todyl

Todyl 2025 Product Year in Review

As we close out 2025, we want to share what we built this year and why it positions you to win in 2026.

The Shift to Unified Assurance

The market is fundamentally changing. Your clients aren't just asking for security anymore—they're asking for proof. Cyber insurance underwriters scrutinize controls and demand evidence of continuous monitoring. Third-party risk assessments require detailed validation of security postures. Compliance frameworks that once applied only to enterprises now impact businesses of every size. And regulators expect organizations to demonstrate ongoing adherence, not just point-in-time certifications.

This shift from reactive security to continuous assurance changes what success looks like. It's no longer enough to prevent, detect, and respond to threats. Your clients need to validate controls, automate evidence collection, align with insurer requirements, and prove security and compliance outcomes to stakeholders who don't speak technical language.

That's why we're focused on Unified Assurance, the convergence of threat, risk, and compliance management into a single, continuous platform that delivers measurable protection, insurability, and resilience. It connects prevention, detection, and response with control validation, compliance enforcement, evidence automation, and insurer alignment.

This approach solves real problems you're facing. When clients receive questionnaires from insurance carriers or third parties asking detailed questions about their security controls, you need answers backed by evidence. When prospects evaluate your proposals against competitors, demonstrating measurable outcomes and compliance readiness wins deals. When renewals approach, showing continuous improvement in their security posture and risk profile keeps them from shopping around.

A unified platform delivers these outcomes in ways point solutions can't:

Prove outcomes, not just promise them - Integrated telemetry across network, endpoint, identity, and cloud provides comprehensive visibility into your security posture. Automated evidence collection and validation demonstrate to insurers, auditors, and clients that controls are working as intended. You're not claiming protection; you're proving it.

Deliver better security with less complexity - Threats don't respect product boundaries. When SASE, EDR, SIEM, and MXDR share context automatically, you detect attacks faster and respond more effectively. This includes optimizing automated playbooks to rapidly respond to threats by leveraging more integrations and actively protecting against advanced threats faster than a human analyst. And a single agent, unified policy engine, and consolidated console mean you deploy quickly and support more clients without burning out your team.

Build sustainable competitive advantage - While competitors juggle vendor renewals, integration headaches, and tools that don't talk to each other, you deliver comprehensive threat, risk, and compliance management from one platform. That story resonates with sophisticated buyers who are exhausted by tool sprawl and vendor fatigue.

This is what drove our 2025 roadmap: building capabilities that excel individually while delivering stronger outcomes together.

Here's what we delivered.

SIEM: Rebuilt for the Demands of Modern Security Operations

SIEM is the connective tissue of effective security operations and continuous assurance. It powers real-time threat detection and correlation, enables deep forensic investigations, supports proactive threat hunting, and provides the data retention, evidence collection, and validation reporting that compliance frameworks and insurers require. For SIEM to deliver on that promise, it needs exceptional performance, rock-solid reliability, and cutting-edge detection capabilities.

This year, we rebuilt it from the ground up.

What We Delivered:

- **Complete backend rearchitecture** - Rebuilt the entire SIEM infrastructure for 10x performance improvements in search, reporting, and data ingestion. This foundation supports the continued delivery of advanced analytics and machine learning capabilities that modern threat detection demands, while providing the speed and reliability needed for continuous compliance monitoring and evidence generation.
- **Accelerated detection development** - New architecture lets our research and threat intelligence teams iterate detection rules faster than ever before, keeping you ahead of emerging threats and zero-day exploits without waiting for quarterly updates.
- **Dramatically faster search** - Query months of data across millions of events in seconds. When you're investigating a potential incident, every minute matters. Faster search means faster containment and reduced business impact. When auditors or insurers ask for evidence of specific control effectiveness, you retrieve it immediately.
- **Extended data retention** - Access and analyze data from any retention period with the same performance. Long-term forensics and compliance reporting that used to require expensive archives are now seamlessly available. Meet any regulatory retention requirement without compromise.
- **Cold storage support** - Todyl-hosted cold storage provides cost-effective options for regulatory requirements that mandate multi-year data retention. Store what you need for compliance without paying premium prices for inactive data.
- **Data rehydration** - Bring historical data back from cold storage for full-speed forensic analysis when investigating long-term compromises, conducting retrospective threat hunts, or responding to audit requests.
- **User and host behavioral profiling** - Machine learning builds baseline behavioral profiles for every user and endpoint over time, detecting anomalies that indicate compromise before traditional indicators appear. Early detection of lateral movement and privilege escalation can stop breaches in their tracks. These profiles also provide evidence of normal operations and documented deviations for compliance validation.
- **Expanded integrations** - New connectors for critical security and business platforms mean more comprehensive visibility, faster time to value, and richer evidence for demonstrating control effectiveness across your entire technology stack.

