The Security Tax

Why the cybersecurity industry is collapsing under its own weight — what replaces it — and how the industry can thrive

February 2026

The weight

The average enterprise runs between 60 and 80 security tools. Not features within a platform. Separate products, from separate vendors, with separate consoles, separate licensing models, separate integration requirements, and separate sales teams calling every quarter to discuss renewal.

Each tool exists for a reason. When cloud computing created new attack surfaces, the industry produced CASB, CSPM, and CWPP. When those overlapped, it produced CNAPP to consolidate them. When SaaS applications introduced new risks, the industry produced SSPM. When APIs became attack vectors, API security platforms emerged. When AI agents arrived, AI security products followed immediately.

This is the security industry’s business model: every new technology surface generates a new product category. Every product category generates revenue. Every revenue stream generates incentive to maintain the complexity that justifies the product’s existence.

The result is a security stack that grows monotonically. Tools are added. Tools are rarely removed. Budgets expand. Complexity compounds. And the outcomes — the actual security of the organization — have not improved proportionally. Breach frequency is up. Breach severity is up. Time to detect is still measured in months for many organizations. The industry is selling more product into worse outcomes.

> *The security industry’s answer to “we have too many tools” has consistently been “here’s another tool.”*

The tax nobody can afford

For a large enterprise, the security tax is painful but survivable. A Fortune 500 company might spend $20–50 million annually on cybersecurity — tools, staff, managed services, compliance, insurance. It hurts, but it’s a rounding error on a $10 billion revenue line.

For a mid-market company doing $50 million in revenue, the same security posture might require $1–2 million annually. That’s 2–4% of gross revenue on security alone, competing directly with investment in product, people, and growth.

For a small business doing $5 million in revenue, the math simply does not work. Implementing MFA, endpoint protection, a SIEM, encrypted backups, patch management, vulnerability scanning, incident response planning, and security awareness training properly costs $200–500K annually. That’s 4–10% of revenue. Most small businesses cannot do it. So they implement fragments, hope for the best, and carry the risk.

> **The market failure:** Small and mid-size businesses know what best practices require. They understand the risks. They simply cannot afford the time, cost, and complexity of implementing the full security stack that the current model demands. They are priced out of security, not ignorant of it.

When these companies are breached, the narrative is predictable: they should have invested more in security. But the honest assessment is that the security model requires investment that is disproportionate to their resources. The model was designed for enterprises with dedicated security teams and multi-million-dollar budgets. Everyone else is expected to buy a scaled-down version of the same architecture and hope it’s enough.

Cyber insurance was supposed to bridge this gap. Instead, it has widened it. Premiums have increased dramatically in recent years. Insurers now require specific security controls as prerequisites for coverage. Companies that cannot afford the controls cannot get insurance. Companies that get breached without insurance face existential financial exposure. Security is becoming a privilege of scale, and the companies least able to afford a breach are the least able to prevent one.

The speed mismatch

All of the above was already unsustainable. Then AI changed the speed of attack.

AI-driven attacks operate at machine speed. Phishing campaigns are generated, personalized, and deployed in seconds. Deepfake voice calls impersonate executives in real time. Vulnerability scanners powered by AI identify and exploit weaknesses faster than patch cycles can respond. Credential stuffing attacks test millions of combinations per minute. Malware variants are generated automatically to evade signature-based detection.

The defensive stack operates at human speed. Security events flow into a SIEM. The SIEM correlates and generates alerts. Alerts enter a queue. A SOC analyst triages the queue, investigates suspicious events, consults playbooks, and escalates when necessary. This process takes minutes to hours on a good day. On a bad day — high alert volume, understaffed SOC, Friday afternoon — it takes longer.

The gap between attack speed and response speed is not closing. It is widening. Every advancement in AI capability benefits attackers at least as much as defenders. The attacker uses AI to generate novel attacks at scale. The defender uses AI to generate more alerts, which still require human judgment to act on. The fundamental architecture — detect, triage, respond

— has a human bottleneck that no amount of AI assistance eliminates, because someone must still decide what to do.

