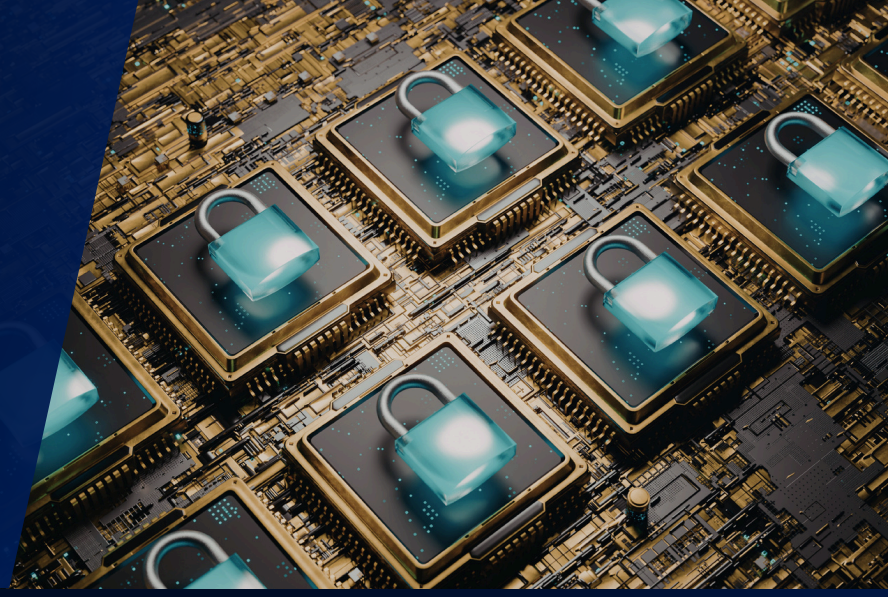
InfoSight®
www.infosightinc.com

INFOSIGHT INSIGHTS

March 2026 Issue

Stay Ahead with the Newsletter
for OT & IoT Cyber Risk & Strategy.



The Expanding Cyber Risk Landscape: AI, Identity, Exposure, and Resilience

March 2026, Vol. I, Issue XIV

This issue examines how cyber risk is widening across every layer of the enterprise—from AI-scaled FortiGate attacks and a more assertive U.S. cyber strategy to critical exposure in backup systems, remote support platforms, and AI development tools. It also highlights the operational impact of agentic AI governance gaps, credential theft, cryptojacking, data breach extortion, and converged malware tradecraft through the latest coverage on OpenClaw, Google's Antigravity restrictions, Claude Code, Wynn Resorts, CharlieKirk Grabber, wormable XMRig activity, and Steaelite RAT. The common thread is clear: today's threats are moving faster, blending tactics, and exploiting weak controls in identity, access, and visibility just as often as they exploit software flaws.

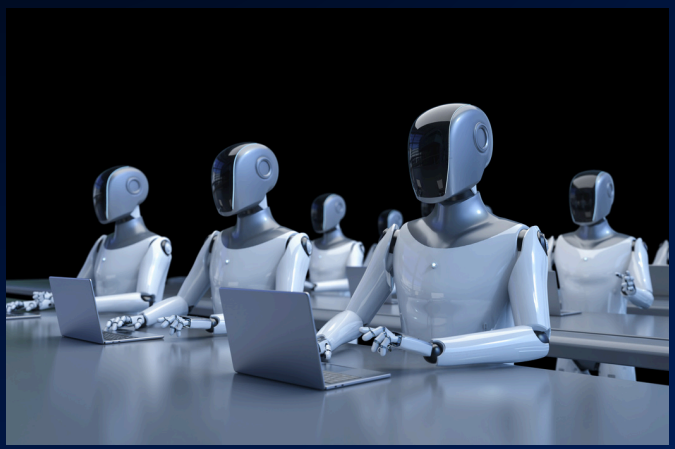
What's Inside

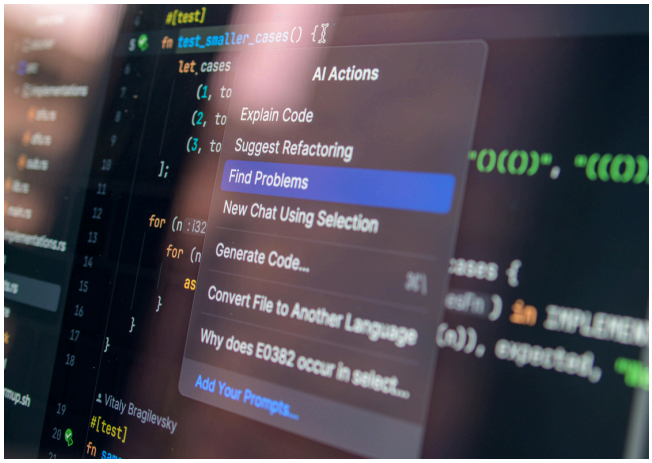
- AI Governance & Emerging Platform Risk
- Critical Enterprise CVEs & Privileged Infrastructure
- Cloud, Firewall & AI-Accelerated Perimeter Attacks
- Malware Evolution, BYOVD & Enterprise Extortion
- Sector Breach Fallout & National Cyber Strategy

