nexustek

NexusTek AI Email Security White Paper

WHY EMAIL SECURITY CAN'T WAIT

A Modern Guide For IT and Security Leaders

Executive Summary

Email remains the primary entry point for cyberattacks, with phishing accounting for 16% of all breaches.[1] Modern attackers do not rely on obvious tactics or malware-laced attachments. Instead, they exploit identity, trusted context, and collaboration workflows to operate invisibly inside an organization's cloud environment. Traditional secure email gateways, built for on-premises infrastructure, cannot provide the in-tenant visibility or behavioral analysis required to detect these attacks.

Meanwhile, financial exposure continues to rise. Phishing-driven breaches average millions in total incident cost. Business Email Compromise (BEC) schemes, a subset of phishing-based fraud, averaged $4.9 million in financial losses per incident.[2] Organizations also face increasing pressure from cyber insurers, regulators, and boards as modern attacks outpace the capabilities of legacy email defenses.

This white paper outlines how email threats have evolved, the business risks of relying on outdated defenses, and why cloud-integrated, AI-driven protection delivered through a managed service model is now foundational to modern security operations.

The Modern Threat Landscape

A finance manager at a regional company received a routine vendor update. Same contact. Same thread. Same tone. She replied, moved on, and thought nothing of it. Hours later, attackers using her legitimate session token accessed financial records from a different city without tripping any alerts. The email looked routine, and that was enough.

This scenario reflects a broader shift in how email threats operate. Attackers now insert themselves into active workflows, impersonating vendors, executives, or internal staff with messages that appear timely and contextually accurate.

These attacks succeed because they appear credible, not because they contain malicious payloads. None of this triggers a perimeter gateway because nothing in the message is technically malicious, only contextually suspicious.

Growing collaboration ecosystems amplify this risk. Tools like Microsoft Teams, SharePoint, OneDrive, and Slack are now common channels for sharing links and files. Attackers target whichever platform employees trust most, and traditional email security tools sitting on the perimeter cannot see or inspect these internal communications.

Modern email threats exploit context and trust rather than obvious technical weaknesses.

Why These Attacks Succeed: Three Fundamental Shifts

1

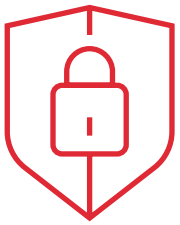
AI-Driven Social Engineering

Attackers now use AI to generate messages that mirror corporate tone, timing, and writing style. These emails reference active projects, invoices, or internal workflows, making them appear legitimate to both employees and traditional detection tools. AI enables attackers to craft individualized messages at scale, bypassing signature-based or rule-based controls.

2

Identity-Centric Attacks

Email is now a pathway to authentication tokens, session cookies, and OAuth authorizations attackers can exploit. A single phishing page can capture a valid token, bypassing multi-factor authentication entirely. Once inside, attackers operate as authenticated users, making behavioral detection essential.



