DIGITAL DEFENSE DIGEST

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

WHAT'S NEW

Zero Trust Momentum Builds: 81% of orgs plan full Zero Trust adoption by end-2026; Gartner notes strong shift amid AI/cloud risks. Perimeters are gone–verify every access to shrink breach impact. Start small: secure admin & cloud first.

Ransomware Surge Intensifies: 2025 attacks rose 30-58% YoY, hitting essentials hardest. Offline backups, segmentation, and fast patching enable quick recovery without payment–basics still win.

AI Threats Evolving Rapidly: AI vulnerabilities now fastest-growing risk; used for smarter phishing, deepfakes, and automation. Counter with phishing-resistant MFA, behavioral detection, deepfake training, and safe-AI policies.

This monthly publication is provided by Black Belt Secure

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

Welcome to the February edition of the Black Belt Secure Newsletter! As 2026 begins, cyber threats are accelerating: AI-related vulnerabilities are now the fastest-growing risk (with 87% of leaders identifying them as top concern per the World Economic Forum's Global Cybersecurity Outlook 2026), supply chain disruptions remain a major barrier for 65% of large organizations (up sharply from last year), and ransomware persists with greater sophistication—fueling more targeted, high-impact campaigns that exploit AI for speed and scale.

In today's hybrid, cloud-first world—where perimeters have dissolved and remote work expands the attack surface—businesses face mounting pressure to protect sensitive data, achieve strict compliance, prevent operational downtime, and safeguard reputation amid escalating costs and regulatory scrutiny. At Black Belt Secure, we're dedicated to helping you build truly resilient defenses through managed cybersecurity, 24/7 SOC monitoring, and strategic vCISO guidance tailored to your needs. This month, we share practical, high-impact tips to strengthen your security posture immediately and explain why Zero Trust is essential—not optional—for containing breaches, limiting lateral movement, and enabling secure innovation in this dynamic threat environment. Read on for actionable advice, and don't miss our latest white paper on implementing Zero Trust (linked below).Quick Stats Teaser (to grab attention):

- 81% of organizations plan to adopt full Zero Trust by end of 2026.
- AI-related vulnerabilities are the fastest-growing cyber risk this year.
- Supply chain attacks remain a top concern for 65% of large businesses.

continued on page 2...

...continued from cover

WHY ZERO TRUST MATTERS MORE THAN EVER IN 2026

Traditional perimeter-based security is outdated in today's hybrid, cloud-heavy world. Threats assume no one—inside or outside your network—should be trusted by default.

Key Reasons Zero Trust is Becoming Essential:

1 Dissolving Perimeters

Remote/hybrid work, widespread cloud adoption, and the explosion of IoT devices have completely eliminated traditional network boundaries. Employees access resources from home offices, coffee shops, and mobile devices, while data flows across multiple clouds and third-party platforms. Attackers exploit these gaps to move freely once inside. Zero Trust counters this by verifying every access request continuously—regardless of location or user—following the core principle of "never trust, always verify." This continuous validation replaces outdated perimeter defenses with identity- and context-based controls that adapt to today's borderless environment.

2 Rising Threats

Ransomware, sophisticated phishing campaigns, and supply chain attacks have surged dramatically in recent years, with attackers leveraging AI to automate reconnaissance and evasion techniques. These threats often start small (e.g., a single compromised credential) but rapidly spread across networks. Zero Trust limits lateral movement by enforcing strict segmentation and least-privilege access, dramatically reducing breach impact and containing the "blast radius." Even if a threat actor gains initial entry, they face repeated verification barriers, making it far harder to escalate privileges or exfiltrate data.

3 Business Benefits

Adopting Zero Trust builds greater trust with customers and partners by demonstrating proactive, modern security practices. It simplifies compliance with regulations such as GDPR, HIPAA, and emerging U.S. cyber requirements, while enabling secure innovation—safely adopting cloud services, AI tools, and new technologies without exposing the organization. By replacing risky, always-on VPNs with granular, context-aware controls, businesses gain improved security posture, better scalability, and operational simplicity. Independent studies consistently show Zero Trust reduces incident response time, lowers overall risk, and supports long-term cost savings.

