Abnormal

The Essential Guide to Retiring the SEG

Rethinking Email Security Architecture for the Cloud and AI Era

Email Security in the Cloud-Native Era

$10.22M

Is the average cost of a breach in the United States

IBM Cost of Data Breach Report 2025

68%

Of breaches stem from exploited human behavior

Verizon DBIR 2025

$2.8B

Lost to Business Email Compromise in 2024

FBI Internet Crime Report 2024

Over the past decade, organizations have shifted from server-bound email to fully cloud-native communication, bringing speed, scale, and flexibility along with them. Attackers have followed that shift closely. Where once they relied on malicious payloads and recognizable signatures, today's threat actors operate by exploiting context, trust, and human behavior. Their most effective attacks contain no obvious indicators at all.

Secure email gateways (SEGs) were built for a different generation of threats. Their filtering logic was designed to stop known bad content before it reached the inbox, a model that worked when most attacks were signature-driven and perimeter-based. Today, messages often originate from legitimate services, compromised vendor accounts, and well-crafted impersonations. They pass SPF, DKIM, and DMARC. Increasingly, they are machine-generated, allowing attackers to adapt quickly and mimic familiar communication styles with little effort.

The result is an erosion in the marginal value of standalone, third-party SEGs. Even heavily tuned gateways often miss modern attacks while still demanding significant operational effort to maintain. For many organizations, this imbalance between effort and protection has prompted a closer examination of whether a separate gateway layer continues to justify its cost and complexity.

Importantly, this shift in thinking does not fully remove the SEG layer itself. Native protections in Microsoft 365 and Google Workspace continue to provide foundational email filtering, while organizations reassess the need for separate third-party gateways that often duplicate those same controls.

Modern email security architectures focus on extending native cloud protections to address threats that bypass traditional SEG detection. Rather than treating email security as a single, perimeter-bound control, organizations are evaluating architectures that add contextual, behavior-based detection and remediation alongside existing platform defenses.

This guide explores what that approach looks like in practice. It examines the modern attack techniques that consistently bypass legacy defenses, the operational and economic impact of maintaining a third-party SEG, and the capabilities required to protect cloud email in an environment shaped by behavioral manipulation and AI-driven adversaries. It also provides a clear roadmap for retiring the third-party SEG and understanding what day-to-day operations look like after the shift.

Table of Contents

Modern Attacks Bypassing the SEG

As cloud email platforms have matured, attackers have shifted toward exploiting the human and relational elements of communication rather than relying on payloads or obvious indicators of compromise. The most damaging attacks now often arrive as clean, text-only messages that mimic trusted workflows.

These attack patterns highlight the limitations of standalone, gateway-based inspection when confronted with identity-driven and socially engineered threats.

Traditional gateway inspection, built to identify spam, known malware, and signature-based threats, cannot interpret the subtle markers that define these campaigns. With generative AI enabling adversaries to imitate communication styles and gather organizational detail at scale, these attacks increasingly blend into legitimate business traffic.

Why Modern Attacks Get Through SEGs

- No payloads → pass scanning
- Legitimate sending infrastructure → pass authentication
- AI-written content → no linguistic anomalies
- Familiar communication patterns → no heuristic flags
- Vendor impersonation → exploit trusted relationships

Business Email Compromise and Executive Impersonation

BEC attacks target the relationships within an organization. Messages often mimic an executive's tone, reference ongoing projects, or request urgent action. When adversaries compromise a legitimate mailbox or use well-crafted impersonation, they gain access to authentication signals that SEGs trust, such as clean domains, intact DMARC, and a conversational writing style. These messages contain no payloads and pass standard checks, making them difficult for traditional filters to detect and easy for recipients to accept as genuine.

Vendor Email Compromise and Supply Chain Fraud

Attackers increasingly infiltrate the mailboxes of trusted vendors or create convincing look-alike identities to insert themselves into real financial workflows. The emails they send include accurate invoice data, payment timing, or contract details scraped or stolen from prior correspondence. Because these messages originate from legitimate accounts and follow established communication norms, they bypass SEG logic and often rely on a single employee to spot subtle inconsistencies before a fraudulent payment is made—an unreliable final safeguard.

