GUARDIENT® | POWERED BY USX CYBER®

PRODUCT UPDATE

VOL. 01 — ISSUE 02 • MAY 2026

One month ago, **Guardient v3.0** went live and replaced the prior platform. In this issue we cover what has shipped since launch — a major **Box** integration, automated **CMMC Level 2** evidence generation, and redesigned security reporting — plus two advisories worth a moment of your team's attention.

PLATFORM UPDATES

New Features & Enhancements

NEW

Guardient Now Monitors Box

Guardient now provides real-time monitoring of Box cloud storage activity — file access, uploads, previews, and sharing events — alongside your endpoint, network, and cloud telemetry. For contractors who rely on Box for day-to-day collaboration but lack native logging visibility, this closes a real compliance blind spot.

More than a feature, the Box integration reflects how we keep building toward being the premier solution for CMMC: Guardient works with the environment you have already purchased and built, bringing your existing tools into compliance. **We are not an enclave solution.**

As part of the integration, GUARDIENT® continuously produces audit evidence from security operations, reducing the manual collection work required for traditional audit preparation. Built by our CISO, Doug Gray.

NEW

140 CMMC Level 2 Artifacts, Automated

Building on the Policy & SSP Builder introduced last issue, Guardient now automatically generates 140 of the technical artifacts a CMMC Level 2 assessment requires.

Answer a few guided questions and Guardient assembles the supporting documentation — mapped to the CMMC framework — that assessors expect to see. The result is a dramatic reduction in the manual preparation that has historically consumed assessment timelines, freeing your team to focus on remediation rather than paperwork.

ENHANCED

New & Improved Security Reports

Reporting in Guardient has been redesigned for clarity. Cleaner formatting, refined layouts, and more digestible summaries make it easier to communicate security posture to both technical teams and leadership.

The same depth of detail, presented in a format that is faster to read, easier to share, and ready to put in front of stakeholders.

MILESTONE

Guardient v3.0 — One Month Live

A month on from the May 1 cutover, v3.0 is fully in production. The unified single-pane experience — case management, the integrated GRC platform, and Zero Trust capabilities under one roof — has tightened day-to-day workflows for analysts and administrators alike.

Thank you to every client who came along through the transition. The integrations and improvements in this issue are a sign of the cadence to come.

SECURITY ADVISORIES

Advisories & Action Items

MEDIUM SEVERITY

Meta's AI Support Bot Abused to Hijack Instagram Accounts

On May 31, instructions circulated on Telegram showing how to trick Meta's AI support assistant into linking an attacker-controlled email to an account and triggering a password reset — with no breach of Meta's back-end systems required. Attackers used the technique to briefly deface high-profile Instagram accounts, including the dormant Obama White House account, before Meta pushed an emergency patch.

The lesson extends well beyond Instagram. As more platforms hand sensitive account-recovery workflows to AI chatbots, those bots become a social-engineering target in the same way human support agents always have been — equally eager to help, and equally vulnerable to persuasion. **Action required:** enforce phishing-resistant MFA (passkeys or hardware security keys) on all business social and SaaS accounts. Notably, attackers reported the exploit failed against any account with MFA enabled — even an SMS code would likely have blocked it.

→ VIEW FULL ADVISORY (KREBSONSECURITY)

HIGH SEVERITY

Secrets in Source Control — GovCloud Keys Leaked on GitHub

Through mid-May, a public GitHub repository maintained by a government contractor exposed plaintext credentials, cloud keys, and tokens for highly privileged AWS GovCloud accounts and numerous internal systems. The repository had been used like a personal folder to sync files between work and home machines, and the owner had deliberately disabled GitHub's built-in secret-scanning protection.

Researchers confirmed the exposed keys authenticated to GovCloud at a high privilege level — and that they remained valid for roughly 48 hours after the repository was taken offline. **Action required:** never commit credentials, keys, or tokens to any repository; keep secret scanning and push protection enabled; rotate any exposed secret immediately and assume it is compromised; and avoid predictable passwords built from a platform name and the current year.

→ VIEW FULL ADVISORY (KREBSONSECURITY)

How Guardient helps: *this is exactly the class of activity Guardient's GitHub and GitLab log ingestion — launched last issue — is built to surface: unauthorized repository changes, secret exposure, and suspicious access, in real time rather than after the fact.*

Questions or Need Support?

Our team is available to help you understand these updates and ensure your environment is fully protected.

CONTACT YOUR GUARDIENT TEAM →

GUARDIENT®

DYNAMIC DEFENSE — POWERED BY USX CYBER

Portal Login Support Documentation Unsubscribe