VIPERBYTE SECURITY

WHITEPAPER

Cyber Insurance in Crisis:

How Viperbyte Satisfies Underwriter Requirements, Reduces Premiums, and Provides Claims-Defensible Evidence

For the CFO, Risk Manager, or IT Director who just received a cyber insurance renewal quote 30–50% higher than last year — or was told their organization no longer qualifies for the coverage they had.

TARGET READER	ORGANIZATION SIZE	COVERAGE TYPE	DOCUMENT DATE
CFO / Risk Manager / IT Director	25–500 Employees	Standalone Cyber / Tech E&O	August 2026

1. The Cyber Insurance Market Reality — What Changed and Why

Cyber insurance used to be a checkbox — a relatively inexpensive policy most CFOs signed without asking many questions. That era is over. The ransomware epidemic of 2020–2023 drove claims to historic highs, forced underwriters to rethink their entire risk model, and produced a market that now functions more like health insurance than property insurance: you are assessed on your specific risk profile, your controls are verified, and your premium reflects what the underwriter actually believes about your likelihood of a claim.

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

258 days
Average attacker dwell time
Before detection — IBM 2024

$1.54M
Average ransomware payment
Sophos State of Ransomware, 2023

73%
SMBs reporting premium increases
Coalition Cyber Insurance Index, 2024

Three forces are reshaping the market simultaneously. First, underwriters lost money — ransomware claims exploded, reinsurers pulled back. Second, the regulatory environment shifted — carriers can no longer cover 'reasonable negligence' broadly. Third, the questionnaire became the underwriting tool — carriers discovered that organizations with specific documented controls file dramatically fewer claims, so the presence or absence of those controls now directly determines your premium and your eligibility.

The Three Cyber Insurance Problems Organizations Face Today

Problem	Who It Hits	What Happens
Premium Shock	Any organization renewing after a claim or after market hardening	Renewal quote arrives 30–80% higher than the prior year. No incident occurred. The underwriter re-priced based on the current market and a closer look at your control answers.
Qualification Failure	SMBs that have not implemented specific technical controls	Insurer declines coverage entirely or offers a policy so loaded with

		exclusions it provides no meaningful protection. Most common trigger: no MFA on remote access, no EDR, no documented IR.
Claims Denial	Organizations that experienced a breach and filed a claim	Carrier invokes 'reasonable security' exclusion. Attacker had access for months with no detection. No logs. No evidence of controls. Claim denied or substantially reduced.

THE FUNDAMENTAL SHIFT: Cyber insurance underwriting has moved from 'Do you have a firewall?' to 'Show us evidence that your controls were active, tested, and working — every day, not just the day before you applied.' This is the gap Viperbyte was built to close.

2. The Underwriter Questionnaire Decoded — What They're Actually Asking

Every major cyber insurer — Coalition, At-Bay, Chubb, Travelers, Marsh, Beazley — uses a questionnaire that has grown from 5 pages in 2018 to 25+ pages today. The questions converge on the same eight control families. Organizations that can answer 'Yes' with evidence to these eight categories file substantially fewer claims and receive substantially better pricing.

The Eight Control Categories Every Carrier Asks About

#	Control Category	Typical Carrier Question	Why It Matters to Underwriters
1	**Multi-Factor Authentication (MFA)**	*Is MFA enforced on remote access, email, cloud admin, and privileged accounts?*	Coalition data: MFA on remote access reduces claims by up to 35%. Ransomware operators overwhelmingly enter via compromised credentials at VPN/RDP. MFA eliminates the most common entry vector.
2	**Endpoint Detection & Response (EDR)**	*Is EDR deployed on 100% of endpoints? Are alerts monitored 24/7?*	EDR-equipped organizations file 40% fewer claims (Coalition, 2024). Underwriters want behavioral detection, not just antivirus. The '100%' coverage question is intentional — partial deployment = no deployment.
3	**Privileged Access Management (PAM)**	*Are privileged/admin accounts separately managed? Is access time-limited?*	Once an attacker has admin credentials, the breach is total. PAM limits blast radius. Absence triggers exclusions on admin-credential incidents.
4	**Network Segmentation & Monitoring**	*Is your network segmented? Are connections monitored at the boundary?*	Segmentation limits lateral movement. Monitoring enables detection before an attacker reaches crown