Credential Phishing and Multi-Step Social Engineering

Rather than delivering an obviously malicious link, modern phishing campaigns rely on benign-looking services, layered redirects, or well-known file-sharing platforms to stage credential theft. Each step appears harmless, but the sequence leads the user to an attacker-controlled authentication page. These multi-stage attacks deliberately avoid the threat markers SEGs depend on, reducing the likelihood of detection while increasing the probability of a single moment of user error.

OAuth and Third-Party App Abuse

Instead of stealing passwords, adversaries now attempt to trick users into granting OAuth permissions. A single approved consent request can give persistent access to mail, files, calendars, or contacts. Because the email prompting the action originates from a legitimate cloud provider and links to a genuine-looking consent screen, perimeter defenses have no clear basis for blocking the message.

Payloadless and Hybrid Social Engineering

In many cases, attackers avoid email-based payloads entirely to escape detection. They begin with a harmless-looking message and then transition to another communication channel—phone, SMS, or a messaging app—to deliver instructions or request sensitive actions. The email serves only as an entry point, offering no malicious content for a SEG to analyze, yet establishing enough credibility to allow the attack to progress.

AI-Assisted Personalization at Scale

Generative AI has made it dramatically easier for attackers to personalize messages and scale their operations. With minimal input, AI can imitate writing styles, gather insight into corporate hierarchies, and create highly tailored emails that blend seamlessly into organizational communication patterns. These messages lack the linguistic anomalies that once signaled phishing and are designed specifically to evade static detection rules.

Static Filters vs. Dynamic Threats

Traditional SEG Logic

- Relies on known-bad indicators
- Filters based on rules, signatures, and heuristics
- Focuses on payloads, spoofing, and obvious anomalies

Modern Attack Reality

- No payloads to scan
- AI-crafted content tailored to recipients
- Identity abuse and supply chain compromise
- Legitimate domains and accounts
- Behavioral manipulation instead of technical exploits
- Attack signals distributed across systems and channels

Across all these attack patterns, the failure mode is consistent: legacy filters evaluate content, while modern threats exploit context. As long as detection hinges on static indicators rather than identity and behavior, attackers will retain the advantage.

The Economics of Retiring Your Third-Party SEG

Email remains one of the highest-volume communication channels inside the enterprise, and early secure email gateways were designed for that world, built to filter large quantities of spam and known-bad content at the perimeter. For many years, this offered meaningful value. But as cloud platforms have evolved, the cost structure of maintaining a separate gateway has changed—often significantly.

Today, Microsoft 365 and Google Workspace provide strong native protections against commodity threats, including spam, basic phishing, and known malware. When those capabilities are combined with a modern behavioral detection layer, much of the third-party SEG's functionality becomes redundant. Yet the operational overhead of maintaining a superfluous gateway remains high.

For many organizations, this creates a mismatch: **they continue paying for a tool that duplicates baseline filtering while offering limited benefit against the threats that matter most.**

Beyond licensing, the economic impact shows up across several dimensions.

Operational Complexity and Analyst Overhead

SEGs require constant upkeep, such as rule tuning, policy adjustments, allow/deny list management, and frequent troubleshooting when legitimate mail is delayed or blocked. Analysts spend hours triaging false positives, reviewing quarantined messages, and adjusting rules for new attack patterns.

The result is a steady drain on SOC time. Even with experienced teams, the gateway often demands disproportionate manual effort for diminishing security returns. This burden is especially visible in large environments where thousands of messages are flagged daily and require manual analyst review.

Cloud-native email platforms and modern API-based security tools automate much of this operational labor, decreasing dependency on manual filtering decisions and reducing alert fatigue so that teams can focus on high-priority issues.

Redundant Spend Across Overlapping Tools

Most organizations running a third-party SEG today also rely on the native controls built into their cloud email platform. This creates duplicated functionality in:

- **Spam filtering**
- **Basic phishing defenses**
- **Commodity malware detection**
- **URL inspection and sandboxing**

When these capabilities exist both in a third-party SEG and in the cloud platform, organizations pay twice for similar outcomes—once in direct licensing costs and again in operational time spent managing parallel systems.

Consolidating onto a cloud-native model often reduces both tool spend and total cost of ownership, without compromising coverage.

