

DIGITAL DEFENSE DIGEST

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHAT'S NEW

Ransomware Surge Alert for Growing Businesses:

2025 hit 7,515 victims (+58% YoY) and 2026 is accelerating with AI in 80% of attacks. Get the latest intel to keep your SMB safe.

New Free Ransomware Defense Guide for 2026:

Our March report delivers Q1 TTPs, Zero Trust steps, AI detection tactics, backup essentials, case studies, and ROI metrics. Download free now!

Lock Down Perimeter Vulnerabilities Before It's Too Late:

ESXi and FortiGate remain top ransomware entry points in Q1 2026. Learn our quick steps to patch, hide interfaces, and stop smash-and-grab attacks.

This monthly publication is provided by Black Belt Secure



OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

RANSOMWARE: RECORD-BREAKING IN 2025, ACCELERATING INTO 2026- DON'T GET CAUGHT OFF GUARD

The ransomware threat didn't just persist in 2025—it exploded. Reports from GuidePoint Security's 2026 GRIT Ransomware Report show **7,515 publicly posted victims across 124 distinct groups—a staggering 58% year-over-year increase**. Q4 2025 alone saw over 2,000 incidents, with January 2026 continuing the surge (679 claimed victims in one month per Cyble). Attackers are faster, smarter, and more automated: **AI tools now feature in 80% of attacks** (MIT 2025 study), enabling low-skill actors to scale phishing, reconnaissance, and even negotiation bots.

For businesses, the stakes are higher than ever—average recovery costs hover around \$2-3M (with downtime often 20+ days), and many victims face data extortion, regulatory fines, and reputational hits long after payment. Edge devices (ESXi servers, FortiGate firewalls) remain prime entry points, as seen in our recent blogs on persistent vulnerabilities. This month's spotlight: [Our new March 2026 report](#)

Ransomware Defense in 2026: Prevention, Detection, and Recovery Best Practices This comprehensive guide cuts through the noise with:

- Real Q1 2026 TTPs from groups like Qilin, Akira, and emerging players
- Prevention roadmap: Zero Trust implementation, rapid patching (e.g., for ESXi/Fortinet CVEs), MFA enforcement
- Detection tactics: Behavioral EDR, deception tech, AI-driven anomaly hunting
- Recovery essentials: Immutable/air-gapped backups, tested restores, isolated environments
- Case studies from recent campaigns (e.g., FortiGate mass breaches, supply-chain hits)
- ROI-focused metrics to align security with board priorities

[Download your free copy today.](#)

Black Belt Secure's 24/7 SOC responds in 5 minutes or less (average 3.5 minutes)—let's put that speed to work for you.

continued on page 2...

THREAT LANDSCAPE UPDATE Q1 2026 RANSOMWARE & VULNERABILITY SNAPSHOT

What's Hot Right Now Ransomware isn't slowing, it's evolving:

Perimeter Exploitation Dominates

Firewalls, VPNs, and exposed servers (e.g., VMware ESXi) are top initial access vectors. Our Feb 11 blog "Neverending ESXi Security Vulnerabilities" details how unpatched public-facing ESXi instances enable VM escapes and rapid encryption. GuidePoint notes continued emphasis on these "smash-and-grab" footholds. Attackers prioritize these edge devices for quick entry, often exploiting known CVEs like arbitrary write flaws or privilege escalations to gain hypervisor control, encrypt VMs en masse, and demand ransom before defenders can respond effectively, underscoring the persistent danger of internet-exposed virtualization infrastructure in 2026 threat landscapes.

Fortinet Family Under Fire

Persistent CVEs (e.g., auth bypasses, 2FA flaws) in FortiGate and FortiSIEM drive mass compromises—hundreds affected in recent waves (see our Jan blogs on Fortinet woes). Vulnerabilities such as CVE-2024-21762 and

CVE-2024-55591 continue enabling remote code execution and super-admin access on unpatched SSL-VPN devices. Ransomware affiliates exploit these repeatedly in automated campaigns, targeting misconfigured or legacy systems, resulting in widespread network infiltration, data exfiltration, and encryption across diverse sectors despite available patches.

AI as Force Multiplier

80% of groups promote AI for phishing automation, code generation, and scaling (Acronis/MIT insights). Low-skill attackers now breach at volume, as in the AI-assisted FortiGate campaign we covered. Tools enhance reconnaissance, craft hyper-personalized lures, optimize extortion messaging, and automate negotiations, allowing even novice operators to execute sophisticated, high-volume operations that evade traditional detection and dramatically increase the speed and scale of successful intrusions across global targets.

Supply-Chain & Insider Risks

Notepad++ hijacks (Chinese state-linked, Feb 4 blog), ShinyHunters SSO/vishing (Feb/Jan blogs), and initial access brokers selling network footholds signal a maturing cybercrime economy.

Global Surge

30%+ above 2025 monthly averages (Cyble), with tactics like DDoS-as-a-Service, insider recruitment, and gig-worker exploitation on the rise (Recorded Future). January 2026 alone saw 679 claimed victims, sustaining Q4 2025's elevated pace. This acceleration reflects industrialized operations, affiliate models, and diverse extortion methods, pressuring organizations worldwide as attackers diversify entry points, leverage underground services, and exploit human elements for faster, more profitable campaigns.

Bottom line: Reactive patching fails against adaptive threats. Proactive, layered defenses—backed by continuous monitoring—are essential for resilience.

