Zero Trust Security Solutions

ThreatLocker: Allowlisting, Ringfencing, Storage Control, Elevation Control, Network Access Control

Protect your applications, data, users, devices, and networks against cyber threats with GSI's Zero Trust cybersecurity solutions and services. Our unified approach defends against ransomware, malware, zero-day attacks, and more while also addressing vulnerabilities. Our comprehensive solutions include Application Allowlisting, Ringfencing, Storage Control, Elevation Control, and Network Access Control.

The SolarWinds/Orion software attack recently shook the cybersecurity landscape, penetrating over a hundred companies and government agencies. Among the affected entities were industry giants Microsoft, Intel, and Cisco, as well as federal departments such as the Treasury, Justice, Energy, and even the Pentagon and Cybersecurity and Infrastructure Security Agency (CISA).

Protect yourself against such cyber threats now with our Zero Trust cybersecurity solutions and services. Contact us today to secure your applications, data, users, devices, and networks.

Zero Trust Solutions and Services:

- Allowlisting / Whitelisting
- Ringfencing
- Storage Control
- Elevation Control
- Network Access Control (NAC)

Zero Trust Solutions and Services

Allowlisting / Whitelisting

Keeping your computer safe from malicious software is of utmost importance, and ThreatLocker's Allowlisting provides an effective security measure to achieve this. This approach acts as a strong barrier against ransomware and malware infiltrating your device by explicitly approving applications that are permitted to run on your system. During installation, the agent identifies all applications and dependencies running on your computer and creates policies that permit them. This allows you to review the list and remove any unnecessary applications, giving you a high level of control over the software running on your servers and endpoints. Such control is crucial in minimizing cyber threats and preventing unauthorized applications from accessing your network.

Ringfencing

ThreatLocker's Ringfencing™ empowers you with complete control over the behavior of applications that are already running, thus limiting the possibility of successful attacks or exploitation. With Ringfencing™, you can manage the software, scripts, executables, and libraries that can operate on your servers and endpoints, providing additional protection against cyber threats and unauthorized access. The feature enables you to withdraw file access permissions for applications that don't require access, remove network or registry permissions, and customize detailed application policies to suit your organization's unique requirements. Deploying Ringfencing™ aligns your device with default policies that provide a baseline level of protection for all endpoints, ensuring your data remains secure and protected from fileless malware, application attacks, or unauthorized access.

Storage Control

Protection of your data against unauthorized access or theft is of utmost importance. The all-encompassing Storage Control provides a solution through policy-driven control, allowing you to manage storage devices, including local folders, network shares, and external storage such as USB drives. ThreatLocker® Storage Control offers granular policies, from simply blocking USB drives to blocking access to backup shares, except when accessed by your backup application, providing you with a comprehensive solution to safeguard your data.

Elevation Control

Elevation Control by ThreatLocker takes your security to the next level by allowing IT administrators to remove local admin privileges from users yet still permitting them to run specific applications as an administrator. This grants complete control over which applications can be run as a local admin without giving users local admin rights.

Network Access Control (NAC)