Where SEG Costs Accumulate

- Licensing and maintenance fees
- Continuous rule tuning and policy updates
- SOC time spent triaging false positives
- Investigations of delayed or blocked legitimate mail
- Duplicate filtering efforts across SEG + native cloud tools
- Operational drag from maintaining parallel systems

The Hidden Cost of Delayed Detection

When SEGs miss advanced, low-signal attacks—phishing without payloads, vendor impersonation, multi-step fraud—the downstream costs are significant. These threats often result in account compromise, invoice manipulation, or data exposure, requiring extensive remediation effort across IT, security, and finance teams.

Economic impact goes well beyond the immediate incident, and includes:

- **Incident response and forensics**
- **Recovery and reporting requirements**
- **Reputational and third-party impacts**
- **Business disruption**
- **Lost productivity during investigation**

The longer these attacks go undetected, the broader and more disruptive the downstream impact becomes.

Modernization Pressure and Cloud-Native Efficiency

Across industries, organizations are modernizing their security stacks to reduce complexity and adopt architectures aligned with cloud-first operations. In this environment, legacy appliances and inline filters introduce points of friction, such as latency, routing dependence, and manual configuration overhead, which no longer match how cloud email systems operate.

Retiring a third-party SEG is often part of this broader shift to:

- **Simplify the email routing path**
- **Reduce reliance on static rules**
- **Decrease total cost of ownership**
- **Centralize policy management**
- **Align defenses with identity-driven, contextual detection**

This transition is not simply about cost savings; it is about ensuring security investments reflect the realities of modern cloud workflows and AI-assisted threats.

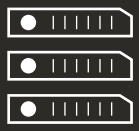
A More Sustainable Model for Email Security

For many organizations, the case for retiring a third-party SEG becomes clear when evaluating the balance between cost, effort, and protection. Maintaining a separate perimeter tool demands continuous operational investment yet provides limited benefit against today's biggest threats.

A more sustainable approach layers behavioral detection on top of strong native defenses, eliminates duplicate filtering, and reduces manual workload—ultimately focusing security resources where they have the greatest impact.

Where Third-Party SEGs Add Cost Without Coverage

Third-Party SEG (Legacy)



Adds Cost

- Licensing
- Routing complexity
- Rule tuning

Limited Protection

- Signature-based detection
- Payload focus
- Weak behavioral/identity insight

Native Cloud + Behavioral Layer

Provides Baseline + Advanced Coverage

- Spam/malware (native)
- Behavioral + identity detection

Less Overhead

- No inline routing
- Minimal configuration
- Automated remediation

▸▸ *Third-party SEGs add cost without delivering meaningful additional protection. Cloud-native filtering plus behavioral detection provides stronger coverage with far less overhead.*

What a Modern Email Security Platform Must Deliver

As organizations modernize their security stacks, they increasingly look for tools that complement native cloud protections rather than duplicate them. Strong baseline filtering from Microsoft and Google now handles much of the commodity threat landscape, but advanced attacks—those that exploit identity, context, and human trust—demand a different approach.

This perspective is consistent with analysts' guidance for email security buyers in 2025, which emphasizes a layered approach that pairs core email security controls with complementary or supplemental solutions to address modern threats, while prioritizing integration, operational simplicity, and total cost of ownership.

A modern email security platform must integrate deeply with cloud ecosystems, analyze behavior rather than static indicators, and automate the work that once required constant human intervention. The following capabilities define what security teams now expect from a next-generation solution.

01 Behavioral and Identity-Centric Detection

Modern attacks rarely depend on malicious payloads. Instead, they exploit relationships, conversation histories, and established communication patterns. A modern platform must:

- **Build a dynamic understanding of normal behavior across email users and vendors**
- **Detect subtle anomalies that indicate social engineering or impersonation**
- **Analyze identity signals, communication tone, and relationship patterns**
- **Identify risks even when messages contain no traditional indicators**

Where legacy systems search for the "known bad," modern systems must identify the **unexpected**, the **uncharacteristic**, and the **behaviorally suspicious**. To do this, they must also be able to identify the "good," or the baseline of everyday ordinary communications across the enterprise.

