VIPERBYTE SECURITY

USE CASE

Private Sector Security:

See Everything. Stop the Threats You Didn't Know Were There.

How Viperbyte delivers complete network visibility, autonomous AI enforcement, and continuous compliance evidence — without agents, without downtime, without an MSSP.

TARGET AUDIENCE	ORGANIZATION SIZE	DEPLOYMENT TYPE	DOCUMENT DATE
IT Manager / CISO / Risk Officer	50–1,000 Employees	On-Premises Hardware Appliance	August 2026

1. The Detection Gap — What You Don't Know Is What Hurts You

THE CORE PROBLEM: The average organization has 40% of its network-connected devices invisible to its security tools. These are printers, IP cameras, HVAC controllers, building access systems, and unmanaged IoT devices — each one a potential entry point that no agent-based tool will ever touch. Viperbyte sees all of them on Day 1, without installing a single agent.

Most private sector organizations have invested in security tools — endpoint protection, email filtering, firewalls. These tools cover the devices that were purchased by IT and enrolled in the managed device program. They do not cover the devices that weren't. An attacker who gains access through an unmanaged printer or IP camera operates in a blind spot that your existing tools will never report on. Viperbyte closes this gap at the network level, regardless of device type, operating system, or vendor.

40%
of enterprise devices
invisible to agent-based EDR tools

258 days
average attacker dwell time
before detection — IBM Cost of Data Breach 2024

$4.9M
average total breach cost
IBM Cost of Data Breach Report 2024

99.24%
F1 detection accuracy
insider threat model — verified in production

Why Traditional Security Tools Have This Gap

Tool Category	What It Covers	What It Misses
Agent-Based EDR (CrowdStrike, Defender)	Managed Windows/Mac laptops, servers with agent installed	Unmanaged IoT/OT, printers, IP cameras, badge readers, HVAC, guest devices, contractor laptops, BYOD — anything without an installed agent.
Perimeter Firewall (Palo Alto, Cisco)	WAN-facing traffic, boundary in/out decisions	East-west (lateral) movement inside the network. An attacker already inside the perimeter is invisible to a boundary firewall.
Email Security	Inbound email threats,	Any attack that doesn't arrive via

(Proofpoint, Defender for O365)	phishing links in email	email. All post-click behavior — what the user did after clicking — is outside email security scope.
SIEM (Splunk, Sentinel)	Log aggregation from tools you've already deployed	Can only correlate what other tools report. If a sensor has a gap, the SIEM has the same gap. Garbage in, garbage out.

Viperbyte operates at the network layer via passive SPAN monitoring — it sees every packet that crosses the switch, from every device, without being installed on any of them. From Day 1, you have complete behavioral visibility across your entire network.

2. Five Private Sector Use Cases — Real Scenarios, Real Outcomes

2.1 Scenario: The Cyber Insurance Renewal

Audience: CFO / Risk Manager

The Problem:	Annual cyber insurance renewal arrives with a 40% premium increase. The underwriter questionnaire asks for evidence of EDR, SIEM, network monitoring, DNS filtering, and continuous vulnerability scanning. Your current tools can only document partial coverage.
Viperbyte Role:	Viperbyte satisfies six of the eight underwriter control categories with continuous, timestamped, exportable evidence. Full network monitoring — including the 40% of devices agents miss. 365-day log retention. DNS Security Engine with documented block history. On-demand Pentest Report for the vulnerability scanning requirement.
Outcome:	Documented controls submitted with questionnaire. Premium reduced by $42,000/year vs no-controls scenario. Ransomware sublimit removed. Claims-defensible evidence in place for the life of the policy.