What This Means for You:

When you're investigating suspicious activity at 2am, you're not waiting on slow searches. When clients ask for compliance reports, you have the data retention and flexibility to meet any framework requirement with validated evidence. When you're proactively hunting threats, you have the speed and depth to find what matters. When your MXDR team triages an incident, they have the behavioral context to distinguish real threats from false positives, reducing alert fatigue, and improving effectiveness. And when insurers ask for proof that your security controls are working as intended, you demonstrate continuous monitoring and validated protection with documented evidence.

todyl

GRC: From Compliance Burden to Competitive Advantage

Endpoints remain the primary entry point for most attacks. Your clients run diverse environments acros Windows, Mac, Linux, and they all need the same level of advanced protection without adding tool sprawl or operational complexity.

What We Delivered:

- **Comprehensive security assessment platform** - Extensive library of customizable templates aligned to industry standards (CIS, NIST, CMMC, HIPAA, PCI-DSS) plus a simple builder for creating custom assessments. Send assessments securely to prospects or existing clients with granular control over access and editing permissions. All responses are stored in a centralized, searchable repository for immediate review, trend analysis, and historical benchmarking. Turn risk assessments into evidence of continuous improvement.

- **Reimagined Frameworks page** - Complete restructure improves navigation and makes finding specific compliance assets effortless. Quickly map controls to frameworks, track implementation status, and generate evidence reports that satisfy auditors and insurers. Streamlines GRC operations and simplifies delivering compliance insights to the stakeholders who need them.

- **Integrated evidence repository** - Centralized capability within Frameworks for collecting and organizing evidencespanning files, SIEM widgets, policies, assessment responses, that validates adherence to regulations and operating standards. Automated evidence collection means you're always audit-ready. When insurers or third parties ask for proof of controls, you have documented validation at your fingertips.

- **Expanded policy library and management** - Significantly grown on-demand library of expert-crafted operating policies aligned to common regulations and frameworks. Create custom policies directly in the platform using existing templates or building from scratch. Policies aren't just documentation, they become enforceable controls you can demonstrate to underwriters and auditors.

- **Expert-driven compliance content** - Comprehensive library of guidance tied to CIS, CMMC, HIPAA, NIST, and other frameworks. Content is embedded throughout GRC spanning Assessments, Frameworks, Policies, and can be used as-is or customized. Accelerates implementation and delivers immediate value without requiring specialized compliance expertise.

What This Means for You:

Compliance becomes a growth driver instead of overhead. When prospects ask how you'll help them meet cyber insurance requirements, you have documented answers. When clients face third-party security assessments, you have validated evidence ready to share. When underwriters ask about control implementation, you demonstrate continuous monitoring and validation, not point-in-time snapshots. When renewals come around, you're not just maintaining security—you're proving measurable improvements in their compliance posture and risk profile that can directly impact insurance premiums and stakeholder confidence. GRC helps you win deals, retain clients, and expand into regulated industries without needing dedicated compliance staff.

todyl

Endpoint Security: Uncompromising Protection Across Every Environment

GRC has been completely transformed. We recognized that as insurance requirements tighten and third-party risk assessments become standard, compliance capabilities are shifting from "nice to have" to business critical. But enterprise GRC tools are expensive and complex. We built something better: powerful yet practical tools designed specifically for how MSPs work and what your clients need to prove, not just promise.