02 API-Based Access to Cloud Signals

Inline filtering alone is no longer sufficient for cloud email. Modern collaboration platforms require visibility into signals that SEGs cannot access, including:

- **Authentication patterns and unusual sign-in activity**
- **Device, location, and IP anomalies**
- **Directory relationships and organizational structure**
- **Changes to mailbox rules and forwarding behavior**
- **Third-party app permissions and OAuth risk**

API-level integration allows security tools to analyze identity, context, and message behavior holistically—something impossible through perimeter inspection alone.

03 Autonomous Remediation and SOC Efficiency

Security teams cannot manually process every suspicious message, nor should they have to. A modern platform must reduce operational burden by:

- **Automatically remediating high-confidence malicious emails**
- **Handling routine triage tasks without analyst intervention**
- **Reducing false positives through contextual understanding**
- **Removing threats from user inboxes in real time**
- **Surfacing only high-risk incidents for review**

Modern defenses must not only detect more. They must **demand less** from the busy SOC.

04 Supply Chain and Vendor Relationship Intelligence

As vendor email compromise becomes increasingly common, organizations must understand not just their own communication norms but also the behavior of the suppliers and partners they rely on. A modern platform must:

- **Map vendor communication patterns over time**
- **Detect deviations in tone, timing, financial workflows, or sender infrastructure**
- **Identify newly compromised or suspicious vendors**
- **Surface risk signals across cross-organizational relationships**

Protecting inbound communication is no longer enough; defenses must extend across the supply chain.

05 Multi-Channel Protection Across Cloud Applications

Communication no longer lives in email alone. Attackers increasingly pivot across applications such as messaging platforms, calendars, file-sharing tools, HR portals, and more. Modern email security must evolve alongside this reality:

- **Detect suspicious activity across interconnected cloud applications**
- **Prevent cross-channel social engineering attempts**
- **Recognize identity compromise in one system that impacts another**
- **Provide unified visibility across collaboration, identity, and workflow tools**

A single compromised identity can move laterally with little friction; defenses must be able to follow it.

06 Cloud-Native Architecture and Operational Simplicity

Modern organizations expect tools that align with the flexibility and speed of the cloud. A next-generation platform must:

- **Deploy without rerouting mail flow**
- **Operate without creating new latency or points of failure**
- **Minimize maintenance overhead**
- **Avoid complex MX record changes**
- **Integrate seamlessly with existing cloud configurations**

The strongest platforms amplify cloud-native capabilities rather than working against them.

How Email Security Architecture Shapes Detection and Response

SEG	Inline API	API-Based (Asynchronous)
Pre-delivery inspection	Pre-delivery, cloud-connected inspection	Post-delivery, in-mailbox analysis
Content, reputation, and signature-based detection	Limited platform telemetry at delivery time	Full identity, behavioral, and historical context
Limited identity and behavioral context	Detection fixed at point of delivery	Continuous detection beyond delivery
Primarily inspects external inbound mail	Adds routing and configuration complexity	No inline routing or mail-flow disruption
Requires ongoing tuning and policy maintenance	Often overlaps with native or gateway controls	Automated, high-confidence remediation

A Foundation for the Cloud-Native Era

The capabilities outlined here reflect a shift from perimeter-based inspection to **intent-based**, **behavior-aware**, **cloud-integrated protection**. Modern email security platforms must not only detect advanced attacks but also reduce operational complexity, support cloud-first architectures, and strengthen identity-centric defense.

These requirements set the stage for the next section of this guide: **how organizations transition from legacy SEGs to modern platforms without disruption**.

Core Requirements for Modern Email Security

Behavioral + Identity-Centric Detection

Understands normal communication patterns and flags anomalies that suggest impersonation, manipulation, or compromise.

API-Based Cloud Visibility

Accesses identity, authentication, and message signals unavailable to perimeter filters.

Vendor + Supply Chain Intelligence

Monitors communication with external partners and detects deviations in financial or operational workflows.

Autonomous Remediation

Handles routine triage and removes malicious messages without manual intervention.

Cross-Channel Protection

Extends detection across cloud apps where communication, identity, or access can be exploited.

Cloud-Native Architecture

Deploys without routing complexity, latency, or manual overhead, aligning to modern email environments.