			jewels. Flat networks with no monitoring are a red flag.
5	**Vulnerability Scanning & Patching**	*How often are vulnerability scans run? What is your mean time to patch critical CVEs?*	Unpatched known vulnerabilities are the second most common breach entry point. Carriers want documented scan results — not a promise to patch, but evidence it happened.
6	**Data Backup & Recovery Testing**	*Are backups offline or immutable? When was recovery last tested?*	Ransomware impact is catastrophic without clean backups. Carriers have learned that untested backups often fail at recovery time.
7	**Incident Response Plan & Testing**	*Do you have a documented IR plan? Tested via tabletop in the last 12 months?*	Organizations with tested IR plans contain breaches faster — lower dwell time, lower breach cost, lower claim size. Undocumented IR = carrier assumes worst-case.
8	**Centralized Logging & SIEM Monitoring**	*Are logs from all critical systems centralized? Reviewed for anomalies?*	Absence of logging is the most common reason claims are denied. If there are no logs, the insurer cannot determine cause, scope, or timeline.

3. The Control Gap — Why Most SMBs Fail the Questionnaire

Most organizations with fewer than 500 employees can only confirm three or four of the eight control categories with actual evidence. The remainder are either not implemented, partially implemented, or implemented without documentation — which is the same as not implemented from an underwriter's perspective.

#	Control Category	Typical SMB Answer	What It Costs in Premium or Coverage
1	**MFA**	**Partial — email only, not remote access**	Most carriers require MFA on remote access specifically. Email-only MFA leaves the most dangerous gap open. Typical loading: +15–25% premium.
2	**EDR**	**Partial — Windows laptops only**	Servers not covered by EDR = high-value target with no detection. Typical loading: +10–20% or ransomware coverage limit reduced.
3	**PAM**	**No — shared admin passwords in use**	Shared admin credentials are flagged immediately. Typical loading: +20% or admin-credential incidents excluded

			entirely.
4	Network Monitoring	**Partial — firewall present, no internal monitoring**	A perimeter firewall answers the boundary question. No internal monitoring means an attacker inside the perimeter is invisible. +15%.
5	Vuln Scanning	**No formal program — patching ad-hoc**	Ad-hoc patching with no documentation is treated as unpatched. Carriers correlated unpatched CVEs with 28% of all breach claims. +10–15%.
6	Backup Testing	**Backups exist — never tested recovery**	Untested backups fail 30–40% of the time in real ransomware scenarios (Veeam 2023). Effect: ransomware sublimit applied — $500K cap instead of full policy limit.
7	IR Plan	**No documented plan**	No IR plan = guaranteed worst-case dwell time and breach scope. Typical loading: +10% and minimum retention requirement increased.
8	SIEM / Logging	**No SIEM — logs in individual systems**	Decentralized logs with no monitoring = no detection capability. Most common reason for claims denial post-breach. Typical loading: +20–30%.

THE MATH: An organization with all eight gaps pays a combined loading of 100–130% above the baseline rate. A company that should pay $40,000/year for $5M in cyber coverage ends up paying $80,000–$92,000 — or gets declined entirely. Closing the gaps does not just improve coverage. It cuts the premium in half.

4. Viperbyte — Control-by-Control Underwriter Questionnaire Mapping

Viperbyte is an on-premises autonomous AI security platform deployed as a hardware appliance. The following table maps each of the eight underwriter control categories to specific Viperbyte capabilities — what the carrier asks, how Viperbyte satisfies it, and the evidence artifact the underwriter or claims adjuster would receive.

ON EVIDENCE: Every Viperbyte capability below produces continuous, timestamped, exportable evidence — not a screenshot from audit week. The evidence exists for every day Viperbyte has been running. When you fill out the questionnaire, you are not attesting to a policy. You are reporting on documented, verifiable, ongoing controls.

