Quest's Overview of the CyberDefense Suite

Learn more about how our **CyberDefense Suite offerings** can help ensure your data is protected.

Quest
TECHNOLOGY MANAGEMENT

Continuous Threat Protection, Monitoring, and Alerting

Gain protection and visibility across your organization, from endpoint to network and into the cloud, and expand your view of the virtual landscape. With Quest's expert resources and sophisticated tools, you will have the perspective to determine what requires your immediate attention and which action is most appropriate. Rest easy knowing that Quest Cyberdefense professionals are watching your environment in real-time and around the clock.

Endpoint Device Security/EDR

Quest will provide and monitor your endpoint platform and alert you of events as they happen. With an AI-driven, Cylance-powered approach, Quest's Endpoint Device Security Protection and Endpoint as a Service (EPaaS) delivers reliable security intelligence from events generated at all your endpoints to deal with suspicious activity immediately. Quest's EPaaS can be instrumental in shortening incident response times and serve as the first step toward proactive, continuous threat hunting. Quest offers full EDR, endpoint detection and response, services.

CyberDefense Suite Overview

Endpoint Device Security/EDR

Email Security Protection

Device Monitoring/ Alerting/MDR

Vulnerability Scan/Attack Surface Management

Patch Management

DNS Security

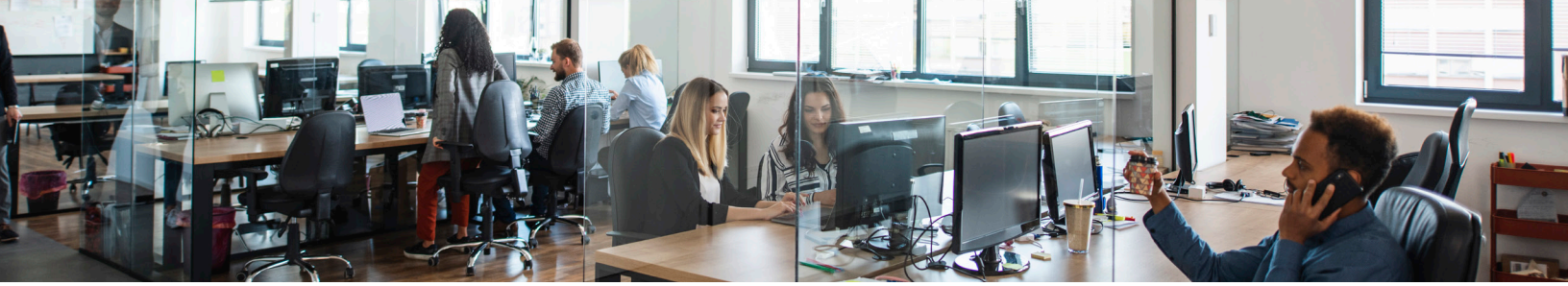
Password Protection/ Breach Detection

MFA: Multi-Factor Authentication

SIEM: Security Information & Event Management

ZTNA: Zero Trust Network Access

Immutable Storage



Email Security Protection

Quest's Email Security Suite (powered by Proofpoint) helps you protect your people, data, and brand. Quest's Email Security Suite meets the needs of even the most complex enterprise deployments supporting cloud, hybrid, and on-premises installations.

Device Monitoring/Alerting/MDR

Quest monitors and alerts 24/7 on the thousands of messages generated by your firewalls and IDS/IPS. Quest keeps your IDS/IPS devices up-to-date and appropriately monitored—allowing you to swiftly identify and respond to any potential threat.

Vulnerability Scan/Attack Surface Management

Quest provides an external vulnerability assessment and enforcement of security policies. There is no infrastructure to deploy or manage. Quest helps organizations accurately and systematically document regulatory and policy compliance. We advise companies to scan monthly and adhoc as new services are added or a new threat emerges. Quest offers continuous monitoring for complete attack surface management.

Patch Management

Patch Management Agent provides patching and remote access to help reduce support time and limit vulnerabilities for patching capabilities.

DNS Security

Quest's DNS as a Service (DNSaaS), including cloud security services, provides a first line of defense against threats, wherever users access the internet—on or off the corporate network. We provide and monitor with 24/7 alerts when and how you need it. Quest deploys our DNS enterprise-wide in minutes so your security team gains threat intelligence and the context needed to block threats before they become attacks.

Password Protection/ Breach Detection

How your passwords are managed can make or break your defense against identity theft. Our specialized security framework provides premium protection for all data and systems that is easy to implement and manage. Quest gives you transparent guidance and compliance to ensure your organization is safe and secure.

MFA: Multi-Factor Authentication

With a sophisticated series of tools from Quest, you can reinforce your workforce and your security protocol. Multi-factor authentication provides endpoint platform protection while monitoring for advanced threats on all endpoints, and you'll be able to leverage the extensive skills and capabilities of our pedigreed Incident Response team. Additionally, invaluable insights empower your organization with actionable threat intelligence.

ZTNA: Zero Trust Network Access

Discover how Cloud ZTNA services from Quest are a smarter way to grant private app access to the right users at the right time. A central hub serves as a connection point between users and apps, eliminating the need for interaction with your network or the apps themselves. Instead of a time-consuming, frustrating, and high-risk method, you can easily master app access across the board.

SIEM: Security Information & Event Management

Quest's SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure. The software then identifies, categorizes, and analyzes incidents and events. You'll receive comprehensive reports on security-related incidents and events, and will be alerted in the event that an activity runs against predetermined rulesets (and thus indicates a potential security issue).

Immutable Storage

The benefit of Quest's Immutable Storage is that data, once written, cannot be deleted, or altered for a predetermined length of time. We're seeing more cases of bad actors encrypting and/or deleting backup files. This is essentially a third copy of your backups that cannot be altered in any way due to WORM (Write-Once Read-Many) storage solution. You can select from any one of our global Service Delivery Centers to store your data.

How can we help?®

1-800-326-4220 • www.questsys.com

Quest TECHNOLOGY MANAGEMENT

0822.V1.2