What We Delivered:

- **Continuous detection enhancements** - Ongoing improvements to prevention, detection, and response capabilities keep pace with evolving attack techniques. Machine learning models are continuously refined to catch new ransomware variants, fileless malware, and sophisticated APTs that signatures miss.
- **Agent performance optimization** - Significantly reduced CPU and memory utilization while maintaining detection effectiveness. Better performance means happier end users and fewer complaints about security tools slowing down their work.
- **Cross-platform parity** - Full feature parity across Windows, Mac, and Linux endpoints. Protect every device in your clients' environments with the same advanced threat prevention, behavioral analytics, and automated response capabilities from a single console.
- **Enhanced behavioral analytics** - Expanded detection of anomalous process behavior, suspicious memory manipulation, and unusual lateral movement patterns. Behavioral analytics catch novel attacks and zero-days that traditional signature-based defenses miss entirely.

What This Means for You:

You deliver enterprise-grade endpoint protection to clients regardless of their OS mix. The agent runs reliably without impacting user experience or generating helpdesk tickets. Behavioral analytics provide defense-in-depth against sophisticated threats. And because endpoint telemetry flows directly into SIEM, if you have the right modules and integrations enabled you can correlate against network and identity activity for faster, more accurate threat detection and response, with documented evidence of protection that satisfies auditors and insurers.

SASE: Secure Connectivity That Just Works

Traditional VPNs create security blind spots, frustrate end users, and generate endless helpdesk tickets. SASE and Zero Trust Network Access solve these problems by verifying every user, device, and connection before granting access, regardless of location. But deployment is only half the battle. Your clients need secure connectivity that's fast, reliable, and invisible to users doing their jobs.

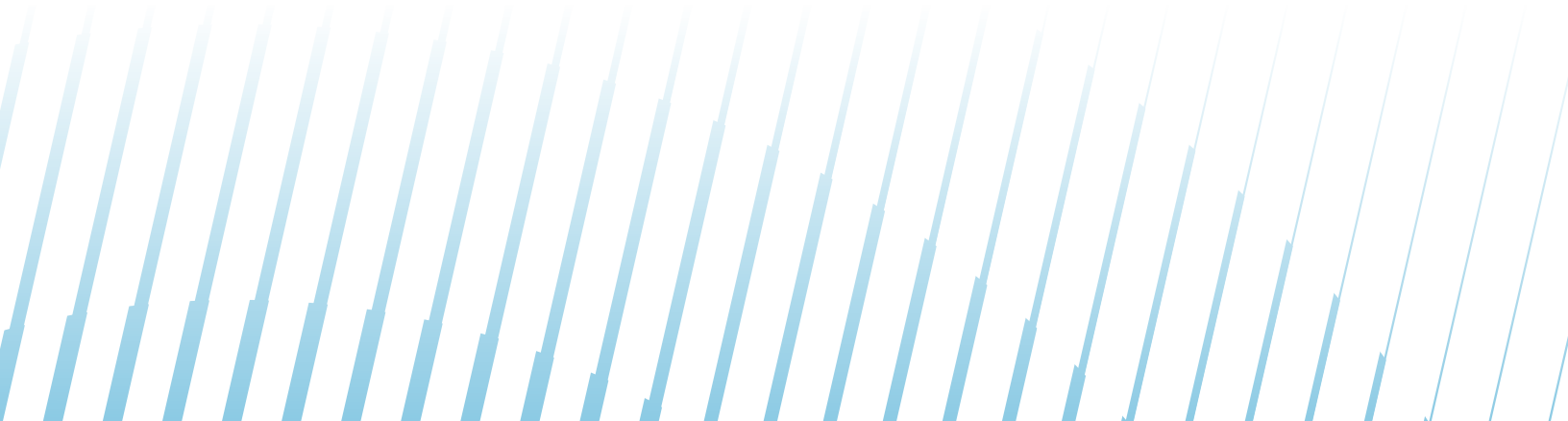
This year, we focused on making SASE not just secure, but dependable and performant at global scale.