3

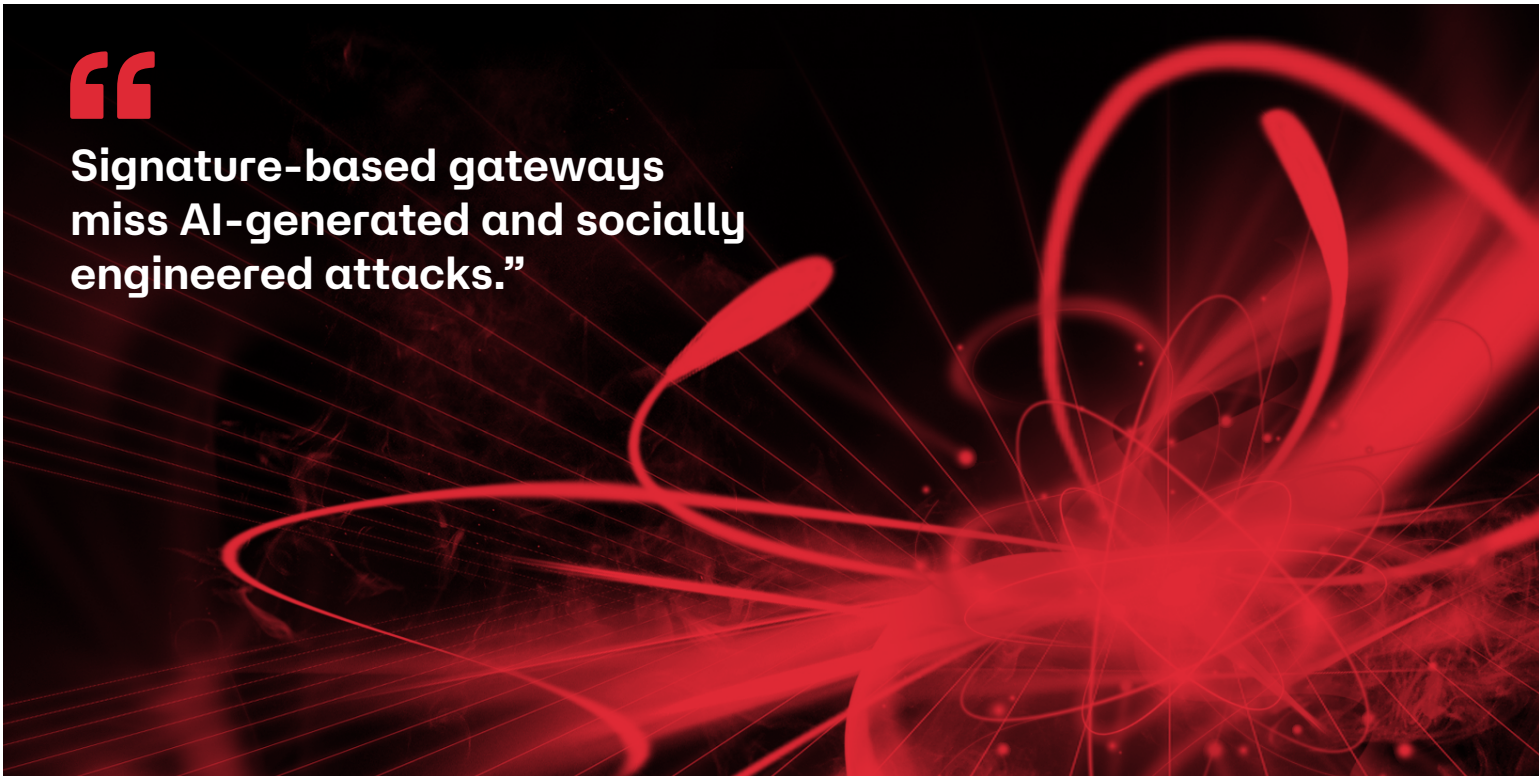
The Collaboration Surface Expansion

Organizations rely on a wide ecosystem of communication tools, and attackers target whichever channel users trust most. Traditional gateways were never designed to monitor internal Teams chats, SharePoint links, or Slack messages. As a result, the attack surface has expanded dramatically while visibility from legacy tools has stayed the same.

Why Now: The Business Imperative for Modernization

Multiple forces have converged to transform email security modernization from a future consideration into an immediate priority. According to IBM X-Force, 30% of all intrusions in 2024 used valid account credentials.[3] Attackers are logging in, not breaking in.

THE AI ARMS RACE IS ACCELERATING. Generative AI enables personalized phishing at unprecedented scale. Organizations relying on pattern-based defenses are fighting today's threats with yesterday's tools. Countering AI-powered attacks requires AI-powered defenses.



INSURANCE REQUIREMENTS ARE TIGHTENING. Cyber insurers have dramatically tightened underwriting requirements. Email security controls now appear on every coverage questionnaire, and inadequate protection leads to denied claims, coverage exclusions, or prohibitive premiums.

REGULATORY PRESSURE CONTINUES TO MOUNT. Frameworks including GDPR, CCPA, and industry-specific mandates increasingly hold organizations accountable for data breaches. Fines for inadequate security controls can reach tens of millions.

