Gladiator Total Protect™

Next-Generation Suite of Security Services

You face increasingly complex cyber threats. Traditional methods for protecting your community or regional financial institution (FI) against cyber threats have become less effective over time. And in today's challenging business environment, addressing security in silos provides an incomplete picture. **How prepared are you to mitigate today's evolving cyber threats?**

increase cyber resiliency through complete visibility

Cyber-attacks can often only be detected through a holistic view and analysis of events occurring across your network. So it's more important than ever to gain a comprehensive view of your entire institution. Aggregation and correlation of events across all systems and networks can provide management with better visibility of potential cyber threats. More visibility leads to a better assurance that your security controls are effective, which will lower your risk profile and reduce your total cost to mitigate threats.

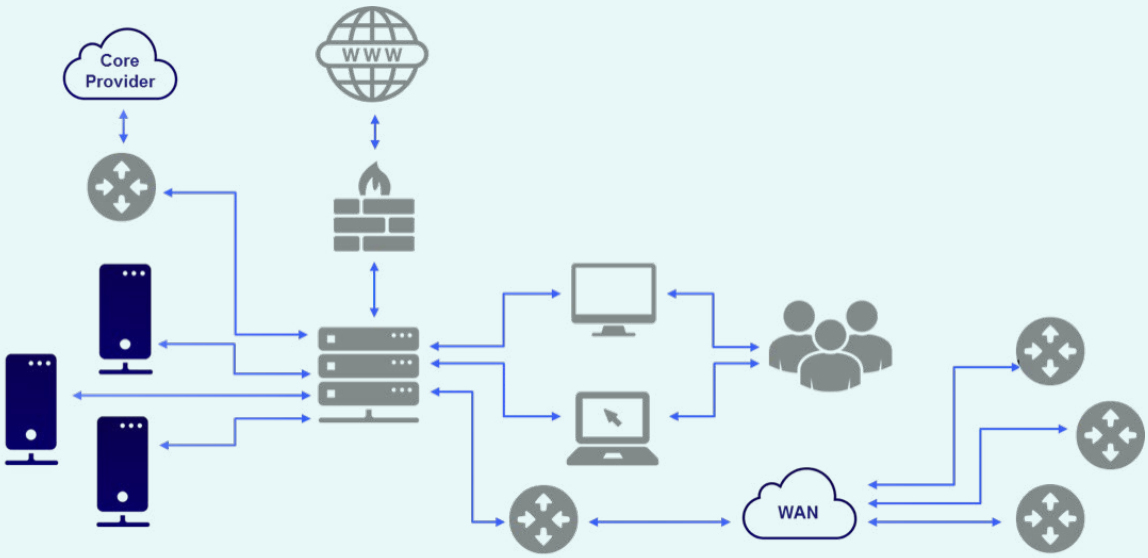
cybersecurity

Gladiator's Total Protect suite of services provides an arsenal of tools that empower you to proactively detect, mitigate, and prevent cybersecurity risk. With our suite of security services, you gain comprehensive visibility across your FI by incorporating the protection of the following primary elements:

- People
- Internal Network
- Servers
- Mobile Devices
- Internet
- Vendor Connectivity
- Workstations
- Branch Offices

jack henry™

financial institution sample network



features and benefits of Gladiator Total Protect

Managed Security Services	Features and Benefits
Unified Threat Management (UTM)/Firewall Management and Monitoring	Service includes secure firewall configuration and change management, periodic firewall configuration audits, ongoing IDS/IPS tuning to ensure the security baseline is optimized, 24/7 advanced security information and event management (SIEM) correlation and security monitoring, raw traffic analysis, adaptive threat management, and regulatory-focused reporting.
Incident Alert – Sandbox Detection and Protection	Service examines encrypted and unencrypted files in emulation to detect unknown malware, stop those threats at the UTM device before they can reach your internal systems, and alert your organization to the blocked file(s).
Gateway Data Loss Prevention (DLP)	Service leverages your internet UTM device(s) to analyze file uploads, alert you to, and potentially block suspected data leaks. Your internal files containing sensitive data can be pre-watermarked, enabling the UTM to block the transmission of all watermarked files. The service also detects large file uploads to an external destination to detect potential data exfiltration events.

features and benefits of Gladiator Total Protect (continued)

Managed Security Services	Features and Benefits
Enterprise Vulnerability Scanning	Provides you with accurate information on vulnerabilities that exist in your environment. Automatically scans your internal network on a weekly basis for new vulnerabilities and provides access to detailed reports and remediation recommendations.
Microsoft M365 Intune Mobility Management	Provides mobile device management services that are tailored to device content management, security policy enforcement, and secure bring your own device (BYOD) support. It keeps mobile endpoints running securely with scalable configuration. (Requires M365 E3 or O365 E3 with mobility + security add-on licensing.)
e/cSAT (electronic/commercial Security Awareness Training)	Web-based IT regulatory compliance education for employees and commercial customers. Provides a customized and convenient online program that educates on policies and procedures and helps ensure that day-to-day business practices foster a secure, compliant workplace.
System Monitoring and Reporting	Part of our managed IT services (MITS), this service provides 24/7 monitoring and reporting of system availability, server performance, critical applications, and data backups.
Endpoint Protection	Centrally managed endpoint security on all computers to ensure optimal performance and security protection. It also includes proactive scanning, agent management, and 24/7 SIEM correlation and security monitoring.
System Patching	Critical security patches are tested and deployed weekly to help protect against exploits. Windows and third-party applications are automatically updated.
Server Event Log Analysis	Service delivers 24/7 advanced SIEM correlation and security monitoring for failed log-on activity, administrative activity, administrative-level group creation/deletion, administrative user privileges granted/removed, and security log maintenance.

features and benefits of Gladiator Total Protect (continued)

Managed Security Services	Features and Benefits
Server Security Monitoring	Enhanced server monitoring to detect access or changes to critical system and registry files. A “honeypot” file is also installed and monitored for any access attempts. This service expands Server Event Log Analysis to detect early indications of a compromise or suspicious threat activity on your servers.
Router and Switch Monitoring	Service delivers 24/7 advanced SIEM correlation and security monitoring for routers and switches to detect port security activity and log-on security violations.
Authentication Monitoring	Service provides 24/7 advanced SIEM correlation and security monitoring of authentication services and platforms outside of the traditional server, firewall, or switch/router logins.
Enterprise-Level Backup and Recovery	Immutable, air-gapped backup and recovery of Windows-based core systems, complementary, and business software, as well as data assets.

connect with next-generation technology

Learn more about our cybersecurity solutions.

For more information about Jack Henry, visit jackhenry.com.