AI Governance & Emerging Platform Risk

OpenClaw Security Risks & CISO Guidance

OpenClaw highlights how emerging AI-integrated platforms can introduce governance blind spots when security controls lag behind deployment. The risk is less about the model itself and more about access control, misuse potential, and insufficient oversight of AI outputs. CISOs must evaluate how AI systems connect to identity systems, internal data sources, and automation pipelines. Without structured governance, AI tools can become unmonitored escalation paths. Read more.





Google OpenClaw / AntiGravity AI Governance Risk

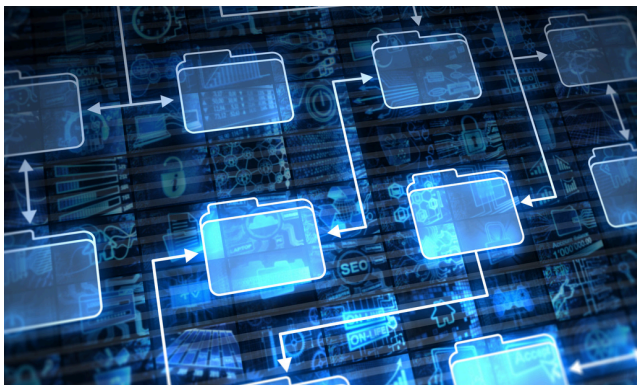
Google's OpenClaw and AntiGravity initiatives underscore the growing tension between AI innovation and enforceable guardrails. As AI systems gain broader operational capabilities, improper constraint mechanisms can allow misuse, manipulation, or unintended automation at scale. Governance maturity (not just technical sophistication) will determine enterprise resilience. Security leaders must ensure AI deployments are continuously evaluated against policy, access scope, and abuse potential. Read more.

Claude Code Vulnerabilities in AI Coding Tool Security

AI-assisted coding tools like Claude Code introduce new risk layers when vulnerabilities affect how generated code is handled, reviewed, or integrated. Even minor control failures in AI development pipelines can propagate insecure configurations across environments. Organizations adopting AI coding assistants must implement validation, secure SDLC integration, and strict permission boundaries. Trust in automation should never replace verification. Read more.

Critical Enterprise CVEs & Privileged Infrastructure

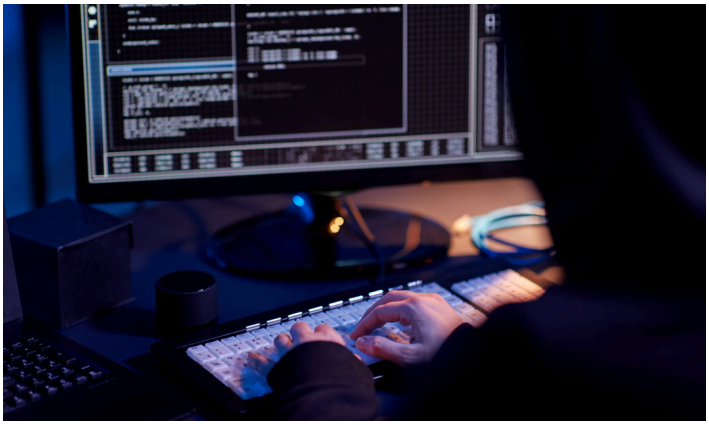
BeyondTrust CVE-2026-1731 Remote Support Vulnerability



CVE-2026-1731 in BeyondTrust's remote support infrastructure demonstrates how privileged access platforms remain high-value targets. Exploitation of remote support tools can provide attackers with elevated visibility and control inside enterprise networks. When trust-based tools are compromised, lateral movement becomes significantly easier. Continuous patch validation and strict access segmentation are critical safeguards. Read more.

Dell RecoverPoint Hardcoded Credential Vulnerability

Dell RecoverPoint's hardcoded credential vulnerability exposes the ongoing risk of embedded trust within enterprise backup and recovery systems. Hardcoded credentials undermine authentication boundaries and create predictable access points for attackers. Because recovery systems often sit deep within infrastructure, compromise can have cascading operational consequences. Identity governance must extend to infrastructure components often considered "trusted by default." Read more.