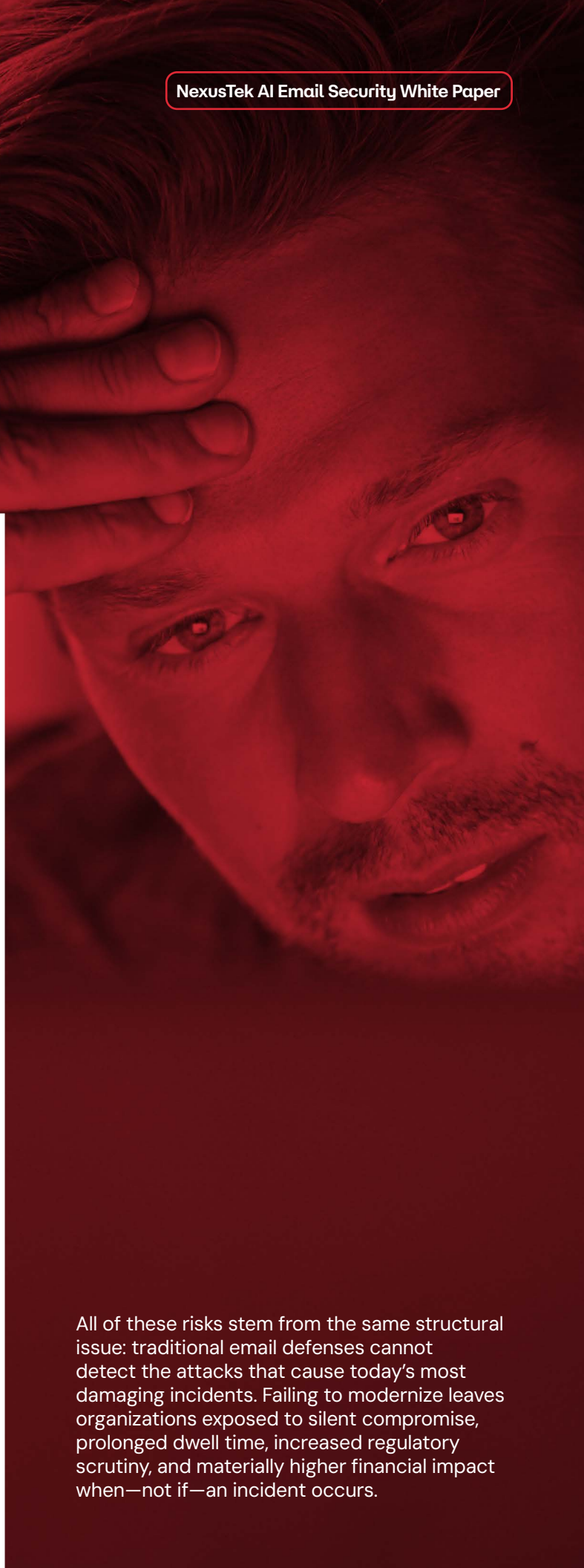
BOARDS ARE ASKING HARDER QUESTIONS. Security expectations have reached the executive level. Board members demand visibility into security posture and risk exposure. Email security now appears as a standing agenda item in board-level risk discussions.

THE TALENT SHORTAGE SHOWS NO SIGNS OF ABATING. The cybersecurity skills gap has widened by 8% since 2024, with two-thirds of organizations reporting they lack essential talent. Only 14% have confidence they possess needed expertise. Organizations cannot hire their way to better security.[4]

These financial and regulatory pressures coincide with internal constraints that make it increasingly difficult for teams to operate modern email defenses on their own.

The Cost of Inaction

Organizations that delay modernization face compounding financial, operational, and compliance exposure. Email remains a starting point for security incidents, and the majority of these involve stolen credentials, vendor impersonation, or account takeover rather than malware. When legacy controls fail to detect these attacks, the downstream impact is substantial.



$4.9 million

Financial losses escalate quickly. **BEC incidents now average $4.9 million per event**,[5] but the direct loss is only part of the cost. Post-incident containment, legal review, forensic consulting, and mandatory notifications routinely add six-figure to low-seven-figure expenses even for mid-market organizations.

> 200 days

Operational fallout is equally disruptive. Credential misuse incidents often go undetected for weeks or months, creating prolonged exposure windows where attackers exfiltrate data, manipulate payments, or expand laterally across collaboration platforms. Average dwell times for credential-based intrusions **exceed 200 days**,[6] leaving organizations with extensive uncertainty about what was accessed, what was altered, and what may still be compromised.

Millions per violation

Regulatory and contractual consequences add additional risk. GDPR, CCPA, and industry-specific regulations impose heavy penalties for preventable breaches, and in some cases reaching **millions per violation**. Many organizations must also notify customers, partners, and vendors when compromised email accounts may have exposed sensitive information, creating reputational fallout and erosion of trust.

All of these risks stem from the same structural issue: traditional email defenses cannot detect the attacks that cause today's most damaging incidents. Failing to modernize leaves organizations exposed to silent compromise, prolonged dwell time, increased regulatory scrutiny, and materially higher financial impact when—not if—an incident occurs.

