

Security and Compliance

Swimage Monthly Newsletter



Swimage Compliance Enforcer Has Arrived!

For decades, Swimage has been trusted by many organizations for PC provisioning, upgrades, replacements, and full system recovery. Based on customer demand, Swimage's patented automation and intelligence engines have been broadened to include PC health monitoring and zero trust security compliance enforcement.

What does this mean for you? Simply put, Swimage Compliance Enforcer, combined with Swimage automation technology, ensures that all of your systems remain healthy, secure, and compliant. Through easy-to-configure rules, you can monitor, alert, and remediate any PC issue automatically and rapidly. Even under the most extreme conditions, Swimage alerts, secures, and resolves PC problems within minutes, all without tech support and even when the PC is remote or offline.

For example, if malware is detected on a PC, Swimage can be triggered to take immediate action. First, Swimage locks the PC down and creates an alert. Second, Swimage automatically remediates the problem. Remediation can include anything from removing malware to a complete system rebuild. In the case of a broad malware outbreak, Swimage quickly repairs all systems simultaneously, making an essential solution for disaster recovery to ensure business continuity.

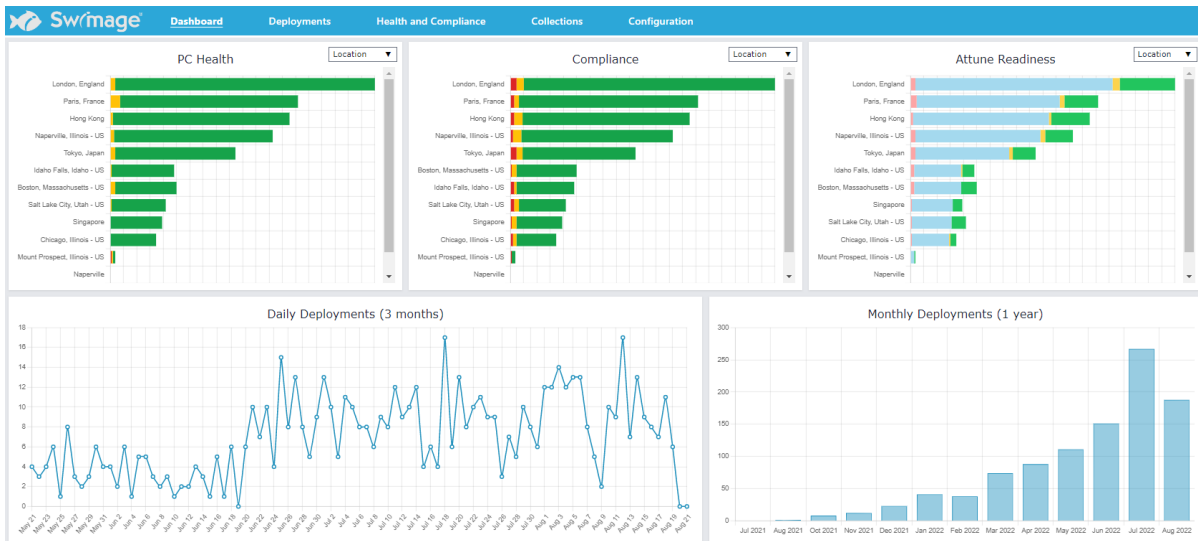
Swimage's interactive and customizable dashboard provides a bird's-eye view of the health, compliance, and deployment status of all your PCs.