1. Multi-Factor Authentication (MFA)	**[FULL]**

Carrier asks:	Viperbyte Identity Engine ingests MFA signals from MS365/Azure AD and flags any session where MFA was bypassed or not enforced.
Viperbyte coverage:	Remote access (VPN) + identity attribution Viperbyte Identity Engine ingests MFA signals from MS365/Azure AD and flags any session where MFA was bypassed or not enforced. Every VPN session is attributed to a named user with authentication method recorded. Impossible travel detection catches credential abuse.
Evidence artifact:	Identity → VPN Session Log (auth method per session) Identity → Anomalies (MFA bypass alerts)
Questionnaire answer:	**YES — with continuous evidence log**

2. Endpoint Detection & Response (EDR) **[FULL]**

Carrier asks:	Viperbyte covers ALL network-connected devices agentlessly via passive SPAN monitoring — laptops, servers, IoT devices, printers, cameras, HVAC controllers, badge readers.
Viperbyte coverage:	100% of network-connected devices — including those agents miss Viperbyte covers ALL network-connected devices agentlessly via passive SPAN monitoring — laptops, servers, IoT devices, printers, cameras, HVAC controllers, badge readers. ~60% of enterprise endpoints are invisible to agent-based EDR. Viperbyte's AI brain monitors behavioral patterns 24/7 with F1 accuracy of 99.24%. Optional: pair with Microsoft Defender for depth on managed Windows endpoints.
Evidence artifact:	Brain → Device Baseline · Viper Live → Detection Events (24/7 log) Metrics: 100,000+ threats blocked · 2,929 AI decisions
Questionnaire answer:	**YES — 100% network coverage including agentless devices**

3. Privileged Access Management (PAM) **[SUBSTANTIAL]**

Carrier asks:	Viperbyte Identity Engine identifies and separately tracks all privileged accounts (domain admins, service accounts) via Zeek NTLM/Kerberos and MSAD LDAP connector.
Viperbyte coverage:	Privileged account monitoring + behavioral profiling Viperbyte Identity Engine identifies and separately tracks all privileged accounts (domain admins, service accounts) via Zeek NTLM/Kerberos and MSAD LDAP connector. Any privileged account behavior outside its established baseline triggers an anomaly alert. NOTE: Viperbyte monitors PAM; it does not replace a PAM vault (CyberArk, BeyondTrust).
Evidence artifact:	Identity → Privileged Account Cards Identity → Behavioral Anomaly Log · MSAD → Admin Change Log

Questionnaire answer:	**YES (monitoring) — PAM vault recommended for full credit**

4. Network Segmentation & Monitoring — [FULL]

Carrier asks:	Viperbyte enforces network segmentation via zone architecture: WAN (honeypots + limited ingress), LAN (full trust), WiFi (captive portal), VPN (profile-specific).
Viperbyte coverage:	Network zones enforced + all boundary traffic monitored Viperbyte enforces network segmentation via zone architecture: WAN (honeypots + limited ingress), LAN (full trust), WiFi (captive portal), VPN (profile-specific). nft/ipset ruleset enforces zone boundaries with 1.38M threat indicators. Every connection inspected. Deception Layer (43 honeypots) profiles lateral movement.
Evidence artifact:	Security → Enforcement Log · Settings → Network Zones Viper Live → WAN Threat Grid
Questionnaire answer:	**YES — enforced segmentation + continuous monitoring with evidence**

5. Vulnerability Scanning & Patching — [SUBSTANTIAL]

Carrier asks:	Viperbyte runs continuous passive vulnerability assessment across all network-connected assets.
Viperbyte coverage:	Continuous passive scanning + on-demand report Viperbyte runs continuous passive vulnerability assessment across all network-connected assets. On-demand Pentest Report generates: open service enumeration, Shodan WAN exposure analysis, known CVE cross-reference against observed services, and remediation priorities. Report is timestamped and exportable for underwriter submission.
Evidence artifact:	Security → Pentest Report (exportable PDF) Threat Intel → CVE Cross-Reference Log
Questionnaire answer:	**YES — continuous passive scanning with dated report artifact**

