CASE STUDY

compucom
Technology Driven.
People Powered.

Endpoint Compliance Made Easy with Our FLO Framework:

65% Fewer Non-Compliant Devices in 60 Days

SNAPSHOT

Non-compliant workplace devices represent a security risk and impact productivity. By leveraging our Full Lifecycle Observability Framework, we cut through the noise to understand the true scope of compliance issues an IT team was facing. We then worked with them to devise an effective, data-driven strategy to achieve their compliance goals.

Challenge: Turn Down the Noise and Tune in to Real Compliance Issues

When the FLO Framework was first integrated with a company's workplace technology data sources, approximately 75% of devices reported non-compliance with established workstation policies based on Microsoft standards and best practices.

This was concerning not only from a security risk standpoint but also resulted in operational disruptions. Devices deemed non-compliant were restricted from VPN connections, directly impacting user productivity.

While the low endpoint compliance raised alarms about possible problems with patch management, feature updates, and settings for disk encryption, secure boot, antivirus software, and firewall configurations, we suspected that many of these non-compliant reports stemmed from data and reporting errors. To get a more accurate picture of device health, we needed to first work on increasing data integrity.

Action: Establish Data Integrity First, Then Strategize Troubleshooting Efforts

Inaccurate information clouded the IT team's understanding of the extent of actual compliance issues. We needed to dramatically improve data integrity so that technicians could zero in on real compliance issues and move quickly to fix them.

To tackle this issue, we leveraged insights from our comprehensive FLO Framework Dashboard to pinpoint the most affected non-compliant policy items. This strategic approach enabled the team to prioritize actions based on severity of non-compliance.

Within the FLO Framework Dashboard, team technicians could drill down to endpoint policies and examine individual devices and their settings, enabling targeted troubleshooting and faster resolutions, including automating processes.

Windows 11 Migration Progress at a Glance: With the FLO Dashboard Drilldowns, CIOs and their IT teams can quickly view their fleet's Windows 11 migration status and identify locations lagging in the upgrade. They can access device details for individual machines, facilitating efficient investigation and troubleshooting.

Key actions included:

- **Targeting Low-Hanging Fruit:** For hundreds of devices, the team enabled the safe boot setting and addressed machines that had not been rebooted, ensuring updates were refreshed. These simple actions had a significant impact on compliance standing.
- **Addressing Common Issues:** The team rolled out updates to address frequent faults like memory leaks. Wherever possible, identified common issues were resolved through self-heal automation.
- **Adjusting the Grace Period:** The IT team reviewed and adjusted the grace period for endpoints, allowing a five-day window before non-compliance status was triggered. This adjustment helped reduce false positives and provided a buffer for remediation.
- **Automated Proactive Remediation:** An automated system was established to create ServiceNow tickets for devices that remained in the grace period for more than three days. This ensured timely remediation before devices transitioned to non-compliance.
- **Filtering and Identifying Devices:** Devices that had not reported to Intune for over 30 days, such as those shelved or for employees on long-term leave, were identified and filtered out. This helped the team focus on devices requiring attention, streamlining the remediation process.

Results: Enhanced Data Integrity and Compliance

Within 60 days, our team's proactive measures led to a remarkable **reduction of approximately 65%** in non-compliant devices There was also a **32% reduction in endpoints** classified as in poor health.

The FLO Framework Dashboard provided a unified view and insightful analytics, allowing the IT team to remediate non-compliant devices more efficiently without the hassle of juggling multiple tools and reports. The automated ticket creation for potential non-compliant devices also ensured timely intervention, further strengthening their security posture.

This achievement enhanced the compliance of the company's IT infrastructure, boosted overall security, and restored lost productivity.

Improved endpoint troubleshooting and compliance is just one of the many ways our FLO Framework helps us shift our customers towards proactive IT management. By providing CIOs with a holistic view of all aspects of their IT environment, including workplace technology, sourcing, infrastructure, and employee experience, we empower them to focus their IT resources on optimizing what matters most to their business.

Proactive IT Management for Our Customers
Helping IT Teams Pinpoint Issues and Troubleshoot Faster

We're continuing to work with the IT team to improve the company's compliance, focusing on helping them:

01

Achieve Over 95% Compliance: We are on track to exceed the target of 95% compliance for endpoints and are working on their server compliance. Our FLO Framework will help us reach our customer's goals faster.

02

Identify Compliance Trends: As we enhance our FLO Framework, we'll integrate real-time data from SysTrack's monitoring platform as a data set. These snapshots will help to identify compliance trends and improve proactive endpoint management.

03

Increase Troubleshooting Efficiency: The continued improvements in endpoint data integrity will ensure compliance monitoring is more accurate and reliable, and the IT team can troubleshoot efficiently, maintaining high rates of compliance.

compucom
Technology Driven.
People Powered.

Learn more about Compucom and how we source, integrate, and support your technology needs at compucom.com