IN THIS ISSUE

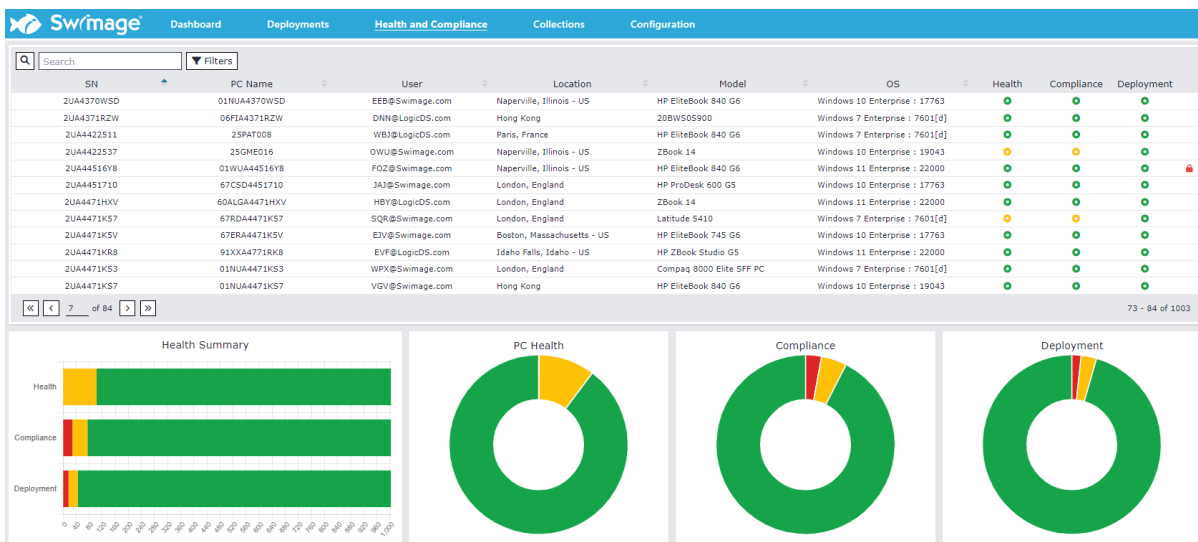
Swimage Compliance Enforcer Has Arrived!

Zero Trust Security and Swimage





The Swimage Compliance Portal is where system compliance is monitored and compliance enforcement rules are applied.



Swimage takes immediate action on any PC that fails compliance or becomes unhealthy. Swimage has numerous built-in actions immediately available to repair your PCs, plus Swimage can be extended to perform any customized actions desired, so that your corporate security policies are enforced.

Some basic actions built in to the Swimage process include:

- Lock the PC
- Reimage the PC
- Clean up drive space
- Reinstall hardware drivers
- Install patches
- Install software
- Remove software
- Rejoin the domain
- Encrypt the PC

Swimage Compliance Enforcer easily integrates with existing Modern Management tools, or it

can run completely standalone. Initial set-up is quick and easy, with base functionality in a few hours.

To learn more, email Info@Swimage.com to schedule a free consultation on your current compliance requirements and see how Swimage may help your organization. You can also view an online demonstration at www.Swimage.com.

Zero Trust Security and Swimage

Swimage is a fundamental component of zero trust security frameworks. Swimage integrates with security stacks and ensures that all PCs, regardless of location, remain secure, healthy, and compliant.



Swimage leverages a combination of templates, compliance rules, triggers, and actions to provision, build, and enforce a PC's desired state. This ensures that PCs are built to your precise specifications and that the PCs remain in that state throughout their life. If a PC is found to be out of compliance for any reason, Swimage automatically and immediately takes action to resolve the issue.

Swimage fulfills zero trust requirements in the following ways:

For continuous monitoring and verification, Swimage:

- Continuously retrieves updated compliance rules from a central server and instantly enforces those rules to ensure all PCs remain healthy and compliant.
- Monitors the software and security stack and remediates immediately if the stack is not aligned with policy. This includes restarting services, reinstalling software, locking the PC, or other actions as needed.
- Monitors for changes in state, such as IP, location, software, network usage, etc. State changes may trigger reauthentication, as needed.
- Maintains and confirms the "known good sources" when repairing or rebuilding a system. This ensures that no application or OS component will be compromised.
- Prevents user interaction or login until the entire security stack has been applied and is functional.

To limit the impact of a breach, Swimage:

- Locks access to critical system files in order to maintain system integrity.
- Encrypts all server communication with private key hashes with multiple verification points.
- Responds in seconds to a breach and takes appropriate action to remediate the problem across the entire network.
- Immediately disables the network, locks the system, and initiates a full redeployment from validated sources.
- Executes actions regardless of PC location or state.
- Rebuilds the entire system - restoring all applications, security policies, settings, and data from known good sources.

To fully automate data analytics and responses, Swimage:

- Provides administrators full visibility into the current status of all endpoints with an intuitive and customizable portal.
- Monitors and applies instant lock or remediation actions based on configurable rules.
- Takes actions using graduated alert levels, including actions to report, lockout, remediate, or redeploy.
- Provides real-time status data processing and rule enforcement using automated response mechanisms.

Additional ways Swimage fulfills zero trust security requirements will be shared in future newsletters.