



What small and mid-size business leaders need to know about cyber risk this week, and what to do about it.

Provided by Major Business Solutions LLC

HEADLINE THREAT

ACTIVE ADVISORY · #STOPRANSOMWARE

CISA and FBI warn SafePay ransomware has hit 600+ organizations, breaking in through VPNs, firewalls and stolen passwords

On October 20, CISA, the FBI, the U.S. Secret Service and UK and German partners issued joint advisory **AA26-293A** on SafePay, now one of the most active ransomware groups. It has breached at least 600 organizations since August 2024. That count is probably low, because the group's leak site lists only victims who did not pay. SafePay gets in mainly through **stolen or brute-forced passwords, phished accounts**, and **known flaws in internet-facing VPNs and firewalls**, using automated scripts. The flaws it uses include older Cisco ASA/FTD bugs that are already on CISA's Known Exploited Vulnerabilities list. Once inside, it steals data before encrypting it (double extortion), deletes shadow copies, and resets network storage (NAS) devices that hold backups so victims cannot recover.

The same pattern showed up elsewhere this week. Palo Alto's Unit 42 reported that the Qilin and Inc ransomware groups are exploiting a GlobalProtect VPN flaw that was patched in May, which means some businesses still have not applied that fix.

Why it matters for you

The way into most businesses right now is the remote-access gear: the VPN or firewall at the network edge and the passwords that unlock it. These devices are often set up once and then forgotten. In Verizon's 2026 DBIR, exploiting a vulnerability overtook stolen credentials as the most common way attackers got in. SafePay also goes after backups on purpose, so a NAS on the same network does not count as a recovery plan.

PATCH PRIORITY

Ransomware-exploited **Palo Alto PAN-OS GlobalProtect, CVE-2026-0257:** An authentication bypass that gives attackers VPN access. Qilin, Inc and Settra are exploiting it. Update PAN-OS, then *end all active GlobalProtect sessions* and check for sessions you don't recognize. Patching does not remove access an attacker already has.

KEV **SafePay** **Cisco ASA / Firepower (FTD), CVE-2020-3259 and CVE-2023-20269:** Named in reporting on the SafePay advisory. If you run a Cisco ASA or FTD for VPN, confirm it is on a current release and that MFA is required for VPN logins.

KEV · Oct 16 **BeyondTrust Remote Support, CVE-2026-102764:** A critical authentication bypass, exploited since late August. Cloud customers were patched October 8. Self-hosted versions 26.2.3 and earlier must be patched by hand, and any appliance that was exposed should be treated as possibly compromised until it has been reviewed.

KEV · Oct 23 **Collabora Online built-in CODE server for Nextcloud, CVE-2026-110447:** Attackers are using it to plant web shells on Nextcloud servers. Update the *richdocumentscode* app to 26.4.303 or later, or remove it. The vendor says disabling the app is not enough.

Vendor incident **ConnectWise Cloud Backup (formerly SkyKick):** A stolen app credential gave attackers access to at least 162 Microsoft 365 tenants, and Microsoft has called it a supply-chain attack. The service was suspended. Disable the apps (don't delete them) and audit app credentials added since October 13.

Patch now **PHP2Shell, CVE-2026-109618 and CVE-2026-109619:** Critical PHP flaws that let attackers run code remotely without logging in. Update to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35. Palo Alto says the PAN-OS management web interface is affected and some fixes are not due until Oct 27–30, so limit that interface to internal addresses.

Also added to KEV this week: four Plex Media Server flaws ("Plex2Shell", fixed in 1.43.3.10861), Siemens Software Center, SiteGuard Server Edition and Arista VeloCloud Orchestrator.

