Ensure company policy enforcement and regulate end-user freedom

The risks associated with unlicensed and unauthorized software on your end-users’ computers have never before been so high.

As end-users habits and behavior continue to evolve, they rarely think twice about downloading their favorite applications or the latest productivity tools. What your users don’t know is that up to 25% of file downloads contain malicious code or spyware. Security analysts’ report that up to 80% of security breaches occur inside the firewall on the end-user side. It has become essential to have effective visibility of the workplace infrastructure and a clear and accurate view of compliance activity.

The existence of a security strategy is only the first step in the process towards complete and effective compliance. With NEXThink V4 you can be sure that all operating tools, patches, security software and security settings are compliant and functioning well all the time. Additionally you can set alerts to identify security risks and other abnormal network activity.

Check your workplace controls in real-time

NEXThink helps you identify and provides for rapid response on all security risks and breaches to corporate security compliance policy.

NEXThink V4 monitors all your desktops to determine if your critical security settings are in place and enforced. These settings can include desktop management agents, anti-virus pattern files, disk encryption settings, back-up software and critical patch files. If a potential breach exists alerts can be set for notification and action to remediate and reestablish compliance.

NEXThink continuously audit your IT workplaces to offer compliance dashboards covering all key controls ensuring enforcement of company security policy and standards (ISO 27001, PCI, etc.).

NEXThink technologies seamlessly integrate with security events monitoring solutions to provide full end-to-end coverage of the security and compliance in the enterprise.
NEXThink simplifies Security and IT management

NEXThink user-centric visibility eases IT operations and Security Administrator jobs with immediate understanding of causes and effects related to the end-user computing environment. Being able to instantly detect unwanted activities (non-corporate applications, malware, etc.) or security control bypass, spot misconfigurations, without endless analysis of log files, and to be alerted immediately change the game for the IT staff. Interdependencies of infrastructure usage from end-users’ perspective are essential to simplify people life who manages the infrastructure, security and compliance to corporate security policies and procedures.

“With NEXThink I have the right information to demonstrate end-user workplace security compliance to the business.”
—Jorge Raposo, CSO, Crédito Agrícola

“NEXThink allows us to find abnormal software behavior in the network much faster.”
—Adrian Senn, Head of Network Management, University Hospital of Zurich

Key benefits

- **Desktop compliance monitoring**: verify the status of all security settings and automatically detect any deviation from corporate rules.
- **Security auditing visualizations**: create security and compliance dashboards for thousands of desktops in minutes.
- **Alerting**: informed notification on suspicious, unauthorized and abnormal software activities, and non-compliant configurations or utilizations.
- **NEXThink Application Library**: more than 400,000 applications and behavioral patterns to identify threats and classification of non-compliant software.
- **End-to-end security coverage**: correlate user-side threat events and activities with your global security reporting to produce comprehensive compliance audit reports.