> **The asymmetry:** The attacker needs to succeed once, at machine speed. The defender needs to detect, analyze, and respond to every attack, at human speed, across every tool in a 60-tool stack. By the time the SIEM says “we have something,” the damage is done.

Drowning in alerts, starving for signal

The security operations center is the command center of modern defense. It is also drowning.

The average SOC receives thousands of alerts per day. Studies consistently show that analysts can meaningfully investigate only a fraction of them. The rest are triaged by severity score, briefly scanned, and closed. When organizations are breached and the incident is analyzed forensically, a consistent finding emerges: an alert fired. It was either missed, deprioritized, or lost in the noise.

This is not a staffing problem. It is an architecture problem. When your security model requires monitoring everything — every network packet, every file access, every authentication event, every API call, every configuration change — you generate noise proportional to “everything.” The signal-to-noise ratio degrades as the environment grows. Adding more tools generates more alerts. Adding AI-powered detection generates smarter alerts, but more of them. The SOC analyst’s cognitive capacity does not scale with alert volume.

The industry’s response has been SOAR — Security Orchestration, Automation, and Response — platforms that automate playbook execution. These help at the margins, but they automate the response to known patterns. Novel attacks, by definition, don't match existing playbooks. And the decision to act on a genuinely ambiguous alert still requires a human being who has the context to distinguish a real threat from a false positive.

The model assumes that if you can see everything, you can protect everything. In practice, seeing everything means seeing nothing, because the volume of "everything" exceeds the capacity of any team to process it.

The compliance theater

A growing percentage of security spending goes not to preventing breaches but to documenting that you tried. SOC 2 audits, penetration test reports, vulnerability scan documentation, vendor risk questionnaires, compliance mapping spreadsheets, evidence collection for regulatory reviews — these are real costs that produce paperwork, not protection.

An organization can be fully SOC 2 Type II compliant and still be breached, because compliance measures the existence of controls, not the effectiveness of outcomes. The audit verifies that you have a policy. It does not verify that the policy prevents a determined attacker. The checkbox gets checked. The risk remains.

For small and mid-size businesses, compliance costs are particularly crushing. A SOC 2 audit costs $50–200K. PCI-DSS compliance requires ongoing investment in specific controls. HIPAA compliance demands security risk assessments, business associate agreements, and documented policies. Each compliance framework requires its own evidence, its own documentation, and often its own tooling. The company spends heavily to prove it is secure, then spends again to actually be secure. Or, more commonly, it spends on compliance and hopes the compliance was sufficient.

> *We have built an industry where companies spend as much proving they're secure as they spend being secure. And neither expenditure guarantees the outcome.*

The people who aren't there

The global cybersecurity workforce gap is estimated at millions of unfilled positions. This is not a pipeline problem that will resolve with more university programs. It is a structural mismatch between the complexity of the defensive model and the number of humans capable of operating it.

The current security model requires specialists. SIEM engineers who understand correlation rules. Cloud security architects who can navigate multi-cloud environments. Penetration testers who think like attackers. Incident responders who can operate under pressure. GRC analysts who understand regulatory frameworks. Each specialty requires years of training and experience. The tools are getting more sophisticated, which means the operators need to be more sophisticated, which means the talent gap widens.

Large enterprises compete for this talent with high salaries and interesting problems. They still struggle to fill roles. Mid-size companies offer less compensation and less interesting work. They fill roles with less experienced people. Small businesses cannot compete at all. They either outsource to managed security providers — adding another layer of cost — or operate without dedicated security expertise.

The talent scarcity is not a temporary condition. It is a permanent feature of a model that requires more human expertise than the market can produce.

The lock-in trap

Once an organization has built its security stack on a specific set of vendors, switching costs become prohibitive. SIEM correlation rules are vendor-specific. EDR deployment agents are vendor-specific. SOAR playbooks reference vendor-specific APIs. Compliance documentation references specific tool outputs. The institutional knowledge of how the tools work together lives in the heads of the people who configured them.