With cyber threats on the rise, protecting your network is more important than ever. That's where Network Access Control (NAC) solutions come in, and ThreatLocker® NAC provides the ultimate protection for your endpoints and servers. Thanks to custom policies allowing access to specific IP addresses authenticated by agents, you can watch endpoint policies and network traffic from a central location. And with dynamic ACLs that block unauthorized access to servers and endpoints and opening ports based on the device's location or group, you can ensure a secure connection between the server and the client. By deploying ThreatLocker® NAC, you can rest easy knowing your devices and data are shielded from cyber threats.
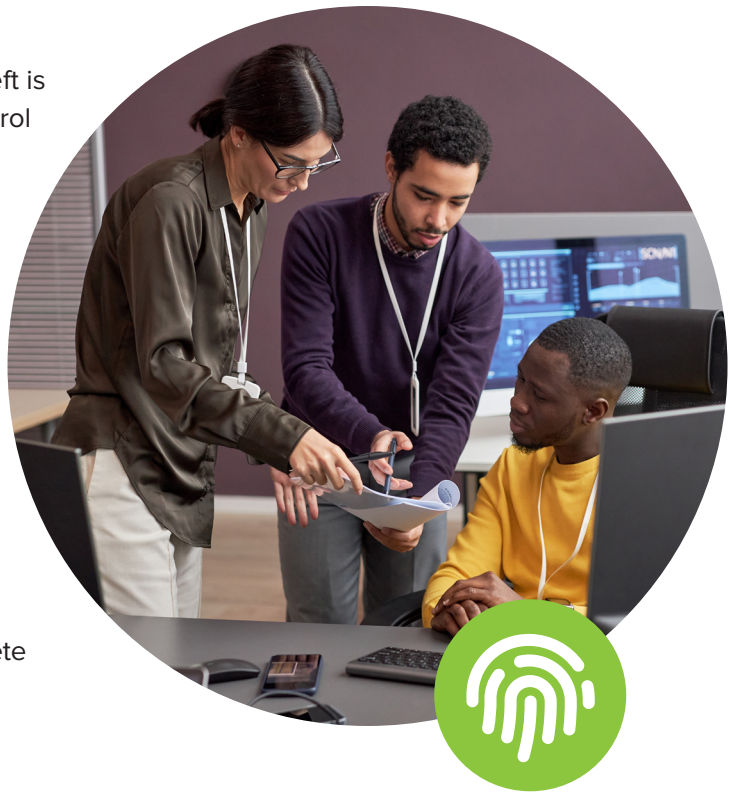
What Makes GSI's Zero Trust Solutions Different?

Application Expertise

Industry-leading enterprise application experts with an average of 18+ years of application, security, industry, cloud, business, and managed services experience.

Certified CISO & vCISO Resources

GSI has certified Chief Information Security Officer (CISO) and virtual Chief Information Security Officer (vCISO) resources.

Certified ISO 27001 Lead Implementer

Certified ISO 27001 Lead Implementer resources on staff. GSI is certified to implement the formal structure, governance, and policy of an ISO 27001 conforming to the Information Security Management System (ISMS) standards.

AICPA SOC 2 Certified

GSI is SOC 2 certified by the American Institute of CPAs (AICPA) which demonstrates that GSI has specific security controls in place.

Sub-5-Minute Response Time

Average sub-5-minute response time to tickets and alerts.

100% Signature Guarantee

All Services Backed by GSI's Signature 100% Guarantee.

Challenges Addressed by Zero Trust Solution

Challenge
Credential-based attack

Solution
Strong authentication mechanisms and multi-factor authentication

Challenge
Virus, malware, ransomware attacks

Solution
Zero Trust uses a combination of Default Deny & Ringfencing to protect against known and unknown malware threats

Challenge
Erosion of traditional control points: Remote work, Cloud, SaaS, digital supply chain create vulnerabilities

Solution
Enforcing stringent access controls, checking device health, and monitoring user activity for remote workers, cloud resources, SaaS solutions, and digital supply chain

Challenge
Insider threats

Solution
Strict access controls

Challenge
Compliance requirements (NIST, HIPAA, CIS, PCI and other regulators)

Solution
Implementing rigorous access controls, encryption, and monitoring capabilities

Challenge
Lateral movement on network after breach

Solution
Granular access controls to limit movement on the network

For more information:

Contact us today to learn more. You can also email us or call (855) 474-4377.

GSI, Inc.

GSI is a forward-thinking organization that aligns and optimizes your digital footprint with your business goals. We combine our deep business and industry experience with our expert knowledge of enterprise applications, automation, cloud and cybersecurity to deliver secure and flexible systems that allow your business to thrive and not just survive.

GSI's comprehensive suite of solutions includes: AppCare, a 24/7 managed service that includes EaaSy with flexible "on-demand" services and dynamic pricing; GENIUS AI, an Application Intelligence Platform (AIP) for creating application health and user experience monitors; GENISYS, a solution for optimizing system performance; RapidReconciler®, its inventory reconciliation software; GENOME, which automatically Detects, aNalyzes and Automates the process of converting customizations into Orchestrations; and GatewayNow, low-cost, accelerated time-to-value ITSM solution using the industry-leading ServiceNow platform in a fully managed environment.

GSI consulting and managed services are backed by its signature 100 percent guarantee. Founded in 2004, the rapidly growing company is headquartered in Atlanta with worldwide resources. With over 100 employees, GSI consultants average over 15 years of real-world experience and are certified experts in business, industry, and enterprise applications. GSI provides comprehensive 24/7 global support.