FREE REPORT:

Ransomware Defense in 2026

- Ransomware has become a ruthless, billion-dollar criminal machine—attacks up 47% in 2025, projected to smash 12,000+ globally this year. It's in 44% of all breaches, targets backups in 96% of cases, and uses AI for deadly phishing and deepfakes.
- CEOs and executives can no longer shrug it off with "It won't happen to us." Your company—whether a Fortune 500 giant or a local SMB—will be in the crosshairs. The average attack now costs millions in recovery, downtime, and lost trust, even if you refuse to pay (and more organizations are refusing, driving criminals to evolve even faster).



Claim Your FREE Copy Today At: blackbeltsecure.com/reports

QUICK HITS & BEST PRACTICES

5 PRACTICAL STEPS TO BUILD RANSOMWARE RESILIENCE IN 2026

Prioritize Immutable & Isolated Backups

Adopt WORM storage, air-gapped/off-site copies, and quarterly restore testing. Many victims learn too late that backups were encrypted—don't join them. Implementing the modern 3-2-1-1-0 rule ensures three copies of data on two different media types, with one off-site and one immutable or fully air-gapped for unbreakable isolation. Regular integrity checks and automated verification eliminate the "0 errors" goal, while physical or logical air-gapping (via tapes, offline drives, or compliant cloud object lock) prevents ransomware from reaching backups even after network compromise. This layered approach drastically reduces recovery time and financial impact.

Lock Down Perimeter & Lateral Movement

Hide management interfaces (no public ESXi/FortiGate exposure), enforce micro-segmentation, and deploy EDR with rules for PowerShell/RDP anomalies. Patch aggressively—our blogs highlight why delays cost dearly. By eliminating direct internet exposure to critical admin tools and applying zero-trust principles, you block initial footholds. Micro-segmentation creates granular barriers between workloads, limiting east-west attacker propagation even if one system is breached. Advanced EDR monitors behavioral anomalies like unusual PowerShell execution, RDP brute-forcing, or credential dumping, enabling rapid isolation. Consistent patching closes exploited vulnerabilities before ransomware actors can chain them into full

network takeover.

Combat AI-Enhanced Phishing & BEC

Use email gateways for domain spoofing detection, train on deepfake/vishing red flags, and monitor for unusual data exfiltration. In 2025–2026, AI has supercharged attacks with hyper-personalized spear-phishing, voice-cloned vishing calls mimicking executives, and deepfake videos in urgent BEC scenarios—driving massive surges in successful fraud. Robust secure email gateways now incorporate AI-driven spoofing and anomaly checks, while employee training emphasizes callback verification, behavioral red flags (e.g., unexpected urgency or slight audio glitches), and multi-channel confirmation. Pair this with data loss prevention tools that flag abnormal outbound transfers, ensuring early detection before funds or data are lost.

Leverage Executive Oversight

Our Jutsu Program delivers fractional vCISO leadership: risk assessments, compliance roadmaps, quarterly board reports, and strategic alignment—so security supports growth, not just survival. A fractional vCISO brings executive-level expertise without the full-time cost, providing tailored risk prioritization, policy development, and board-ready communication in business terms. This bridges the gap between technical teams and leadership, ensuring cybersecurity investments align with organizational goals. Regular assessments identify gaps, while compliance roadmaps navigate regulations like GDPR or NIS2 efficiently. The result: proactive security

posture that builds stakeholder confidence, reduces regulatory fines, and positions security as a business enabler rather than a cost center.

Enable Rapid Response

Partner with a 24/7 SOC for threat hunting and containment. Black Belt Secure guarantees executive-level assurance—if our guidance falls short, we remediate at our expense. A dedicated round-the-clock SOC combines continuous monitoring, proactive threat hunting, and automated playbooks to detect ransomware indicators early—often before encryption begins. Skilled hunters use behavioral analytics and threat intelligence to uncover hidden persistence, while rapid containment (e.g., endpoint isolation) minimizes damage. Our skin-in-the-game model means we stand behind recommendations with remediation accountability, delivering peace of mind, faster mean-time-to-respond, and true resilience against evolving threats.

QUICK STAT SPOTLIGHT

2025 Record:
7,515 victims, 124 groups
(GuidePoint GRIT 2026)

2026 Trend:
AI in 80% of attacks; Q1 surges
continuing (Cyble, Palo Alto
Unit 42)

Business Impact:
Recovery averages millions +
weeks of downtime—
prevention saves far more.



Defend Today, Thrive Tomorrow.

CALL TO ACTION & CONTACT SECURE YOUR BUSINESS BEFORE THE NEXT WAVE HITS



Black Belt Secure stands ready with:

24/7 Managed Detection & Response (MDR)

Continuous monitoring, threat hunting, and incident containment

vCISO & Jutsu Program

Strategic governance, risk/compliance roadmaps, board-ready insights

Ransomware-Specific Services

Assessments, backup hardening, recovery planning, Zero Trust integration

Award-Winning MSSP Expertise

National recognition for rapid response and peace-of-mind guarantees

Take the Next Step Today

Claim your free Ransomware Defense in 2026 report:

<https://marketing.blackbeltsecure.com/asset/22:ransomware-defense-2026-guide>.

Book a no-obligation 30-minute posture review: (<https://blackbeltsecure.com/audit>)

Subscribe for future Digests & exclusive alerts: blackbeltsecure.com/newsletter



Questions? Email info@blackbeltsecure.com or visit blackbeltsecure.com for a free assessment.