What We Delivered:

- **Global infrastructure expansion** - Grew to 40 points of presence worldwide, dramatically reducing latency and improving connection speeds for clients regardless of where their users work. Better geographic coverage means faster access to applications and resources, whether users are connecting from New York, London, Singapore, or anywhere in between.
- **Enterprise-grade reliability** - Improved uptime from 98.9% in 2024 to 99.99% in 2025. That's the difference between occasional disruptions your team has to explain, and connectivity clients can depend on without thinking about it. Fewer outages mean fewer emergency calls and happier end users.
- **Intelligence-driven threat blocklists** - Built an intelligence layer analyzing 60,000+ threat indicators daily from multiple threat intelligence feeds. This powers more accurate, real-time blocking of malicious domains, URLs, and IPs before they reach users, stopping threats at the network edge without impacting performance or generating false positives that disrupt legitimate work.
- **Advanced content and file scanning** - Expanded HTTP response scanning detects and blocks malicious JavaScript, drive-by downloads, and other web-based threats in real time. Optimized engine eliminates latency while keeping signatures current so that users stay protected without noticing the security working behind the scenes.
- **Streamlined SSL inspection** - New Auto Resolve and Auto Resolve with Warning features automatically manage SSL bypass lists when applications require it, dramatically reducing administrative burden. Users get secure, inspected traffic without broken applications or help desk calls. You get hidden threat detection without operational headaches.

What This Means for You:

Your clients get secure connectivity that feels faster and more reliable than their old VPNs, not slower. Users connect from anywhere without thinking about it, which means fewer complaints and support tickets. Intelligence-driven blocking stops threats before they reach endpoints, reducing incident response workload. And because SASE telemetry integrates with SIEM and EDR, you get unified visibility for faster threat detection, while the improved reliability means you're managing security, not fighting infrastructure fires. Better user experience drives adoption, reduces friction, and makes renewals easier.



Platform Stability and Performance: The Foundation Everything Builds On `

Reliability isn't glamorous, but it's essential. From agent stability to UI responsiveness, a seamless experience for you and your customers directly impacts your ability to scale efficiently. This year, we made significant investments in platform stability, performance optimization, and quality assurance processes that catch potential issues earlier in development. These improvements build confidence in platform reliability as your business grows.

By the Numbers

This year, together we:

- Processed **20+ billion** security events daily through SIEM
- Handled **32,000+ critical and high-severity cases** with a median response time of just over seven minutes
- Operated SASE from **40 points** of presence globally, delivering secure connectivity anywhere your clients work
- Earned recognition as **#89** on the Deloitte Technology Fast 500 and **#8** in security on the Inc. 5000

Looking Ahead at 2026

Everything we built in 2025 becomes the foundation for what's next. We're deepening our commitment to Unified Assurance, where threat prevention, detection and response, risk management, and compliance validation work together seamlessly to help you prove outcomes your clients and their stakeholders demand.

The security landscape isn't getting simpler. Insurance requirements will keep tightening. Third-party risk assessments will become more detailed. Compliance frameworks will keep expanding. Threats will keep evolving. But you don't have to navigate it alone, and you don't have to do it with a dozen disconnected point solutions that make promises without providing proof.

Our realigned go-to-market and customer success teams will provide clearer ownership, faster responses, and more consistent experiences as you scale. We'll keep listening to your feedback and roadmap ideas because this partnership works when we're solving real problems you face in the field.

We're building something important together, a platform that doesn't just protect, but proves protection. Thank you for trusting us with the businesses and communities you protect.

Here's to 2026.