DATA SHEET

ControlUp for Compliance

The ControlUp for Compliance solution empowers IT and cybersecurity teams to collaborate effectively, providing the tools and visibility needed to safeguard your enterprise

Organizations face ever-evolving security challenges, from network vulnerabilities and out-of-compliance devices to weak configurations.

ControlUp for Compliance empowers IT and cybersecurity teams to collaborate effectively, providing the tools and visibility needed to safeguard your enterprise—across all devices, anywhere in the world.

>10M

Devices infected with data-stealing malware in 2023

29,000+

Published vulnerabilities in 2022

$4.45M

The global average cost of a breach in 2023

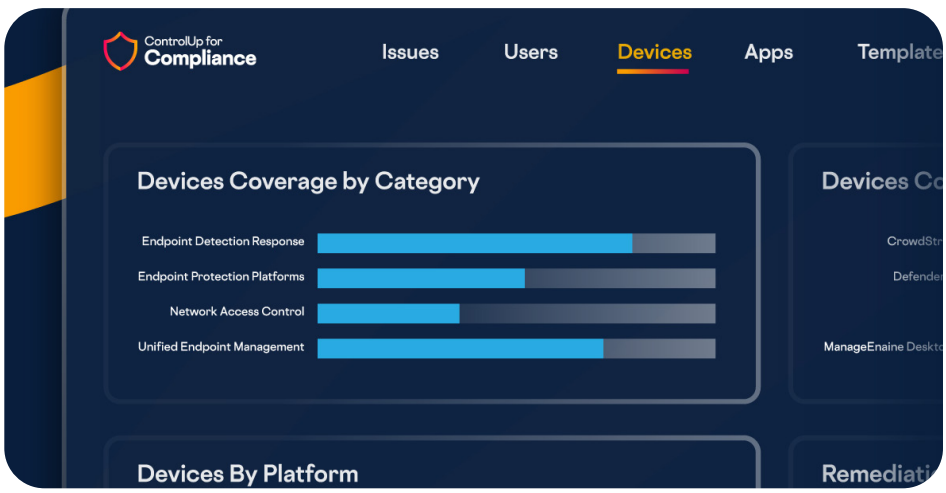
Safeguarding Your Business Is Everyone's Business

Cybersecurity teams often rely on desktop administrators to address various security issues, such as device integrity, vulnerability risks, patch management, and compliance. But these tasks can quickly become overwhelming without the right tools, leading to lapses in compliance and increased exposure to risks. ControlUp for Compliance bridges this gap, equipping IT teams with comprehensive security solutions to maintain compliance and protect the organization.

Stay Ahead of Security Threats—Automatically

ControlUp for Compliance proactively identifies, prioritizes, and addresses security concerns across your digital ecosystem.

- **Security Insights:** Access detailed overviews of security issues related to users, devices, and applications across locations, severity, and priority.
- **Vulnerability Management:** Keep operating systems and applications up-to-date and secure by scanning and remediating vulnerabilities.
- **User Risk Monitoring:** Capture SaaS application logins to evaluate user risk and minimize exposure.
- **Endpoint Compliance:** Audit security settings and ensuring endpoint security software compliance.
- **Intelligent Automation:** Leverage built-in and customizable scans, automated remediation workflows, and detailed templates to maintain a secure environment 24/7.



User Risk Analytics Improve your digital workplace risk assessment and reporting by providing insights into what SaaS applications your employees are using.	• **Application Login Risk:** For each SaaS application login, determine the user risk based on the authentication type used, if the login came from a managed or unmanaged device, and the certification strength of the SaaS application. Support for SaaS application logins through native Entra ID and Okta integrations, or browser extension for email-based logins. • **Shadow IT Insights:** Uncover non-IT managed SaaS applications by tracking where corporate credentials are being use and evaluate and reduce risk. • **User Risk Score:** Combine data from SaaS logins to calculate a per user risk score to quickly understand where additional mitigation is needed and improve security posture.
OS Patch and Vulnerability Management Ensure employees' productivity is not hindered by poor-performing applications through comprehensive data collection.	• **OS Patch and Vulnerability Management:** With over 2,000 vulnerabilities discovered last year, ControlUp for Compliance automatically scans and remediates OS vulnerabilities. • **OS and Device Risk Details:** Quickly determine the severity of the exposure to your environment with OS versions and patch level, remediation status reporting.
Drift Prevention Verify that computers remain compliant with comprehensive audits of account permissions, device hardening measures, and web security policies, coupled with detailed reports on the status and impact of these configurations.	• **Scan and Remediate Misconfigurations:** Ensure corporate compliance and consistency by scanning and remediating operating system settings and configurations across your Windows devices. • **Versatile Security Settings:** Audit for Windows account privileges and permissions, check for device hardening settings, BitLocker configuration, and test for web protection and block policies. • **Detailed Insights:** Classification of misconfiguration based on severity, remediation status, descriptions of misconfiguration, devices affected, and when the misconfiguration was first discovered.
Security Software Asset Management Manage and track the version, installation date, and active status of security software, including anti-virus and anti-malware.	• **Security Control Management:** Scan and report issues to determine if endpoint security software is installed on your devices and remediate to bring devices into compliance. • **Security Control Inventory:** Report on a wide range of cybersecurity tool vendors and their endpoint security products, including antivirus, antimalware, VPN, EDR, XDR, DLP, and UEM software.

Automated Security Scanning and Remediation Automatically resolve security issues, eliminating the need for manual intervention.	• **Built-In Catalog:** Scan and remediate thousands of vulnerabilities, misconfigurations, compliance issues, and patches. • **Automated Scan and Remediation:** Create scan and remediation templates to determine how often devices get scanned and auto remediated. • **Assigned Devices:** Assign a scanning and remediation template to all devices, or a subset of devices with device tags, device groups, operating systems or Entra ID groups. • **Scanning Scope:** Define the scanning criteria such as misconfigurations, compliance, vulnerabilities, application, and operating system patches. • **Remediation Actions:** Determine if remediations should be automatically remediated or what specific remediations should happen. • **Scheduling:** Plan scanning and remediations, auto-restarting, and user notifications to minimize disruptions to employees. • **Reboot and Notification:** Automatically reboot endpoints and notify users with customizable messages.
Custom Scanning and Remediation Actions Create custom scans and remediations for any security issue in your organization.	• **Custom Actions:** Create custom scans with PowerShell scripts to detect and remediate issues not included in the catalog or unique to your organization. • **Custom Remediation For Catalog Scans:** Create custom remediation actions for catalog scans that have no built-in remediations.
Security Dashboards Analyze user behavior, device status, and application updates to gain insights into your users, devices, and applications, efficiently addressing security concerns by examining key issues, locations, and priorities.	• **Overview:** Gain a high-level understanding of your users, devices, and applications by top 10 issues, locations, severity, and prioritization. • **Issues:** See security problems over time and sort issues by severity to see what should be remediated first. • **Users:** User-based risk scores and dashboard provide actionable insights into the individual risks associate with each employee by considering factors such as device compliance and, authentication methods users are using and a sortable chart to find users with the low security risk scores. • **Devices:** View security issues from a device perspective such as severity score, remediation status, and a sortable list of security controls, security score, and issues. • **Applications:** Know what applications and operating systems have CVEs that need to be remediated and SaaS applications being accessed by certification type and strength.

ControlUp's platform unburdens IT teams so they can proactively deliver a superior digital employee experience powered by true real-time visibility, actionable AI-driven insights, and automated remediation—across any desktop, any application, anywhere.

Get a Demo Start a Free Trial

controlup.com