Security vendors understand this dynamic and price accordingly. Annual renewals include price increases. New features are bundled into higher tiers. Competitive displacement requires months of parallel running, migration, and retraining. The rational economic decision, year after year, is to renew rather than replace, even when the tool underperforms, because the switching cost exceeds the performance gap.

The customer is captive. The vendor knows it. And the incentive to disrupt the model from within the vendor ecosystem is zero, because the model's complexity is what generates revenue.

The structural alternative

Every problem described above shares a common root cause: the security model requires the infrastructure to see, manage, and protect secrets. This requirement generates the complexity (more tools to protect more secrets in more places), the cost (more tools means more spending), the speed mismatch (detection and response must process everything), the alert fatigue (monitoring everything generates noise about everything), the compliance burden (proving you protect secrets you hold), and the talent demand (operating the tools that protect the secrets).

Zero-Knowledge Trust eliminates the root cause. When the platform never holds plaintext secrets, entire categories of security tooling become unnecessary.

> **Secret exfiltration detection?** Unnecessary. There are no plaintext secrets on the server to exfiltrate.
>
> **Data Loss Prevention for credentials?** Unnecessary. Credentials never exist in a form that can be copied, pasted, or leaked.
>
> **Secrets rotation policies enforced by administrators?** Unnecessary. Key rotation is cryptographic and automatic within the vault.
>
> **Privileged access management for vault administrators?** Unnecessary. There is no privileged access to grant because the platform cannot read the vaults.
>
> **Compliance evidence for data handling procedures?** Unnecessary. The architecture makes data exposure impossible. Compliance is a property of the system, not the operator’s behavior.

The 60-tool stack does not shrink incrementally. Entire layers vanish. The tools that remain are the ones that address problems ZKT does not claim to solve: network availability, endpoint malware, application logic vulnerabilities, physical security. But the layers of tooling that exist solely because the architecture puts secrets where they can be reached — those layers are gone.

For small and mid-size businesses, this is transformative. Instead of trying to afford a miniature version of the enterprise security stack, they start with a sovereign vault. The vault provides the security foundation. They grow connections as needed. The cost model shifts from “how much security can we afford” to “security is built into the root.”

Seven billion security analysts

There is one more structural advantage that Zero-Knowledge Trust provides, and it may be the most important: it turns every user into a security sensor.

In the current model, security monitoring is centralized. A SOC team — typically a handful of analysts — watches dashboards, triages alerts, and investigates anomalies on behalf of the entire organization. They are looking for needles in a haystack of events generated by thousands of users across dozens of systems. They have no personal context for any individual user’s behavior. Is that 2 AM API call suspicious? The analyst doesn’t know. They check the logs, consult the baseline, maybe escalate. It takes time. It’s often wrong.

Now consider the alternative. In a Zero-Knowledge Trust architecture, every individual can see their vine. Every active connection. Every agent acting on their behalf. Every credential usage. Every tendril, every graft, every delegation — visible in real time to the person whose vault it is.

Nobody knows better than you whether that 2 AM API call was legitimate. No SIEM rule, no behavioral analytics engine, no AI-powered anomaly detector can encode “that’s not something I would do” as precisely as the person whose identity is being used. The user has the one thing the SOC analyst will never have: personal context.

> *The current model asks a handful of analysts to detect anomalies across thousands of users. The ZKT model asks each user to detect anomalies in their own activity. One of these models scales. The other is what we've been doing.*

This is not a shift from professional security to amateur security. The organizational security team still exists, still monitors infrastructure health, still responds to systemic threats. What changes is where individual-level detection happens. Instead of routing every user's activity through a central monitoring system that must somehow distinguish normal from abnormal for thousands of different people, each person monitors their own vine.

A user sees an unfamiliar connection and revokes it. An employee notices an agent making requests they didn't authorize and severs the graft. A customer spots a transaction they didn't initiate and flags it instantly — not through a support ticket that takes 48 hours, but through their vault's interface in seconds.

