

# The **Complete** Endpoint Security & Compliance Solution

Soliton's **InfoTrace Endpoint Security and Compliance Management Solution** provides multiple layers of endpoint security, data access control, policy enforcement and forensic reporting to maintain compliance, reduce risk, and streamline audits and incident response.

Whether driven by regulatory mandates such as PCI DSS, HIPAA, ISO 27001, FISMA and others, or enforcement of internal policies, endpoint security compliance is a reality for virtually any business today. InfoTrace helps businesses maintain compliance and reduce the risk of malware infection, data breach, and insider data theft.

## Controls Data Access

With role-based profiles, two-factor authentication, and single sign-on enforcement, InfoTrace makes it easy to manage user or device-based access to applications, files, folders, drives and external devices.

## Maintains Compliance Between Audits

InfoTrace provides persistent endpoint monitoring and policy enforcement to ensure your endpoint environment is compliant across all branch locations and inside or outside the network.

## Protects Against Malware & Insider Data Theft

InfoTrace helps to reduce security risks by augmenting your current infrastructure with additional security layers such as behavior-based blocking and remediation of zero-day malware (including ransomware), application whitelisting and blacklisting, web vulnerability protection, network and device access control and file, print and copy restriction.

## Enables Rapid Incident Response

InfoTrace provides detailed logs and an event timeline on endpoint device and user activity. Incident responders can quickly understand what occurred, how broadly it has spread, what data was affected, and which other endpoint systems are at risk.

## Increases Operational Efficiency

Security teams operate more efficiently with InfoTrace by combining endpoint security, policy management and incident response functions into a single, integrated solution that enables monitoring, control, and investigation from a single console.

## Simplifies Policy Rollout

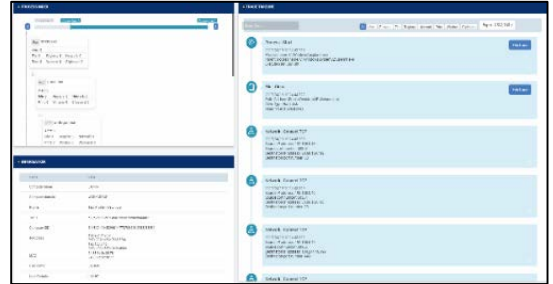
Pre-configured policy templates, based on common regulatory requirements, enable InfoTrace to accelerate and simplify roll-out and enforcement of your endpoint security policies.



# InfoTrace Features

## Detailed Endpoint Logging & Analysis

- Provides detailed timeline for behavior of suspicious files from introduction to execution and propagation
- Investigate insider data theft with data access reports detailing user actions such as copying over the network, file name change, printing, copying to USB device, web activity, etc.
- Detailed syslog data and alerts can be quickly reviewed in the management console or exported to a SIEM
- Log data is encrypted to preserve evidence



## Multi-layer Device & Data Access Control

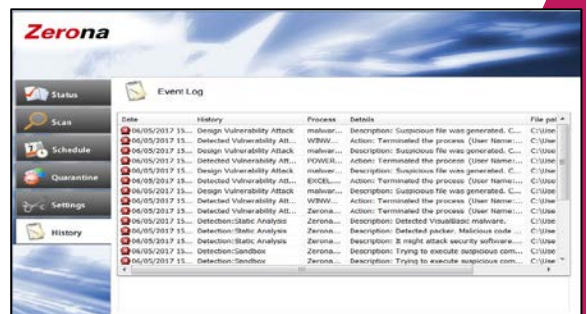
- Controls user access to system tools, files, applications, folders, network servers, and external storage devices
- Blocks unauthorized file access, printing or copying of restricted data
- Flexible controls enable administrator to set access rules to *prohibited*, *read-only*, or *hide* for any file or folder

## Network Authentication of Both User and Device

- Ensures only authorized devices and users are allowed network access
- Controls BYOD and Shadow IT by blocking unsanctioned endpoints
- Enforces multiple authentication methods such as one-time password, smartcard, biometric scanners, etc.

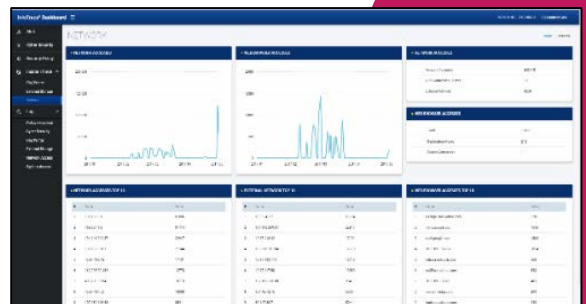
## Advanced Anti-Malware Protection

- Multi-layer scanning blocks known and unknown malware, including ransomware
- Does not conflict with your current endpoint security layer
- Does not rely on threat signatures so it's always up to date
- Enforces application whitelisting and blacklisting
- Kills malicious processes and restricts network and application access to quickly quarantine an active infection



## Easy Policy Management

- Pre-configured policy templates enable administrators to create and distribute role-based security profiles to every endpoint
- Quarantines endpoints which do not meet minimum policy requirements
- Issues administrator and user alerts on restricted behavior
- Real-time reporting on all policy violations



**Contact Us:** 3900 Kilroy Airport Way, Suite 280 Long Beach, CA 90806  
Tel: +1.714.243.6121  
sales@solitonca.com