Guaranteed State Automation

Ineffective monitoring, control and remediation processes leave endpoints vulnerable and organizations exposed to security and compliance risk.

Visibility of current state rather than last known state and automation of continuous, standards-based security controls allows organizations to avoid 'configuration drift'.

Automate for continual compliance. Reduce workload in advance of, and as a result of internal and external audits.

Get real-time visibility. Audit configuration and generate reports in seconds, not weeks.

Global brands trust 1E

Strong IT controls like Microsoft Windows Security Baselines, help organizations prevent successful cyber-attacks and reduce risk.

According to a 451 Research Group Survey

64%

of organizations globally feel that complying with regulatory and industry mandates is either "very" effective or "extremely" effective in combatting security threats.

A recent Federal Cybersecurity survey found

54%

of IT professionals believe that security controls and mandates can lead to complacency as a tick box exercise – without understanding the real, measurable security outcomes achievable.

According to a Verizon report on Payment Security

71%

of organizations fell out of compliance less than one year after being assessed compliant

Compliance drift means controls which are audited annually or quarterly do not provide security value every day.

Existing policy tools have limited capabilities and poor reporting capability as a result organizations face 3 main compliance challenges:

1. The adverse impact of unapproved and often unintentional configuration change by end users and administrators leading to 'Configuration drift' between audit windows. As a result desktops and servers alike are left vulnerable due to a lack of continuous compliance capabilities.
2. Difficulty in visualizing current actual state and ensuring device configurations remain adherent to policy defined requirements at all times - particularly with regard to devices used by remote workers.
3. The skills gap in IT which leads to a lack of resources with the technical capability required to ensure continual compliance leaves organizations exposed.

Organizations need to think strategically about operational controls in order to take care of basic hygiene factors which reduce cyber risk and downtime while improving end user productivity.

Apply best practice controls from well-tested configurations such as Windows Security Baselines for your IT environment to strengthen your security posture.

Ensure you have up to the minute data on current configuration state and compliance of all endpoints - even for remote workers.

1E's Guaranteed State solution leverages Tachyon to remove manual effort and a reliance on tooling such as Group Policy when implementing standardized configuration at scale. Tachyon enables you to configure third party applications as well as Operating System settings. Tachyons distributed computing architecture provides real time visibility and remediation which means you can ensure continual compliance and perform audits of current state in seconds, across all endpoints.

Implement standards such as Windows Security Baselines, NIST 800.53, and ISO 27002 or customized configurations. Tachyon guarantees device configuration stays adherent to controls and will alert personnel (including the end-user) when an attempt is made to alter the mandated configuration setting.

Talk to 1E today about automating your baseline configuration leveraging real-time visibility and automation with Guaranteed State. 1E can help you identify and act on deviations from requirements.

Find out more at: https://1e.com/solutions/guaranteed-state