Why Legacy Defenses Are Failing

Traditional email security tools were built for a very different era. They assumed organizations ran on-premises mail servers, traffic flowed through a predictable perimeter, and attacks announced themselves with malicious attachments or obvious patterns. None of that matches how threats work today. As cloud adoption has grown, these older architectures have produced four persistent blind spots that attackers exploit every day.

PERIMETER-BOUND ARCHITECTURES MISS IN-TENANT ACTIVITY

Secure email gateways sit outside Microsoft 365 or Google Workspace and inspect mail before delivery. That external position limits what they can see. They cannot observe how messages behave once inside the tenant, cannot evaluate authentication context, and cannot correlate activity across email, OneDrive, Teams, or SharePoint. In short: they filter the envelope, not the environment.

SIGNATURE-DRIVEN DETECTION CANNOT KEEP PACE WITH AI-GENERATED THREATS

Most legacy tools still rely on known-bad indicators: familiar URLs, sender patterns, file hashes, or rule-based heuristics. Modern phishing and BEC attacks are personalized, AI-written, and unique to each target. They contain no malicious payloads and no artifacts to match against a threat feed. When nothing looks suspicious "on paper," pattern matching fails by design.

MX RECORD ROUTING CREATES PREDICTABILITY AND A SINGLE POINT OF FAILURE

Because SEGs require rerouting MX records, attackers can easily identify which solution an organization uses and tune their campaigns around it. Worse, redirecting mail through a gateway often forces organizations to suppress native Microsoft or Google protections to avoid conflicts. If the gateway misses something—or is bypassed altogether—there is no second layer waiting behind it.

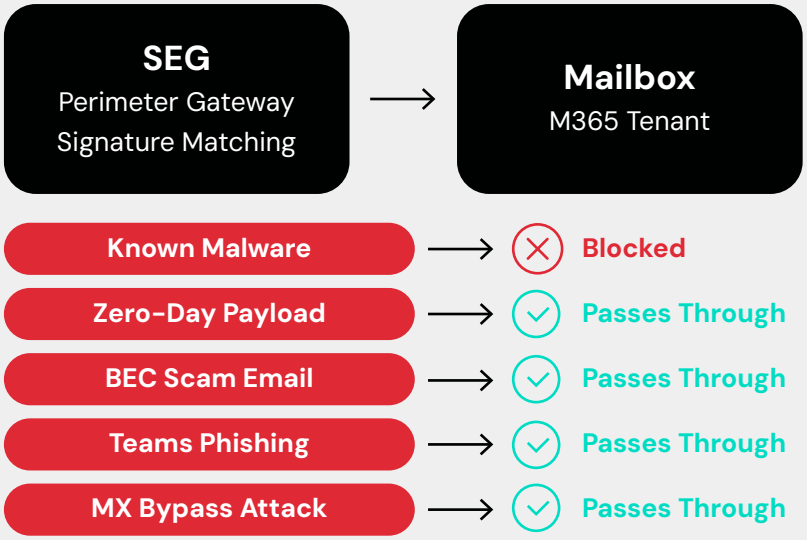
NO VISIBILITY INTO INTERNAL OR LATERAL COMMUNICATIONS

Once a user is compromised, attackers rarely continue with inbound messages. They pivot internally—sending updated invoices to finance, sharing documents with colleagues, or impersonating executives. Because gateways only monitor mail passing through the perimeter, they never see this lateral movement. The most damaging part of an attack often unfolds entirely out of view.

These four limitations share a common theme: legacy tools were built to filter traffic at the edge, but today's attacks unfold inside the cloud, inside accounts, and inside trusted relationships. As long as detection sits outside the environment being attacked, organizations will continue to face blind spots that modern threat actors exploit with ease.

