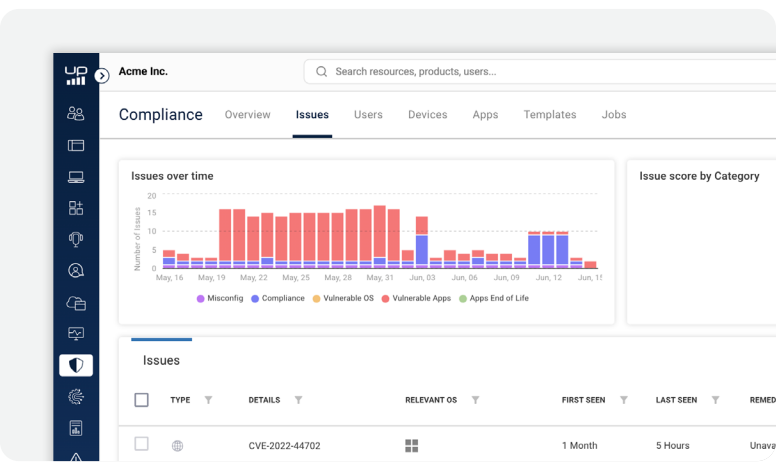
SOLUTION BRIEF

ControlUp for Compliance

Automate Endpoint Compliance, Close Security Gaps, and Enforce Policy Without Slowing IT Down

ControlUp for Compliance goes beyond point-in-time vulnerability scans and manual patch workflows by giving IT and security teams a continuous, automated compliance engine built directly into the ControlUp platform.



Instead of relying on fragmented tools or spreadsheet-driven audit processes, CU4C scans every managed endpoint against a comprehensive catalog of CVEs, misconfigurations, missing patches, and security control gaps, then remediates issues automatically before they become incidents.

With ControlUp for Compliance, teams don't just detect risk, they eliminate it. Template-driven automation handles the full lifecycle from scan to remediation to verification, with split download and install schedules that protect employee productivity and configurable snooze controls that give users agency without sacrificing urgency. Custom Issues and Custom Remediations extend coverage to organizational-specific requirements that no out-of-the-box tool can anticipate.

ControlUp for Compliance transforms endpoint security from a reactive, audit-driven exercise into a proactive, automated, and continuously enforced capability.

BENEFITS OF CONTROLUP FOR COMPLIANCE

ControlUp for Compliance delivers continuous endpoint risk visibility through a live security score for every device, issue, and application across the fleet, updated automatically after every scan and remediation.

Reduce security exposure at scale by automatically detecting CVEs, misconfigurations, missing patches, and inactive security controls, then remediating them without requiring manual IT intervention.

Eliminate compliance overhead with wizard-driven template setup, automated scheduling, and built-in verification scans that confirm every fix landed before closing the issue.

Extend compliance to organizational-specific risks through Custom Issues and Custom Remediations that bring your own scan and remediation scripts under the same automated framework as built-in checks.

Template-Driven Compliance Automation	IT teams configure compliance Templates that define which devices to target, which issues to scan for, and whether to remediate automatically or flag for manual review, with granular scheduling to minimize disruption.	Wizard-driven setup deployable in minutes with no scripting required
		Flexible scan and remediation schedules split by day, time window, and device local time
		Auto-remediation with configurable severity thresholds for tiered response
CVE & Vulnerability Detection	CU4C maps installed application versions against the Mitre NVD CVE database, synced multiple times per day, and surfaces CVSS 2.0 and 3.0 scores per device to help IT prioritize what to fix first.	Continuous CVE detection across 700+ tracked applications and OS components
		CVSS severity scoring with Critical, High, Medium, and Low risk classification
		CVEs reported even when no patch is available, for full risk visibility
Application & OS Patch Management	CU4C silently downloads and installs missing application patches and Microsoft KB updates through a CDN reverse proxy, with split schedules that pre-stage patches during business hours and install overnight.	700+ application catalog including Chrome, Zoom, Slack, Adobe Reader, and more
		Silent patch installation with no user interruption or manual approval required
		Split download and install schedules to separate bandwidth impact from user disruption
Misconfiguration & Security Controls	CU4C checks OS-level settings against security benchmarks and verifies that required security tools including EDR, DLP, VPN, PAM, and UEM agents are installed and actively running on every device.	Checks cover firewall state, UAC, SMB signing, Windows Defender, password policy, and more
		Detects missing or inactive agents from CrowdStrike, SentinelOne, Zscaler, Intune, and 20+ other vendors
		Security validation checks simulate real threats to confirm AV and SWG response
Device Security Scoring	Every device receives a continuous security score on a 0 to 10 scale based on the number and severity of open issues, updated automatically after each verified remediation to reflect the true current risk posture.	Organization, device, application, and user-level scores in a single dashboard
		Score recalculated after each verification scan confirms a fix was successfully applied
		Trend views and top-issue prioritization matrix to guide remediation focus
Custom Issues & Remediations	IT and security teams can extend CU4C coverage with their own scan scripts and remediation scripts, bringing organizational-specific checks under the same automated scan, detect, remediate, and verify pipeline as built-in issues.	Custom scan scripts with configurable expected outputs for pass/fail detection
		Custom remediation scripts with automatic verification to confirm the fix landed
		Supports interim workarounds for CVEs with no available vendor patch

ControlUp is the AI company for IT operations that keeps the digital workplace running. Leading DEX capabilities and agentic AI come together to see, detect, ask, and remediate issues before they reach employees, enabling Autonomous Endpoint Management (AEM). IT leads, employees thrive, and work flows.

Get a Demo Start a Free Trial

controlup.com