The Post-SEG Detection Model

Legacy SEG Model

- Perimeter inspection
- Static rules
- Payload-focused detection

Modern Platform Model

- API-based visibility
- Behavioral detection
- Identity + context analysis
- Autonomous remediation

The Migration Blueprint

Retiring a third-party SEG may seem daunting, especially for teams that inherited complex routing configurations or policy layers built up over many years. In practice, the transition to a modern, cloud-native architecture is far simpler than most expect. With the right planning and support, organizations can retire a standalone gateway while continuing to rely on native protections in Microsoft 365 or Google Workspace, all without disrupting mail flow and often with far less operational effort than maintaining the third-party layer itself.

A successful migration follows a well-defined set of stages, each focused on ensuring visibility, validating detection coverage, and moving configurations safely to the cloud email provider and modern security platform.

PHASE 01 Assessment and Planning

OBJECTIVE ▪ Understand the current routing, policies, and dependencies.

Teams begin by inventorying existing SEG configurations, including policy rules, transport routes, exception lists, and any downstream integrations. This assessment identifies which controls are redundant with native cloud protections, which need to be migrated, and which can be retired entirely.

Clear migration goals are set here: reduce routing complexity, simplify policy management, and enable behavioral detection without adding operational burden.

PHASE 02 Visibility and Evaluation (Monitor-Only Mode)

OBJECTIVE ▪ Establish confidence before removing the SEG.

Before any routing changes, organizations run the newly adopted platform in monitor-only mode alongside the existing SEG. This provides real-world visibility into attacks that bypass legacy filtering while confirming that native cloud protections handle commodity threats.

This evaluation period gives the SOC time to validate detection precision, understand alerting workflows, and compare outcomes, all without affecting mail flow.

PHASE 03 Configuration Migration and Policy Consolidation

OBJECTIVE ▪ Move essential controls from the SEG into the cloud-native environment.

Most SEG rules relate to basic hygiene—spam tuning, anti-malware settings, transport rules—now handled by Microsoft 365 and Google Workspace by default. Teams migrate or recreate only the policies that remain necessary, consolidating configuration into fewer, more efficient layers.

This phase reduces long-term operational overhead with fewer rules to maintain, fewer false positives, and fewer routing dependencies.

PHASE 04 Cutover and Routing Simplification

OBJECTIVE ▪ Remove the SEG from the mail flow safely.

Once visibility is validated and policies are consolidated, teams update routing to remove the SEG. By leveraging a cloud-native architecture, this transition avoids downtime, reduces latency, and eliminates unnecessary hops between systems.

Rollback paths are maintained during this stage, though most organizations complete cutover without needing to revert.

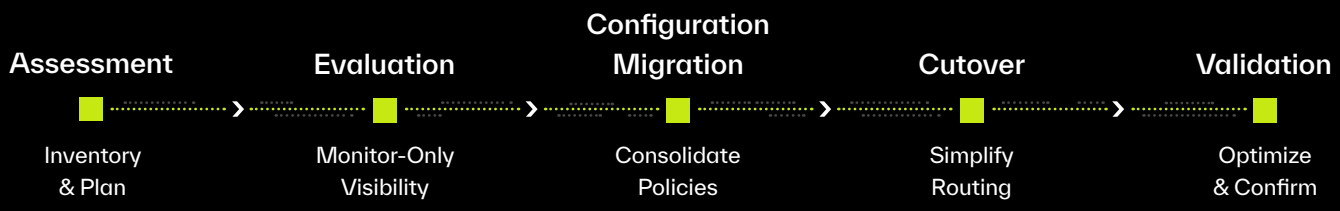
PHASE 05 Validation and Optimization

OBJECTIVE ▪ Confirm protection and operational efficiency.

After third-party SEG cutover, teams verify that mail flow remains stable, detection continues to perform as expected, and policy management is dramatically simpler. SOC teams typically experience an immediate reduction in manual triage burden and clearer visibility into identity- and behavior-driven threats.

The result is a more streamlined, cloud-aligned security architecture with fewer tools to manage and stronger protection against modern attacks.

Migration Timeline



Migrating off a secure email gateway is no longer a disruptive undertaking. With clear stages, monitor-only visibility, and a cloud-native architecture that removes routing complexity, organizations can strengthen their defenses while significantly reducing long-term operational overhead.