2.2 Scenario: The Undetected Insider Threat

Audience: CISO / IT Manager

The Problem:	An employee with legitimate network access begins quietly exfiltrating data — small transfers, after hours, to personal cloud storage. No malware. No firewall alerts. The behavior is invisible to perimeter tools because it looks like normal HTTPS traffic.
Viperbyte Role:	Viperbyte's AI brain builds a behavioral baseline for every user on the network. After 7–14 days of observation, it knows what 'normal' looks like for each identity. Unusual data volumes, access at atypical hours, and transfers to destinations outside the baseline trigger the insider threat model (F1=0.9924). The enforcement pipeline can isolate the user's device within <2 seconds of an AI decision.
Outcome:	Insider threat detected within hours of first anomalous transfer. Evidence chain auto-generated: user, timestamp, destination, data volume, confidence score. HR and legal have documented proof before the employee is approached.

2.3 Scenario: The Printer as an Entry Point

Audience: IT Manager / Security Team

The Problem:	A threat actor exploits an unpatched vulnerability in a networked laser printer — a device that no EDR agent will ever be installed on. Using the printer as a foothold, they begin lateral movement toward the file server. Your existing tools report nothing.
Viperbyte Role:	Viperbyte's device behavioral engine profiles every networked device, including printers, based on expected traffic patterns. Printers communicate with print servers — they do not initiate connections to internal file shares or external IPs. The moment the compromised printer deviates from its behavioral profile, the anomaly surfaces. The Deception Layer's honeypots catch reconnaissance activity the moment lateral movement begins.
Outcome:	Printer compromise detected within minutes of lateral movement. Device isolated before attacker reaches the file server. Forensic evidence of the kill chain logged: initial access, reconnaissance, first lateral contact, enforcement action.

2.4 Scenario: The Compliance Audit

Audience: CTO / Compliance Officer

The Problem:	SOC 2 Type II audit requires evidence of: continuous network monitoring, access control logging, incident response capability, and vulnerability management. Assembling evidence from five different tools takes three weeks and still produces gaps where coverage is unclear.
Viperbyte Role:	Viperbyte's compliance dashboard maps all covered controls to live evidence. Every network event, identity session, enforcement action, and detected threat is logged continuously with tamper-evident timestamps. Evidence exports are structured JSON or human-readable reports that can be handed directly to auditors. The auditor sees 365 days of documented controls — not a pre-audit binder.
Outcome:	SOC 2 evidence package assembled in hours, not weeks. Auditor receives live dashboard access — controls verified in real-time, not reconstructed. No evidence gaps. Audit scope reduction possible due to demonstrated continuous monitoring.

2.5 Scenario: The Remote Workforce Identity Gap

Audience: CISO / HR / Legal

The Problem:	A former employee's credentials are still active in the VPN system — a configuration error from a rushed offboarding. The account is used by an external actor three weeks after termination to access internal file shares. No alert fires.

Viperbyte Role:	Viperbyte Identity Engine attributes every VPN session to a named user and maintains a behavioral baseline per identity. A session from a former employee account accessing systems they never used while employed triggers an impossible travel flag and identity anomaly simultaneously. The session is flagged for review within minutes of the first connection.
Outcome:	Terminated employee credential abuse detected before any data exfiltration. Session terminated. Evidence chain documents exactly which systems were accessed and for how long — critical for legal and HR response.

3. Deployment Timeline — Day 1 / Day 30 / Day 90

Viperbyte is deployed as a hardware appliance connected to your network switch via SPAN port. No software agents are installed anywhere. No network changes are required. The timeline below describes what you gain at each milestone.