The detection surface scales with the user population. An organization with 10,000 employees has 10,000 security sensors, each with perfect context for their own activity. A nation with 300 million connected citizens has 300 million security sensors. No centralized SOC in history has achieved detection coverage at that scale, because centralized monitoring cannot carry the context that distributed monitoring provides for free.

This is the only model that matches the scale of the threat. AI-driven attacks are personalized, distributed, and operate at machine speed. Centralized detection cannot keep up because it lacks personal context and operates through human bottlenecks. Distributed detection — each user watching their own vine — matches the attack surface point for point. The attacker targets an individual; the individual detects the anomaly. No aggregation delay. No triage queue. No false positive from a SIEM that doesn’t know your habits.

Malicious acts at scale — credential theft campaigns, agent hijacking, automated fraud — require that the targets remain unaware. In the current model, awareness depends on a centralized team spotting the pattern across thousands of victims. In the ZKT model, every intended victim can see what is happening to their own vine the moment it happens. Scale the attack and you scale the detection proportionally, because every target is also a sensor.

This does not prevent all attacks. A sophisticated attacker who compromises a device in real time operates within the window before the user notices. But it eliminates the class of attacks that currently succeeds because the victim has no visibility: the credential quietly stolen, the token silently replayed, the agent secretly authorized. When users can see their vines, stealth becomes dramatically harder.

The economics of elimination

The economic case for Zero-Knowledge Trust is not that it costs less than the current stack. It is that it eliminates entire categories of expenditure by eliminating the architectural conditions that created them.

Tool consolidation: When secrets are never exposed to the platform, the tools that detect, prevent, and respond to secret exposure become unnecessary. The 60-tool stack does not need optimization. It needs amputation of the layers that exist solely because the old architecture required them.

Talent reduction: When entire tool categories are eliminated, the specialists who operate them are freed for work that matters. The SIEM engineer redeploys to application security. The secrets management administrator's role is absorbed by the architecture. The talent gap narrows not because more people enter the field, but because the field requires fewer specialized roles.

Compliance simplification: When compliance is a property of architecture rather than operator behavior, the evidence collection process simplifies radically. Instead of documenting procedures for handling secrets, you demonstrate that the architecture makes handling secrets impossible. The audit becomes shorter, cheaper, and more conclusive.

Insurance improvement: An organization that can demonstrate architectural zero-knowledge — that even a compromised administrator cannot access user secrets — presents a fundamentally different risk profile to insurers. The conversation shifts from "do you have these 47 controls" to "is it architecturally possible for this class of breach to occur." The answer, for secret exposure, is no.

SMB accessibility: When security starts with a sovereign vault rather than a 60-tool stack, the barrier to entry drops from hundreds of thousands of dollars to the cost of a vault implementation. The small business doesn't need to choose between security and growth. Security is the root from which growth happens.

A message to the industry: this is your moment, not your funeral

If you are a security vendor reading this, you may feel attacked. That is not the intent. The intent is to point out that the ground is shifting and the vendors who see it first will lead the next era of security rather than be displaced by it.

The transition from perimeter security to zero trust did not destroy the security industry. It transformed it. Companies that had built castle-and-moat products either pivoted to identity-centric security or were replaced by companies that did. Palo Alto Networks, CrowdStrike, Okta, Zscaler — the leaders of the current era are companies that recognized the shift early and repositioned. The companies that insisted the perimeter was fine are largely gone.

The same opportunity exists now, and it is larger. Zero-Knowledge Trust does not eliminate the need for security. It eliminates the need for specific categories of security that exist because the architecture puts secrets where they can be reached. The categories that remain — and the new ones that emerge — represent enormous markets.

SIEM and SOC platforms: Your future is not aggregating alerts about secret exposure. It is providing the user-facing vine visibility layer — the interface through which individuals see their connections, their agents, their credential activity. The SOC does not disappear; it evolves from a centralized monitoring team into an orchestration layer that supports distributed user-level detection. The platform that makes vine visibility intuitive and actionable wins this market.

