | OOKLA | PC MAG

VIPRE SECURITY GROUP

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+45 7025 2223

©2025 VIPRE Security Group. All rights reserved. VIPRE is a registered trademark of Ziff Davis, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies. VIPRE_2025_DS_VIPRE_IES_0714_US