6. Data Backup & Recovery Testing — [NOT COVERED]

Carrier asks:	SEPARATE SOLUTION REQUIRED
Viperbyte coverage:	Outside Viperbyte's scope Viperbyte does not manage backups or recovery testing. This control must be addressed with a dedicated backup solution (Veeam, Acronis, Druva, or cloud-native backup with immutability enabled). Recovery must be tested and documented annually.
Evidence artifact:	No Viperbyte evidence for this control. Requires: backup platform logs + dated recovery test

	record.
Questionnaire answer:	**SEPARATE SOLUTION REQUIRED**

7. Incident Response Plan & Testing — [SUBSTANTIAL]

Carrier asks:	Viperbyte auto-generates a timestamped evidence chain for every detected incident — entity, behavior, confidence score, enforcement action, and resolution.
Viperbyte coverage:	IR evidence chain + detection capability; plan document still required Viperbyte auto-generates a timestamped evidence chain for every detected incident — entity, behavior, confidence score, enforcement action, and resolution. This satisfies the 'documented incident record' requirement and demonstrates active detection. The written IR plan (who does what, escalation, notifications) must still be written — typically a one-time $3,000–$5,000 engagement.
Evidence artifact:	Compliance → Evidence → IR Controls Viper Live → Incident Feed · evidence_chain.json per incident
Questionnaire answer:	**YES (detection + evidence) — written IR plan separately required**

8. Centralized Logging & SIEM Monitoring — [FULL]

Carrier asks:	Viperbyte's Network Intelligence Engine IS the centralized log and monitoring system.
Viperbyte coverage:	On-prem SIEM equivalent — all sensors, continuous, 365-day retention Viperbyte's Network Intelligence Engine IS the centralized log and monitoring system. All network events, DNS queries, identity sessions, threat intelligence hits, and enforcement actions are logged continuously in a single tamper-evident store. The AI brain reviews every event for anomalies 24/7 — no analyst required. Log retention: 365 days. Export: structured JSON or compliance report.
Evidence artifact:	Viper Live → Full Event Log · Compliance → Audit Domain (AU controls) Export: full log archive for any date range
Questionnaire answer:	**YES — 24/7 autonomous monitoring, 365-day centralized log retention**

Secondary Controls — Additional Questions Carriers Ask

Secondary Control	Viperbyte Coverage	Notes
DNS Filtering (malware/C2 blocking)	**FULL**	Viperbyte DNS Security Engine — Pi-hole ML blocks malware callbacks, C2 channels, and known-malicious domains. Every DNS query logged. Carrier question

		answered: Yes, with log.
Email Security (anti-phishing/DMARC)	**NOT COVERED**	Email security requires a dedicated gateway (Proofpoint, Mimecast, Defender for O365). Viperbyte monitors post-phishing-click behavior but cannot filter inbound email.
Security Awareness Training	**NOT COVERED**	Human training requires KnowBe4, Proofpoint, or equivalent. Carrier requires completion rate evidence. ~$3,500–$8,000/yr for 50–200 users.
Third-Party Vendor Risk	**PARTIAL**	Viperbyte monitors outbound traffic to third-party services and flags anomalous data flows. Formal vendor risk questionnaire process requires a GRC tool or manual program.
Zero Trust Progress (larger orgs)	**SUBSTANTIAL**	Viperbyte's identity-based enforcement, network segmentation, and behavioral verification directly implement core zero trust principles — verified identity + device posture per session.

5. The Premium Math — What Documented Controls Are Worth

Cyber insurance pricing is not arbitrary. Carriers use actuarial models that weight specific controls against historical claims data. The following model illustrates the impact for a representative 100-employee organization seeking $5M in cyber coverage. Figures are directional based on published industry data and actual carrier pricing trends — individual results vary by carrier, industry, and risk profile.