Cloud, Firewall & AI-Accelerated Perimeter Attacks

AWS & FortiGate Firewall Attacks Amplified by AI

Recent attacks targeting FortiGate firewalls within AWS environments show how perimeter infrastructure remains under sustained pressure. AI-enhanced reconnaissance and exploitation techniques are accelerating vulnerability discovery and weaponization timelines. Misconfigured firewall rules and exposed management interfaces continue to provide footholds. Organizations must treat cloud perimeter controls as dynamic assets requiring continuous monitoring and validation. Read more.

Malware Evolution, BYOVD & Enterprise Extortion

Wormable XMRig BYOVD Cryptojacking Campaign

The wormable XMRig campaign demonstrates how attackers weaponize Bring Your Own Vulnerable Driver (BYOVD) techniques to bypass security controls. By abusing legitimate but vulnerable drivers, threat actors gain kernel-level privileges and evade detection. Cryptojacking may seem financially modest compared to ransomware, but its stealth persistence can degrade performance and mask deeper compromise. Driver integrity monitoring and EDR validation are essential defensive layers.
Read more.

CharlieKirk Grabber Windows Infostealer

The CharlieKirk Grabber malware reflects the continued effectiveness of credential harvesting campaigns targeting Windows users. Infostealers prioritize session tokens, browser credentials, and stored authentication data, enabling follow-on access and account takeover. These campaigns often act as initial access brokers for larger ransomware or extortion operations. Endpoint visibility and credential hygiene remain critical defensive pillars.
Read more.

StealElite RAT & Double Extortion Enterprise Risk

StealElite's remote access tooling reinforces the persistence of double-extortion tactics across enterprise environments. Beyond data encryption, attackers leverage stolen information as reputational and regulatory leverage. Modern RATs prioritize stealth, command flexibility, and long-term dwell time. Resilience requires not just backup readiness but data exposure containment and continuous detection. Read more.

Sector Breach Fallout & National Cyber Strategy

Wynn Resorts Data Breach & ShinyHunters Activity

The Wynn Resorts breach highlights the ongoing targeting of hospitality and high-profile service sectors. Groups like ShinyHunters continue to focus on data-rich environments with brand sensitivity and regulatory exposure. Beyond financial loss, reputational damage becomes a central pressure point. Sector-specific risk modeling must account for both operational disruption and public-facing fallout. Read more.

U.S. Cyber Strategy: Industry Coordination & Deterrence

The evolving U.S. cyber strategy emphasizes stronger public-private coordination and deterrence signaling. National resilience increasingly depends on collaboration between government and industry stakeholders. Policy frameworks are shifting toward proactive defense, intelligence sharing, and coordinated response mechanisms. Enterprises should align internal preparedness efforts with broader national risk posture developments. Read more.

How InfoSight Helps

These stories point to the same core problem: organizations are being hit from multiple angles at once, including exposed internet-facing systems, hardcoded credentials, vulnerable remote access tools, AI governance gaps, infostealer malware, and extortion-driven campaigns. InfoSight helps reduce that risk by giving security leaders stronger visibility into exposure, clearer prioritization of what matters most, and practical remediation guidance that moves faster than traditional reactive models.

Through vulnerability management, penetration testing, managed detection and response, security assessments, and strategic advisory support, InfoSight helps organizations identify exploitable weaknesses, harden identity and access controls, validate third-party and cloud risk, and improve readiness before a security event becomes an operational disruption. The result is a more resilient security posture built around continuous risk reduction, faster containment, and executive-level clarity on where the greatest threats exist.

- Identifies exploitable weaknesses early through vulnerability management, penetration testing, and security assessments.
- Improves visibility across the environment so teams can see where exposures exist across systems, identities, cloud assets, and third-party access points.
- Prioritizes the risks that matter most by focusing remediation on the vulnerabilities and control gaps most likely to be exploited.
- Strengthens identity and access controls to reduce the impact of credential theft, privilege misuse, and unauthorized access.
- Validates remote access and external-facing risk to help secure firewalls, remote support tools, and other high-exposure entry points.
- Supports AI and emerging technology risk reviews so organizations can address governance, access, and usage risks tied to new tools.
- Enhances detection and response readiness through managed detection and response services that help contain threats faster.
- Reduces operational disruption by helping organizations move from reactive incident response to continuous risk reduction.
- Provides strategic security guidance so leadership can make better decisions around remediation, resilience, and long-term risk posture.
- Delivers executive-level clarity with reporting and advisory insight that helps leaders understand where the greatest threats exist and what actions to take next.