Milestone	Viperbyte Capability Active	Business Value Delivered
Day 1	• Full network asset discovery — every connected device profiled • Real-time threat intelligence matching (1.38M indicators) • DNS Security Engine active — malware/C2 callbacks blocked • Deception Layer (43 honeypots) — lateral movement tripwires live • WAN threat blocking — enforcement pipeline active	Immediate visibility into devices you didn't know existed. First threat detections typically occur within hours of deployment. You see your network as an attacker sees it — not as your asset inventory claims it is.
Day 30	• Behavioral baseline established for every device and user identity • Insider threat model active (requires 7+ days of clean baseline) • Impossible travel / concurrent session detection active • Compliance dashboard populating for supported frameworks • MS365/Azure AD identity attribution wired (if integration configured)	Behavioral anomalies now surface against established 'normal.' The first insider threat and identity anomaly detections begin. Compliance posture visible in dashboard — gaps identified before the auditor is.
Day 90	• 90-day evidence chain established for every covered compliance control • Kill-chain AI model trained on your network's traffic patterns • Vulnerability baseline established — CVE cross-reference current • Pentest Report exportable with 90-day scan history • Identity vector baseline mature — geo-anomaly detection active	Audit-ready evidence package available. 90 days of documented controls satisfies most insurance questionnaire requirements. AI model now specific to your organization's behavioral patterns — false positive rate drops as the model learns what 'your normal' looks like.

NO AGENT. NO DOWNTIME. NO NETWORK CHANGES. Viperbyte connects to your existing network switch via a SPAN/mirror port. It receives a passive copy of all traffic — read-only at the SPAN level. Enforcement (blocking) is applied via nftables on the Viperbyte appliance. There is no

agent to install, no software to maintain, and no network reconfiguration required.

4. Platform Coverage Map — What Viperbyte Covers

Viperbyte is built around six intelligence engines that together cover the full attack surface of a private sector organization. Each engine runs autonomously and feeds findings into the Big Brain AI for correlation.

Intelligence Engine	Primary Function	What It Detects	Evidence It Generates
Network Intelligence Engine	Behavioral baselining of all network-connected assets	Unusual east-west traffic · New device connections · Protocol anomalies · Data exfiltration volume spikes	Device baseline records · Connection logs · Anomaly events with confidence scores
DNS Security Engine	Block malicious domains. Detect DNS-based attacks.	Malware C2 callbacks · DGA (domain generation) activity · DNS tunneling · New malicious TLD patterns	Block log with domain + category + timestamp · Query history per device
Identity Engine	Attribute every session to a named user identity	Impossible travel · MFA bypass · Credential abuse · Privileged account anomalies · Terminated user activity	Identity session log · Behavioral anomaly events · Evidence chain per incident
Deception Layer	43 honeypots across all major protocol classes	Reconnaissance · Lateral movement · Password spraying · Exploit attempts against decoys	Attacker profile · Kill-chain stage · Enforcement action log
Insider Threat Model	AI model trained on your organization's behavioral patterns	Exfiltration patterns · Kill-chain sequences · After-hours access · Anomalous data transfers	AI decision with confidence score · MITRE ATT&CK technique classification
Vulnerability & Compliance Engine	Continuous passive vulnerability assessment	Unpatched services · Known CVE exposure · Compliance control gaps · Configuration drift	Pentest Report (exportable PDF) · Compliance dashboard per framework · Evidence export

5. Return on Investment — Private Sector Economics

The Viperbyte ROI model for a private sector organization has three distinct components: direct cost avoidance (premium savings + MSSP elimination), breach cost reduction (earlier detection = lower impact), and operational efficiency (audit time, compliance evidence assembly, incident response).

3-Year Cost Model — 100-User Organization

Cost Driver	Without Viperbyte	With Viperbyte
Cyber insurance premium	$60,000–$85,000/yr	$38,000–$55,000/yr (documented controls → favorable underwriting)
MSSP / MDR service	$60,000–$120,000/yr	$0 — Viperbyte's AI brain is the 24/7 monitoring function. No MSSP contract.
SIEM licensing	$25,000–$60,000/yr	$0 — Viperbyte's Network Intelligence Engine replaces the SIEM function.