Illustrative Premium Model — 100 Employees / $5M Coverage Limit

Scenario	Controls Documented	Annual Premium (Est.)	Coverage Quality
No Controls Documented	MFA email only No EDR, no SIEM, no vuln scanning	**$95,000–$140,000**	High deductible ($100K+). Ransomware sublimit ($250K). May be declined entirely.
Partial Controls (typical SMB today)	MFA on email+VPN EDR on laptops only No SIEM, no scanning	**$60,000–$85,000**	Moderate coverage. Ransomware sublimit likely. Some exclusions remain.
Viperbyte Deployed (documented controls)	MFA monitored Full network coverage SIEM + logging + DNS Vuln scanning	**$38,000–$55,000**	Standard ransomware coverage. Lower retention. Claims-defensible evidence.
Viperbyte + Full Stack (best-in-class posture)	All above + PAM vault + tested backups + IR tabletop + security training	**$28,000–$40,000**	Preferred pricing. Full ransomware coverage. Lowest deductible available.

$42,000
Estimated annual savings
Scenario 1 vs Scenario 3 (midpoints), 100 employees

$126,000
3-year premium savings
vs no-controls baseline, before any breach reduction

$47,000
Viperbyte annual platform cost
3-yr premium savings exceed Viperbyte cost in year 2

89%
of Viperbyte cost recovered
In year 1 premium savings alone (midpoint comparison)

6. Ransomware — The Claim Type That Reshaped the Market

Ransomware accounts for the majority of cyber insurance claim dollars paid out since 2020. It is the reason premiums increased, the reason carriers added sublimits and exclusions, and the reason the questionnaire grew from 5 pages to 25. Understanding how ransomware actually works — and where Viperbyte interrupts it — is essential context for any cyber insurance conversation.

How a Ransomware Attack Unfolds — and Where Viperbyte Intervenes

Stage	Attacker Action	Viperbyte Interrupt Point
Initial Access	Phishing credential harvester, or brute-force on exposed RDP/VPN	Impossible travel detection — simultaneous remote sessions from different geographies flag immediately. VPN session attributed to user identity; anomalous login source triggers alert.
Establish Foothold	Deploy C2 beacon. Establish persistence via registry or scheduled task.	DNS Security Engine detects C2 beacon callbacks at the DNS layer — even before the payload executes. Deception Layer honeypots catch reconnaissance within minutes.
Privilege Escalation	Dump credentials (Mimikatz). Identify domain admin accounts.	Identity Engine detects unusual privileged account activity. NTLM pass-the-hash and Kerberoasting patterns surface in kill-chain model (GRU F1=0.897).
Lateral Movement	Spread using admin credentials. Map file shares. Identify backup systems.	Network Intelligence Engine detects unusual east-west traffic. Deception Layer honeypots act as tripwires — any lateral movement triggers alert.
Data Exfiltration	Stage data. Transfer to attacker-controlled infrastructure.	Detects anomalous outbound data volume. Unusual destination IPs cross-referenced against 1.38M threat indicators. Exfiltration to known-bad infrastructure blocked.
Encryption	Deploy ransomware payload. Encrypt files. Delete shadow copies. Demand payment.	Multiple interrupt opportunities already occurred. If encryption begins, Viperbyte detects the mass file operation pattern and isolates the affected device within <2 seconds.
DWELL TIME without Viperbyte	**Industry average: 258 days (IBM 2024)**	**With Viperbyte: multiple alert opportunities within hours of initial access. Deception Layer typically provides first alert within minutes of foothold. MTTD compressed from 258 days to hours.**

WHY THIS MATTERS FOR INSURANCE: Carriers price ransomware risk on expected dwell time. 258-day average dwell = attacker has exfiltrated data AND encrypted files = maximum payout.

Organizations with active detection that compresses dwell time to hours represent fundamentally lower ransomware risk — and carriers that use dynamic pricing models price them accordingly.

7. Claims Defensibility — Why Continuous Evidence Changes the Outcome

When a breach occurs and a claim is filed, the insurer's forensic team asks one question: were reasonable security controls active and documented at the time of the incident? If the answer is 'we had controls but cannot prove they were running,' the carrier has grounds to invoke the reasonable security exclusion.