Life Beyond the SEG

Retiring a third-party secure email gateway marks a meaningful shift in how organizations defend their most valuable collaboration environments. With baseline filtering handled natively by cloud email providers and advanced detection delivered through behavioral, identity-centric security platforms, teams experience a simpler, more efficient, and more resilient operating model.

Once the SEG is removed from the mail flow, several benefits become apparent.

Stronger Protection Against Modern Attacks

With direct insight into user behavior, identity signals, and cross-channel patterns, modern platforms detect attacks that perimeter filters routinely miss: vendor compromise, credential theft workflows, conversational phishing, and identity misuse.

Organizations see fewer high-risk messages reaching inboxes and reduced reliance on employees to catch subtle anomalies.

Lower Operational Overhead

Maintaining a SEG demands ongoing tuning, troubleshooting, and review of quarantined or delayed messages. When those responsibilities shift to cloud-native filtering plus behavior-based detection, the operational burden on the SOC drops significantly.

This reflects the time reclaimed when teams no longer manage a separate perimeter appliance with its own rules, routing dependencies, and false-positive queues.

95%

Reduction in SOC operational overhead after retiring the third-party SEG and augmenting native protections with Abnormal

Simplified Architecture and Fewer Points of Failure

Removing the SEG eliminates an entire layer of routing complexity—no additional hops, no inline inspection delays, no dual-policy maintenance. Mail flows directly through the cloud provider, and advanced detection operates through API integration rather than traffic redirection.

The result is a more stable, cloud-aligned architecture with fewer components to maintain.

Greater Analyst Focus and Fewer False Positives

With behavioral analysis and automated remediation handling routine threats, analysts spend less time investigating low-confidence signals and more time on strategic work.

Teams report:

- **Dramatically fewer false positives**
- **Less repetitive triage**
- **Cleaner alert queues**
- **More consistent detection of socially engineered threats**

SOC fatigue decreases, and response effectiveness improves.

42%

Reduction in email security licensing costs after retiring third-party SEGs

Reduced Total Cost of Ownership

Organizations often discover that once commodity filtering is handled by native cloud tools, the SEG provides limited marginal value relative to its cost. Removing it reduces licensing fees, lowers operational labor, and consolidates maintenance into a smaller, more modern set of controls.

Security improves, but complexity and cost decline.

Setting the Foundation for Modern Cloud Defense

Life after the SEG is not simply an exercise in cost savings; it represents a transition to a security model designed for cloud collaboration environments and a threat landscape defined by AI-powered campaigns. With a combination of native controls and behavioral detection, organizations gain stronger resilience against identity-driven attacks while reducing the burden on their security teams.

This streamlined architecture forms the basis for future enhancements across the broader cloud ecosystem—supporting identity, collaboration, and workflow security at scale.

Conclusion

Secure email gateways were originally designed for an era defined by high-volume spam, known malicious payloads, and perimeter-based filtering. As organizations moved to cloud email platforms and attackers shifted to identity-driven, socially engineered threats, the assumptions behind standalone gateway models stopped aligning with how modern communication works.

Today's attacks rely on trust, context, and human behavior rather than the payloads and indicators traditional filters were built to detect. Meanwhile, native capabilities in Microsoft 365 and Google Workspace now provide strong baseline protection against commodity threats, reducing the value of maintaining a separate, duplicative gateway layer. The real challenge facing security teams is not filtering known-bad content, but recognizing the subtle deviations in behavior and intent that characterize modern compromise.

Retiring the third-party SEG is part of this broader shift toward cloud-aligned, behavior-aware security architecture. With clear migration paths, minimal disruption, and significantly reduced operational overhead, organizations can strengthen their defenses while simplifying the systems required to maintain them.

Modern email security depends on understanding people, identity, and the signals that connect them, not on adding more layers of perimeter inspection. By augmenting native cloud protections with behavior-based detection, organizations position themselves for a more resilient and efficient future.

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially-engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including over 20% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Curious to see how Abnormal AI fits in your environment?

Request a Demo ›

Curious to see how many threats could be bypassing your SEG?

Threat Assessment ›