Legacy Secure Email Gateway

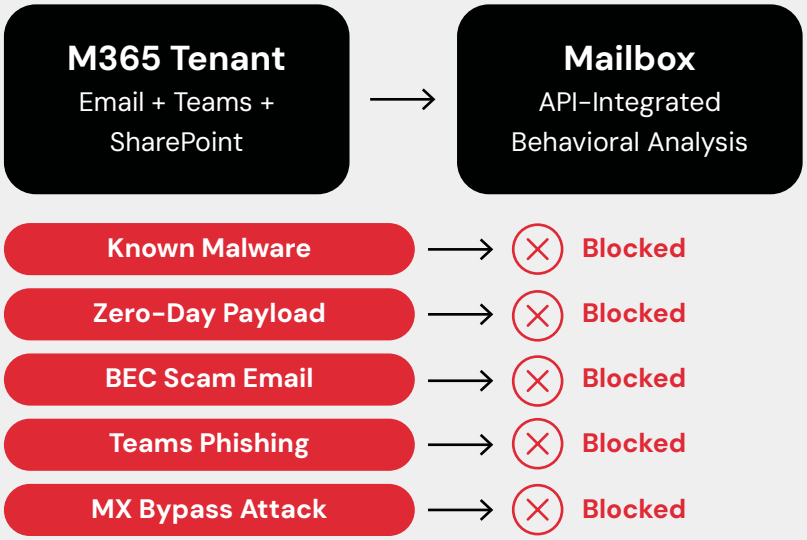
Outside Tenant • MX Record Routing • Signature-Based Detection



Known Malware: **Blocked**
Zero-Day Attacks: **Allowed**
BEC/Impersonation: **Allowed**
Teams/SharePoint Threats: **Allowed**

Cloud-Native Protection

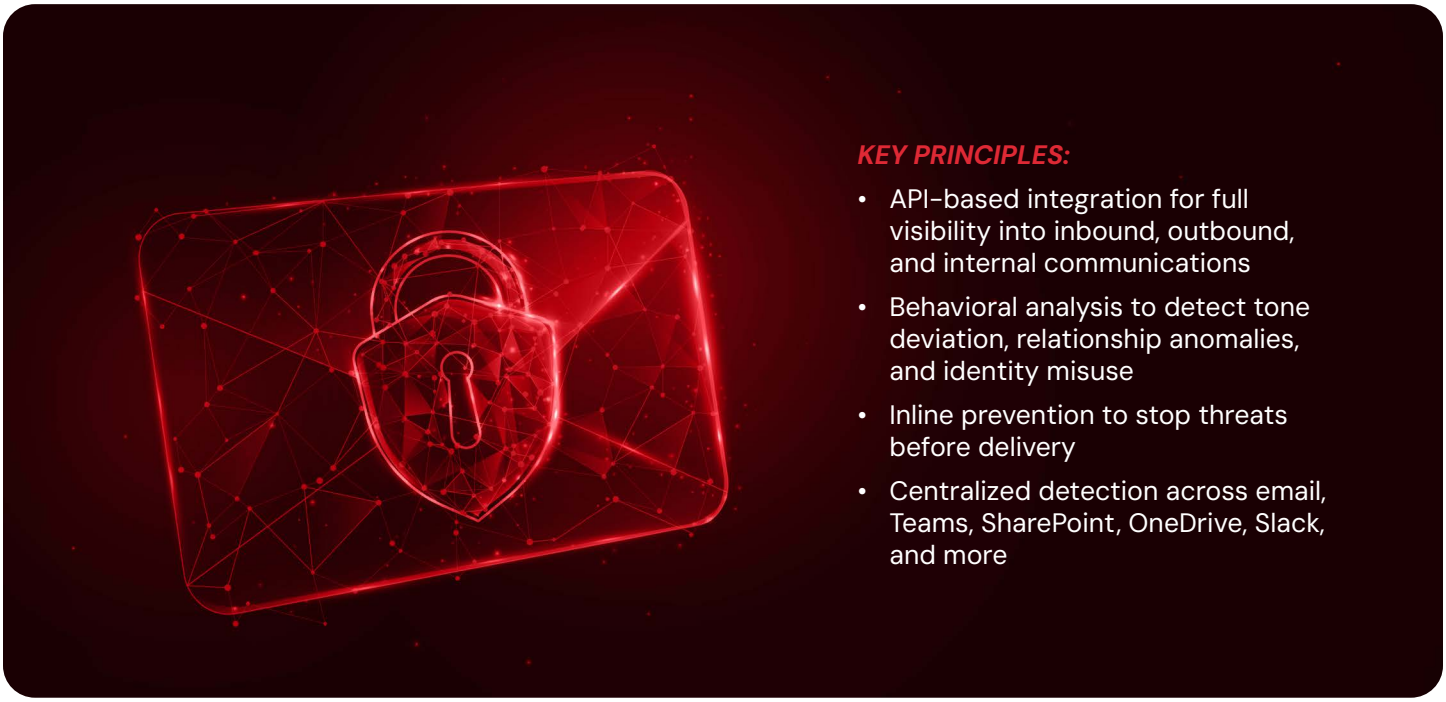
Inside Tenant • API Integration • Behavioral / AI Analysis