Claims Factor	Without Viperbyte — Typical Outcome	With Viperbyte — Claims Position
Evidence that controls were active	Point-in-time attestation. 'We had these controls.' No continuous record. Carrier investigates and finds gaps.	365 days of continuous, timestamped log chain. Every control active and logged every day. Carrier can verify any date in the past 12 months.
Detection timeline (when was breach known?)	Often unknown — attacker dwell for weeks or months with no log. Carrier assumes attacker had full access to all data for entire dwell period.	Exact first-alert timestamp in evidence chain. Dwell time documented from Viperbyte detection forward. Carrier calculates actual exposure.
Scope of breach (what was accessed?)	Forensic reconstruction from fragmented logs — often inconclusive. Carrier prices claim at maximum data exposure.	Identity Engine shows exactly which users and devices were active. Network Intelligence Engine shows all connections made. Actual scope documented.
Incident response actions taken	'We took action once we discovered it.' No timeline. No containment steps. Carrier cannot assess response quality.	Evidence chain records every enforcement action with timestamp: what was blocked, when, AI decision confidence, and what lateral movement was stopped.

THE DIFFERENCE IN A CLAIM: Without Viperbyte: 'We believe we had controls in place.' Carrier disputes. Claim drags 12–18 months. Settlement at 40–60 cents on the dollar.
With Viperbyte: 'Here is the evidence chain. Controls were active every day for the past year. Breach detected at [timestamp]. Scope contained to [documented assets]. Enforcement actions logged.' Carrier has no basis for dispute. Clean claim.

8. Return on Investment — The Full Financial Model

The ROI calculation for Viperbyte in the context of cyber insurance has three components: direct premium savings, reduced breach probability, and claims-outcome improvement. The following model uses conservative assumptions for a 100-employee organization with $5M in cyber coverage.

3-Year ROI Model — 100 Employees, $5M Cyber Coverage

ROI Component	3-Year Value	Basis
Annual premium savings (documented controls)	**+$42,000/yr = $126,000 over 3 yrs**	Scenario 1 vs Scenario 3 midpoints from Section 5. Conservative estimate.

Reduced ransomware sublimit (full coverage restored)	**+$250,000 recovered coverage capacity**	Without documented controls, ransomware sublimits of $250K–$500K common instead of full policy limits.
Lower retention / deductible	**+$25,000–$50,000 in exposure reduction**	Carriers reduce minimum retentions for organizations with documented controls. $50K–$100K retention reduction common when SIEM and EDR are confirmed.
Reduced breach probability (threat prevention in production)	**100,000+ threats blocked 2,929 AI decisions**	Viperbyte's production metrics demonstrate active threat prevention. Each prevented intrusion represents avoided breach costs averaging $4.9M (IBM 2024).
Claims outcome improvement (continuous evidence vs. disputed)	**Avoid 40–60% claim discounting on dispute**	On a $1M ransomware claim, a disputed settlement at 50 cents recovers $500K. A clean claim recovers $1M. Viperbyte's evidence chain is the difference.
Viperbyte platform cost (3-year total)	**-$141,000 ($47K/yr × 3)**	Annual platform license. Hardware one-time ~$3.5K additional. No MSSP. No SIEM license. No additional monitoring cost.
NET 3-YEAR ROI	**+$260,000–$310,000 cash value + risk reduction**	Premium savings ($126K) + retention improvement ($37.5K avg) + Viperbyte cost (-$141K) + unquantified breach prevention value. Payback period: 12–18 months.

What Viperbyte Does NOT Replace — Remaining Insurance Checklist Items

The following require separate solutions and should be addressed alongside Viperbyte to achieve the best possible underwriting outcome:

- **Data backup + tested recovery:** Veeam, Acronis, or cloud-native with immutability + annual recovery test
- **Email security + anti-phishing:** Microsoft Defender for O365, Proofpoint, or Mimecast
- **Security awareness training:** KnowBe4 or equivalent — 50 users ~$3,500/yr
- **Written IR plan:** One-time document — attorney or IR consultant, $3,000–$5,000
- **PAM vault (for full PAM credit):** CyberArk, BeyondTrust, or Delinea

> **THE FINAL WORD:** Cyber insurance is not a substitute for security — it is a backstop. Viperbyte is not built to answer questionnaire questions. It is built to stop attacks, attribute every event to a named identity, and produce continuous evidence that your controls worked — every day. The insurance benefits are a byproduct of running a genuinely secure environment.