4 Industry Momentum

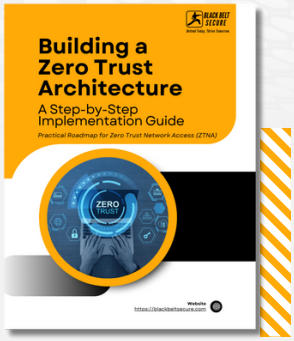
Gartner predicts 70% of enterprises will adopt Zero Trust models by end-2026. 96% favor the approach, with many transitioning from legacy systems for better protection against insider threats and credential theft.
Zero Trust isn't just a buzzword—it's becoming the default security posture for resilient businesses.

FREE REPORT:

Implementing Zero Trust: A Practical Guide for Businesses 2026

It covers steps, common pitfalls, and how Black Belt Secure's ZTNA integration can accelerate your journey

Click here to Download

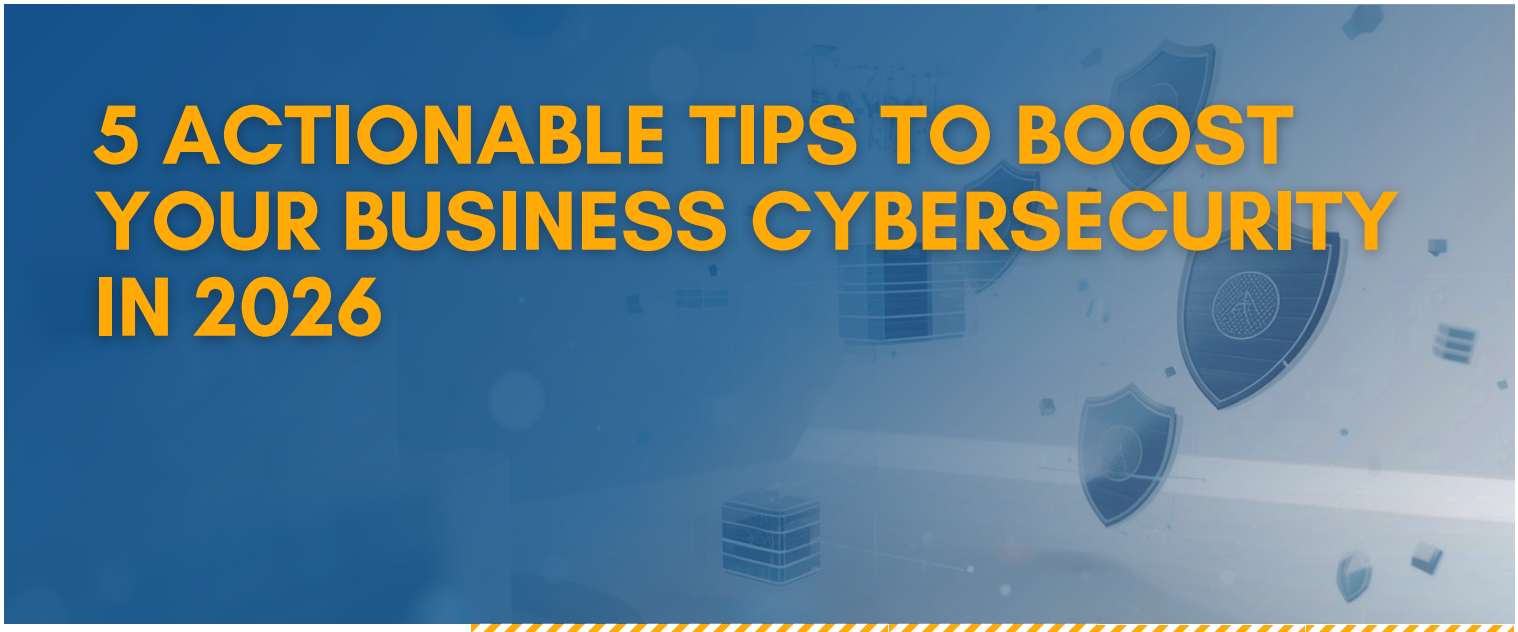


Claim Your FREE Copy Today At: blackbeltsecure.com/reports

TIP

Start small—focus on high-risk areas like admin accounts and cloud access.