Identity providers: OAuth, OIDC, and SAML are not replaced by ZKT. They are strengthened by it. The identity provider that integrates cryptographic token binding, hardware-anchored proof of possession, and zero-knowledge agent delegation into its existing flows becomes the trellis that every vine wants to grow on. The authentication handshake stays yours. The token security that follows it becomes your differentiator.

Endpoint security: The endpoint becomes more important in a ZKT world, not less. The device is where decryption happens, where vaults live, where hardware security modules anchor the root of trust. Endpoint protection that understands vault integrity, secure enclave health, and device attestation is essential infrastructure. The EDR vendor that evolves from “detect malware” to “protect the root” has a larger addressable market, not a smaller one.

Cloud security: Cloud platforms are the trellis. They do not go away. They become the infrastructure that routes encrypted vault traffic, hosts organizational trellis structures, and provides the compute layer for cryptographic operations. The cloud security vendor that provides zero-knowledge-aware infrastructure — confidential computing enclaves, encrypted vault hosting, policy enforcement without plaintext access — becomes the preferred trellis for every vineyard.

Compliance and GRC: The compliance market does not shrink. It transforms. Instead of documenting behavioral controls, GRC platforms verify architectural properties. The audit becomes: “Is this system architecturally incapable of accessing plaintext secrets?” Proving architectural compliance is a software problem, and the GRC vendor that automates it captures a market that is currently drowning in manual evidence collection.

Managed security services: MSSPs are positioned to become the bridge for small and mid-size businesses transitioning to ZKT. The MSSP that can provision sovereign vaults, configure organizational trellises, and provide vine visibility as a managed service becomes the on-ramp for the millions of businesses currently priced out of security. The addressable market expands dramatically.

The vendors who will thrive are the ones who recognize that the value is not in guarding the secrets. It is in building the infrastructure, the interfaces, and the services that make sovereign vaults seamless, vine visibility intuitive, and trellis architecture robust. The security industry does not contract. It pivots from protecting secrets the platform holds to enabling a platform that never needs to hold them.

> *The perimeter-to-zero-trust transition created a generation of billion-dollar companies. The zero-trust-to-zero-knowledge-trust transition will create the next one. The question for every vendor is not whether to pivot, but whether to lead or follow.*

Stop adding walls. Remove the target.

The cybersecurity industry has spent two decades building an ever-expanding perimeter of tools, alerts, processes, and specialists around a fundamentally flawed architecture: one that puts secrets where they can be reached and then invests enormous resources in preventing anyone from reaching them.

The model is collapsing. The complexity is unsustainable. The cost exceeds what most organizations can bear. The speed of AI-driven attacks has outpaced the speed of human-driven response. The talent to operate the tools does not exist in sufficient quantity. The compliance burden grows without producing proportional protection. And the alerts — thousands of them, every day — bury the signals that matter in noise that the architecture itself generates.

Zero-Knowledge Trust does not fix this model. It replaces it. Not by adding a better tool to the stack, but by removing the architectural condition that made most of the stack necessary. When the platform cannot see secrets, you do not need tools to prevent the platform from leaking secrets. When every user can see their own vine, you do not need a centralized team to detect individual-level anomalies. When compliance is architectural, you do not need a compliance team to document behavioral controls.

The security industry will resist this transition, because the transition eliminates revenue streams. Vendors who sell tools to protect secrets that the platform holds have no product in a world where the platform holds nothing. But the economics are relentless. Organizations paying the security tax will eventually discover that the tax is not buying security. It is buying complexity that the vendor ecosystem profits from maintaining.

The organizations that move first will not just be more secure. They will be leaner, faster, and more accessible to the small and mid-size businesses that the current model has priced out of protection. They will have workforces that are security sensors rather than security liabilities. And they will operate in an architecture where the question is not “how do we protect the secrets we hold” but “why would we hold them in the first place.”

> *The most expensive security is the kind you buy to protect an architecture that should not exist. The cheapest security is the kind built into an architecture that needs no protection.*