The Coeus Chronicle

INSIGHT WITH FORESIGHT | VOLUME 1, ISSUE 10 | OCTOBER 2026

Software didn't suddenly get less secure. AI got better at exploiting it.

More capable AI models are helping security researchers, and attackers, uncover serious flaws in software the world has relied on for decades: a 30-year-old bug in the image library inside countless websites and apps, 16-year-old flaws in server firmware and Wi-Fi routers, and an 18-year-old flaw in software that runs a large share of the World Wide Web. October brought so many serious disclosures that the term "Black October" was coined.

An Anthropic security leader warns this flood of AI-uncovered vulnerabilities could last 18 months or more. Owners and executives, IT professionals, MSPs, and technology vendors must work together to protect our businesses and the greater U.S. economy. Every action taken on security essentials makes us all harder to attack, and companies falling behind become the weak link for their customers, vendors, and community.

Protection doesn't necessarily require expensive new tools. It starts with awareness and getting the most from the technology you already own.

Linus Malefors

Managing Director, Coeus Consulting

The Omen

Signals of Change

Black October: The Bugs Were Already There



AI is finding vulnerabilities faster than ever, and the pace is still climbing.

PHP2Shell, October's most disruptive vulnerability, was found by researchers using AI, and Anthropic's own AI-assisted research has uncovered flaws hidden for 27 years in OpenBSD and 16 years in FFmpeg. Each new generation of AI models finds more vulnerabilities, faster, for defenders and attackers alike.

Security leaders expect the pace to keep accelerating. Anthropic's Deputy CISO says conditions will likely get worse before they get better.

Coeus Perspective: Decades of software contain an enormous backlog of undiscovered vulnerabilities, and AI is now finding them faster than vendors can fix them.

Coeus Insight: Don't count on older or less widely adopted systems being safer: inventory them, and replace or isolate any no longer supported by the manufacturer, because new vulnerabilities in those older systems will never be fixed.

Sources: Wiz: PHP2Shell research | Anthropic: Mythos Preview research | Jason Clinton remarks

The Proven Path

Strategies for Today

Not for AI. For the Basics.

On October 22, Anthropic Deputy CISO Jason D. Clinton urged cybersecurity leaders to ask for support "not for AI, for the basics." Many businesses already own capable security tools, including protections built into Microsoft 365 and Windows, that are only partly implemented. Before buying anything new, make sure these fundamentals are fully in place:



- **Stay supported and updated.** Keep firmware, servers, firewalls, operating systems, and applications under vendor support and patched. Plan replacements before support ends.
- **Optimize existing tools.** Turn on and tune the protections you already pay for, such as multifactor authentication, Microsoft Defender, disk encryption, and automatic updates.

- **Reduce unnecessary exposure.** Remove unused applications and services, close unneeded network ports, restrict nonbusiness websites and traffic, and change default passwords.
- **Give access only where needed.** Enforce least privilege: a clerk doesn't need access to every shared file, and a camera system vendor doesn't need full network access.
- **Back up and plan ahead.** Make sure critical data is backed up, test the backups, and plan for outages.
- **Adopt a framework.** Even if you aren't in a compliance-driven industry, a framework such as the CIS Critical Security Controls turns good intentions into a repeatable process, with clear owners and tracked progress.

Coeus Perspective: The basics rarely make headlines, but they decide whether a new vulnerability becomes a routine fix or a crisis. Reducing access and unused services also limits how far an attacker can get.

Coeus Insight: Put named owners, documented routines, and tested results behind the basics before adding more tools.

Sources: Jason Clinton remarks | CIS Controls IG1

The Horizon

Preparing for Tomorrow

What Happens When Your Cloud Software Goes Down?



The coming wave of vulnerabilities will impact cloud and other application availability, whether a vendor shuts down to install emergency fixes, as many did for PHP2Shell, or recovers from an attack, as staffing-software provider Bullhorn did in October. When Microsoft 365 or the ERP, CRM, or industry software you run on goes down, your business goes down with it unless you planned ahead.

A continuity plan decides in advance what your business will do when a critical system goes down. Start with four questions:

- **Which applications matter most?** List your most critical applications and how long the business can operate without each.
- **Can you still reach people?** Keep customer, vendor, and employee contact lists somewhere other than the application that might be down, and agree on a backup way to communicate.
- **Can you keep working?** Decide how scheduling, billing, and other daily work will be handled manually for 48 hours or more, and who does what.
- **Do you have your own copy of your data?** Cloud vendors protect their service, not your access to your data during an outage. Use independent backups or regular exports for your most critical applications.

Coeus Perspective: Cloud uptime is your vendor's job. Business uptime is yours.

Coeus Insight: Test your continuity plan before your vendor's next emergency patch tests it for you.

Sources: Coeus: PHP2Shell | Bullhorn status | Ready.gov: business continuity planning

A Conversation Worth Having

Getting ahead of the vulnerabilities AI has yet to uncover starts with one conversation. Sit down with your IT department, MSP, or trusted technology advisor and ask:

- What are we running that is no longer supported?
- Which of the security basics are not fully in place?
- How would we operate if a critical application went down for 48 hours or more?

If you don't have anyone to ask, Coeus will gladly talk through your concerns with you.

The Agora

Meet Coeus

Meet Us This December

DEC 9-10 | PHOENIX BUILD EXPO

Phoenix Convention Center. Coeus will exhibit, discussing technology that keeps construction projects running.

DEC 9 | MSP TITANS OF THE INDUSTRY AWARDS GALA

The Beverly Hilton, Beverly Hills. Coeus will attend as an MSP Titans of the Industry finalist for the second year running.

Event: Phoenix Build Expo | Practical resource: CIS Controls Implementation Group 1

About Coeus Consulting

Coeus Consulting helps Southwest businesses reduce technology disruption through practical IT management, cybersecurity, cloud, and planning.

Have a technology problem or question you'd like to discuss? Book a 15-Minute Call

COEUS

Managed IT • Cybersecurity • Cloud • Compliance