

The Coeus Chronicle

INSIGHT WITH FORESIGHT

VOLUME: 1 ISSUE: 6

JUNE 2026

PUBLISHED BY COEUS CONSULTING

TRUSTED IT, CYBERSECURITY, AND CLOUD ADVISORS



Welcome to the Coeus Chronicle, your monthly briefing from **Coeus Consulting**.

We bring clarity to the technology decisions shaping modern businesses.

The Omen

Signals of Change

The Firewall Became the Target



In June, security researchers disclosed a widespread credential-harvesting campaign targeting internet-facing Fortinet firewalls and VPN gateways. Attackers were using previously exposed credentials and automated brute-force techniques to gain access to devices that often sit at the very edge of a company's network. Fortinet said its investigation did not identify a new vulnerability behind the campaign, making the underlying lesson even more important: security appliances themselves can become valuable targets when privileged credentials or management interfaces are exposed.

Coeus Perspective: A firewall protects the network, but it is also a highly privileged system with access to traffic, remote connectivity, and security configuration. Patching remains essential, but strong administrative authentication, restricted management access, credential hygiene, and monitoring matter just as much.

Coeus Insight: Treat every internet-facing security appliance as a privileged system. Limit who and what can reach its management interface, require strong authentication, and rotate credentials whenever there is reason to believe they may have been exposed.

Source: Reuters, Fortinet says credential-harvesting campaign is targeting its firewalls and VPN devices, June 17, 2026.

The Proven Path

Strategies for Today

AI Is Giving Small Teams More Capacity

The early business value of AI is looking considerably more practical than many of the predictions surrounding it. The U.S. Chamber of Commerce Foundation's inaugural Main Street AI Monitor, released June 17, found that half of small-business workers were already using AI at work. Only 6% said they primarily used it to automate workflows with minimal human involvement. Instead, most were using AI for drafting, summarizing, brainstorming, recurring tasks, and other productivity work. Among users saving time with AI, 59% said they reinvested those savings into doing more work or producing higher-quality output.

Coeus Perspective: For most SMBs, the immediate opportunity is not replacing entire jobs or processes. It is increasing the capacity of the people already doing the work by reducing repetitive research, writing, analysis, and administrative effort.

Coeus Insight: Measure AI by what employees accomplish with the time it gives back. A workflow that saves two hours is most valuable when the business intentionally decides where those two hours should be reinvested.

Source: U.S. Chamber of Commerce Foundation and Ipsos, Main Street AI Monitor, June 17, 2026.





The Horizon

Preparing for Tomorrow

Passwords Are Becoming the Backup Plan

Passwordless authentication has spent years being described as the future. Microsoft's June Entra updates suggest that future is moving much closer to normal business use. Microsoft made phishing-resistant Entra passkeys on Windows generally available, allowing users to authenticate to cloud resources with a passkey stored securely in Windows Hello and verified through a PIN, fingerprint, or facial recognition. Microsoft is also expanding policies and management capabilities intended to make passkeys easier to deploy at scale.

Coeus Perspective: Traditional passwords, SMS codes, and other shared-secret authentication methods remain attractive targets because attackers can steal, phish, or intercept them. Passkeys change the model by replacing reusable secrets with cryptographic credentials tied to the user and device. The long-term identity question is shifting from "How do we make passwords stronger?" to "Where can we remove passwords altogether?" Businesses that begin adopting phishing-resistant authentication now can improve security while avoiding a rushed transition later as major platforms continue reducing their dependence on traditional credentials.

Coeus Insight: Start identifying applications and users that still depend heavily on passwords or phishable MFA. The transition does not need to happen overnight, but organizations should begin planning for phishing-resistant authentication to become the standard rather than the exception.

Source: Microsoft, What's New in Microsoft Entra: June 2026.

The Agora

Meet Coeus

Cyber Insurance and the Healthcare Sector

New Webinar Replay | Available This Month

Healthcare organizations face a difficult combination of high cyber risk, regulatory obligations, and increasingly detailed cyber-insurance requirements. In this on-demand webinar, Coeus Consulting and Kaseya examine what healthcare organizations should understand before their next insurance renewal, including how to assess cyber exposure, identify HIPAA gaps that may affect coverage, review policy exclusions, and prepare for the actions insurers expect during the first hours of an incident.

Watch the Webinar Replay



About Coeus Consulting

Coeus Consulting helps growing businesses make technology more secure, reliable, and predictable. From our Phoenix headquarters, we bring enterprise-level discipline to managed IT, cybersecurity, cloud, and compliance for businesses across the Southwest.

Book a 15-Minute Call

COEUS