5 ACTIONABLE TIPS TO BOOST YOUR BUSINESS CYBERSECURITY IN 2026



1 Enforce Phishing-Resistant MFA Everywhere

Upgrade to phishing-resistant multi-factor authentication (e.g., FIDO2/WebAuthn hardware security keys like YubiKey or Google Titan, or biometrics via platform authenticators such as Windows Hello) for all users, with mandatory enforcement for admins, privileged accounts, and high-risk systems. Completely phase out SMS-based MFA and legacy one-time passwords due to vulnerabilities like SIM-swapping, phishing, and prompt bombing. This aligns with CISA recommendations and federal guidance, significantly reducing credential theft risks in an era of advanced social engineering. **Tip:** Review and remove legacy/shared accounts monthly, and integrate with Conditional Access policies for stronger enforcement.

2 Prioritize Patching & Vulnerability Management

Focus aggressively on Known Exploited Vulnerabilities (KEV) from the CISA catalog first, as these are actively exploited in real-world attacks—remediate them within tight deadlines (e.g., two weeks for recent entries). Automate patching processes for operating systems, applications, browsers, network rdevices, and third-party software using tools that prioritize KEV entries and track compliance. Establish continuous monitoring, vulnerability scanning, and exception handling for delayed patches to minimize exposure windows and prevent common breach vectors. **Tip:** Conduct quarterly vulnerability scans (or more frequently for critical assets) and address high-severity issues within days—statistics show unpatched software remains a primary entry point for most breaches.

3 Secure Remote & Hybrid Workforces

Replace traditional VPNs with secure access tools like Zero Trust Network Access (ZTNA), which verifies identity, device posture, and context before granting application-specific access—reducing risks from broad network exposure. Ensure home Wi-Fi uses strong encryption, firewalls, and regular employee training on safe usage. **Tip:** Create and enforce a comprehensive mobile device policy, including mandatory endpoint detection/response (EDR) on all work devices to block threats at the edge.

4 Secure Remote & Hybrid Workforces

Maintain offline, verified, and ideally immutable backups following an enhanced 3-2-1-1 rule (three copies, two media types, one off-site/air-gapped, plus one immutable copy). Test restores regularly to confirm recoverability. Develop, document, and routinely test an incident response plan. **Tip:** Segment networks to limit ransomware lateral movement—pair this with 24/7 SOC monitoring (like our services) for early detection and rapid containment.

5 Train Employees & Audit Access Regularly

Run ongoing awareness training on phishing, AI deepfakes, and safe AI tool use. Review user permissions quarterly to eliminate "zombie" accounts. **Tip:** Treat browser extensions like unvetted vendors—monitor and restrict risky ones.

BONUS QUICK WIN

Enable strong password policies + a password manager, and audit third-party vendors for supply chain risks.

These steps align with Black Belt Secure's Managed Security Services—let us handle the heavy lifting while you focus on growth

BLACK BELT SECURE

Defend Today, Thrive Tomorrow.

STAY AHEAD WITH BLACK BELT SECURE THANK YOU FOR READING!

Cybersecurity isn't a one-time fix—it's an ongoing strategy. As threats like AI-supercharged attacks and supply chain vulnerabilities grow, partnering with experts ensures your business stays protected and compliant. Our Services Recap:

- Managed Cybersecurity & 24/7 SOC Monitoring
- vCISO Program for Strategic Guidance
- Zero Trust Implementation & Cloud Security
- Compliance, Auditing, & Disaster Recovery

Call to Action:

- Download our Zero Trust white paper today!
- Schedule a free cybersecurity assessment or vCISO consultation.
- Visit https://blackbeltsecure.com or reply to this email.

We're here to help you defend today and thrive tomorrow.

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