BY THE NUMBERS

600+

organizations breached
by SafePay since Aug
2024

CISA/FBI AA26-293A, Oct
2026

31%

of breaches began with
an exploited vulnerability,
now the #1 way in

Verizon 2026 DBIR

48%

of breaches involved a
third party, up 60% year
over year

Verizon 2026 DBIR

43 days

median time to fully fix
critical KEV flaws

Verizon 2026 DBIR

THREE ACTIONS THIS WEEK

- 1. Patch and check your edge devices today.** List every VPN, firewall and remote-support tool that faces the internet (Palo Alto GlobalProtect, Cisco ASA/FTD, Fortinet, BeyondTrust, and others) and confirm each one is on a current release. For GlobalProtect, end active sessions after you patch. Restrict management interfaces to internal addresses.
- 2. Require MFA on all remote access and remove stale accounts.** SafePay's main ways in are stolen, brute-forced and phished passwords. Make sure every VPN and remote-access login requires MFA, disable unused and former-employee accounts, and turn on lockout or alerts for repeated failed logins.

3. **Ask your MSP or IT provider two questions in writing.** (1) "Do any of our Microsoft 365 tenants use ConnectWise Cloud Backup or SkyKick, and have you disabled those apps and audited app credentials since Oct 13?" (2) "Is at least one copy of our backups offline or immutable, and when did we last test a restore?"

How MajorCompliance can help

- **ConnectWise Cloud Backup incident:** MajorCompliance tracks each vendor's compliance evidence (such as SOC 2 and ISO 27001), checks uploaded documents against the vendor's claims, alerts before that evidence expires, and keeps a tamper-evident log of what each vendor submitted.
- **New KEV entries (BeyondTrust, Collabora) and PHP2Shell:** MajorCompliance checks each vendor's software bill of materials against the OSV.dev and NVD databases, and its Vulnerabilities page shows which affected CVEs are on CISA's KEV list across all vendors at once.
- **Following up with vendors on these flaws:** MajorCompliance drafts the outreach email and gives the vendor a secure portal to respond. A vendor that says it is not affected can submit a VEX statement with evidence, and that statement counts only after your own staff confirm it.

MajorCompliance is a vendor-risk platform from Major Business Solutions LLC.

 Provided by Major Business Solutions LLC

Sources

1. [CISA: #StopRansomware: SafePay Ransomware \(AA26-293A\)](#)
2. [BleepingComputer: CISA: SafePay ransomware hit over 600 critical infrastructure orgs \(Oct 21, 2026\)](#)
3. [Cybersecurity Dive: FBI, CISA warn that SafePay ransomware poses threat to critical infrastructure \(Oct 21, 2026\)](#)
4. [Help Net Security: Ransomware groups exploit Palo Alto GlobalProtect flaw \(Oct 21, 2026\)](#)
5. [BleepingComputer: BeyondTrust patches zero-day exploited in attacks since August \(Oct 16, 2026\)](#)
6. [BleepingComputer: Hackers exploit Collabora RCE flaw to backdoor Nextcloud servers \(Oct 15, 2026\)](#)
7. [The Hacker News: CISA flags two actively exploited critical flaws in Collabora Online and Arista VeloCloud](#)
8. [The Hacker News: CISA orders federal agencies to patch exploited Plex2Shell, Siemens and SiteGuard flaws \(Oct 21, 2026\)](#)
9. [BleepingComputer: Hackers breach Microsoft 365 tenants via ConnectWise supply-chain attack \(Oct 17, 2026\)](#)
10. [Help Net Security: ConnectWise Cloud Backup suspended after security incident \(Oct 19, 2026\)](#)
11. [Help Net Security: PHP2Shell status at Palo Alto, Fortinet and Cisco \(Oct 22, 2026\)](#)
12. [CISA: CISA Adds Six Known Exploited Vulnerabilities to Catalog \(Oct 20, 2026\)](#)
13. [CISA: Known Exploited Vulnerabilities Catalog](#)
14. [Verizon: 2026 Data Breach Investigations Report, Executive Summary \(2026\)](#)

This briefing summarizes public reporting as of October 26, 2026. Always verify advisories, affected versions and fixes directly with CISA (cisa.gov) and your vendors before acting.