Known Malware: **Blocked**
Zero-Day Attacks: **Blocked**
BEC/Impersonation: **Blocked**
Teams/SharePoint Threats: **Blocked**

The Modern Approach: Cloud-Native, AI-Driven Email Security

Modern protection requires deep, in-tenant visibility and behavioral analysis across both email and collaboration platforms. Instead of inspecting traffic outside the cloud, modern solutions operate inside Microsoft 365 and Google Workspace, where attacks are occurring more frequently. This model is fundamentally different from post-delivery scanning. Modern solutions evaluate messages inline, prior to inbox delivery, and do so from inside the tenant rather than at the perimeter.



KEY PRINCIPLES:

- API-based integration for full visibility into inbound, outbound, and internal communications
- Behavioral analysis to detect tone deviation, relationship anomalies, and identity misuse
- Inline prevention to stop threats before delivery
- Centralized detection across email, Teams, SharePoint, OneDrive, Slack, and more

This model ensures threats are blocked before users see them, without modifying MX records or disabling native platform protections.

Effective protection requires inline prevention: blocking threats before they reach users. Modern solutions intercept and analyze messages in transit, quarantining malicious content before delivery rather than racing to remediate after the fact. The goal is prevention, not faster incident response.

NexusTek AI Email Security

NexusTek delivers this modern model through a cloud-integrated, AI-driven platform paired with expert human analysis. The solution prevents phishing, BEC, account takeover, malware delivery, and impersonation attempts across email and collaboration platforms.

CAPABILITIES INCLUDE:

- Behavioral and identity-based threat detection
- Inline prevention before inbox delivery
- Advanced phishing and BEC detection
- Account takeover and token-misuse monitoring
- Unified inspection across collaboration tools

BUSINESS OUTCOMES:

- Reduced risk of financial loss and data exposure
- Stronger identity and collaboration security
- Faster response and clearer visibility
- Lower operational burden for IT and security teams

NexusTek's managed service provides continuous monitoring, threat investigation, tuning, and reporting. Our security analysts triage alerts, investigate suspicious activity, and escalate when needed—reducing workload on internal teams while improving detection accuracy.

Why NexusTek?

98% customer satisfaction

30+ years
of Service Excellence

1,200+
Active Clients

98%
Client Satisfaction Rating

10X years
in a row CRN MSP500 Ranking

250+
Skilled Engineers

48 states+
Canada, Europe, and Mexico

100+
Strategic Partnerships

~6 years
Average Client Relationships

Conclusion

Email security is no longer a peripheral IT function. It directly impacts operational continuity, financial performance, and organizational reputation. The nature of attacks has changed: AI enables adversaries to craft messages indistinguishable from legitimate communication, while credential theft and token abuse bypass traditional defenses entirely.

Legacy secure email gateways, designed for on-premises infrastructure and signature-based detection, are structurally mismatched to these realities. They lack internal visibility, expose security architecture through public MX records, collapse defense-in-depth by replacing native protections, and miss the sophisticated attacks that define today's threat landscape.

Cloud-native email security, powered by artificial intelligence and delivered through a managed service model, addresses both the threat landscape and operational challenges facing IT and security teams. The choice is straightforward: continue relying on architectures designed for yesterday's threats, or modernize protection to match the sophistication of today's attackers.

The question is not whether your organization will face sophisticated email-based attacks. It is whether you will be prepared when they arrive.

Organizations that modernize their email defenses strengthen not only security, but the resilience and reliability of their entire digital business.

1. **Schedule a technical review** to assess your current email and collaboration security posture.
2. **Request a security assessment** to identify gaps and prioritize improvements.
3. **Deploy a pilot environment** to experience modern email protection in your own infrastructure.

Learn more at
nexustek.com/ai-email-security-managed-solutions

SOURCES
1) IBM, Cost of a Data Breach Report 2025, 2025.
2) Hoxhunt, Business Email Compromise Statistics, March 2025.
3) IBM, X-Force Threat Intelligence Index 2025, 2025.
4) World Economic Forum, Global Cybersecurity Outlook 2025, January 2025.
5) Hoxhunt, Business Email Compromise Statistics, March 2025.
6) IBM, Cost of a Data Breach Report 2025, 2025.

nexustek