Compliance audit prep (staff time)	160–240 hrs/audit	8–16 hrs/audit — evidence pre-assembled in compliance dashboard.
Average breach cost if undetected	$4,900,000 (IBM 2024 avg)	Significantly reduced — earlier detection compresses dwell time and scope.
Viperbyte platform cost	—	$47,000/yr + ~$3,500 hardware one-time

$47,000
Viperbyte annual license
Hardware ~$3.5K one-time additional

$42,000
Year 1 insurance savings
vs no-controls scenario (midpoint estimate)

$96,000
MSSP/SIEM annual savings
Typical midpoint — no MSSP, no SIEM license

>$90K
Net annual benefit
Insurance + MSSP/SIEM savings vs Viperbyte cost

6. Buyer's Checklist — How to Evaluate Any Security Platform

Before selecting a security platform, private sector organizations should ask every vendor the same set of questions. The answers reveal whether a solution covers your actual risk surface or only the visible portion of it.

Evaluation Question	Viperbyte Answer	Why It Matters
Does it cover agentless devices (IoT, printers, cameras)?	**YES — all devices**	40% of your network is invisible to agent-only tools. Every unmanaged device is an attack vector.
How quickly does it identify new devices on the network?	**Real-time — Day 1**	Unmanaged new devices are the most common blind spot. Instant discovery closes the gap.
Can it detect threats without cloud connectivity?	**YES — fully on-prem**	Cloud-dependent detection fails when the network is under attack. Viperbyte operates standalone.
Does it require network changes or downtime to deploy?	**NO — passive SPAN**	Complex deployments delay protection. Viperbyte is live in hours without touching your network.
Does it generate continuous evidence (not just alerts)?	**YES — 365-day chain**	Alerts without evidence don't survive insurance claims or audit inquiries.
Can you see every user identity behind every connection?	**YES — attributed**	Anonymous traffic logs are forensically useless. Every event must tie to a named identity.
Does the AI model adapt to YOUR organization's behavior?	**YES — per-site model**	Generic models have high false positive rates. Organization-specific baselines are essential.
What is the documented detection accuracy?	**F1=99.24%**	Vendors must publish verified accuracy metrics — not theoretical ranges.
Does it enforce, or only alert?	**Enforces — <2 sec**	Alerting without enforcement requires a human in the loop 24/7. AI enforcement doesn't.
Does it produce compliance-ready evidence exports?	**YES — JSON + report**	Evidence that requires manual assembly defeats the purpose of continuous monitoring.
What is the total deployment cost including hidden fees?	**$47K/yr all-in**	Many platforms have hidden costs: MSSP overlay, SIEM integration, per-

		endpoint licensing.
What is the hardware requirement?	**One appliance, <$3.5K**	Enterprise security should not require $200K+ in infrastructure to deploy.

7. Getting Started — What Happens Next

Viperbyte is available as an annual license with a hardware appliance. Deployment is completed by a Viperbyte-certified installer in a single site visit. No cloud dependency. No data leaves your network. No agents. No downtime.

Deployment Process

- **Step 1 — Discovery call:** 30-minute call with Viperbyte sales. We identify your network architecture, existing tools, and specific risk priorities.
- **Step 2 — Site assessment:** Remote review of your network diagram. We identify optimal SPAN port placement and integration points (MS365, LDAP, VPN).
- **Step 3 — Hardware shipped:** Viperbyte appliance ships to your facility. Pre-configured for your network. Arrives ready to connect.
- **Step 4 — Day 1 deployment:** Physical SPAN connection made. Passive monitoring begins immediately. First device inventory visible within minutes.
- **Step 5 — Integration:** MS365/Azure AD identity attribution configured. VPN session attribution enabled. LDAP connector for on-prem AD (optional).
- **Step 6 — Dashboard handoff:** Compliance dashboard tour. Alert tuning. First weekly threat brief delivered within 7 days.

READY TO SEE YOUR NETWORK AS IT ACTUALLY IS? Request a demonstration at sales@viperbytesecurity.com · viperbytesecurity.com
We will show you Viperbyte running on a live network — real device discovery, real threat detections, real evidence chain. No sales theater. Bring your hardest questions.