Cybersecurity Services

Keep your network robust, reliable and secure.

Quest®
TECHNOLOGY MANAGEMENT

The Importance of Cybersecurity

In the current digital era, threats range from sophisticated phishing schemes to highly targeted attacks, orchestrated by advanced adversaries. To counteract these challenges, businesses require not just a suite of IT security tools but also seasoned experts to ensure those tools safeguard both data and personnel effectively. The pillars of cybersecurity—risk assessment, protection, and remediation—are crucial for any enterprise. By collaborating with a team of certified professionals who engage closely with your leadership and staff, you can seamlessly build and sustain a robust digital defense. Quest stands poised to demystify these threats and fortify your defenses against them.

Cybersecurity Services Overview

No matter what kind of organization you are, ranging from a local business to a multi-billion-dollar franchise, cybersecurity must be a top priority. In addition to regulatory compliance concerns, you need to avoid the many dangers in the current digital world. Today's IT environment is riddled with risk, including data breaches and ransomware, and the frequency is increasing exponentially. 68% of business leaders feel their cybersecurity risks are increasing—and they're right. You need to defend your business, but where do you start, and what do you do?

Cybersecurity Services

- CyberDefense Suite
- Managed Detection & Response (MDR) Services
- Incident Response
- Endpoint Protection (EPaaS)
- Monitoring & Alerting
- Patch Management (PMaaS)
- Password Management as a Service (PWMaaS)
- Security Information & Event Management
- Data Protection (Immutable Storage)
- Cloud Zero Trust Network Access
- Distributed Denial of Service (DDoS) Protection
- Email Security Suite
- Cyber Risk Monitoring & Management
- Ransomware Assessment
- Cybersecurity Awareness Training & Workshops

Learn more about Quest's **Cybersecurity services.**

The answer: contact Quest. We're committed to establishing and maintaining comprehensive digital and IT infrastructure security to keep your company safe. Our experienced and certified cybersecurity support experts will work directly with your executive teams, key stakeholders, department managers, and subject matter experts to analyze your business processes, then develop and support comprehensive digital security to protect your organization.

A Complete Cybersecurity Program

A complete cybersecurity program includes people, processes, and technologies. At Quest, we customize our programs to address your company's specific needs, based on the assessments performed by our experienced and certified IT experts.

Quest creates a layered approach that ties people, processes, and technologies together to establish and maintain a comprehensive 24/7 safety net for your business. Your cybersecurity and data privacy program can include everything from security awareness training for your staff to cybersecurity risk assessment services to ongoing threat hunting, monitoring, management, and endpoint protection wherever you need the extra level of defense against cyber threats.

Quest is at the forefront of providing a wide array of cybersecurity services tailored to meet the unique needs of diverse industries and businesses. As the digital landscape becomes increasingly intricate, we remain committed to ensuring our clients' assets and data remain protected. Delve deeper into this section to gain a comprehensive understanding of the robust cybersecurity solutions we have crafted to safeguard your operations. Explore our suite of cybersecurity solutions, meticulously designed to fortify your operations and ensure unparalleled protection.

CyberDefense Suite

Protection & Visibility Across Your Network

The average cost of a malware attack today is estimated at **$2.6 million**, and the average cost of a data breach is **$3.9 million**. The longer it takes to detect and respond to threats, the riskier and more costly the remedy. This is why it's so crucial to have constant visibility —a benefit that you can gain through Quest's CyberDefense Suite.

Our expert resources and sophisticated tools let you triage your needs and determine which actions to take. Rest easy knowing that Quest's cybersecurity professionals are watching your environment in real-time and around the clock. The suite contains a variety of useful services.

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 endpoint detection and response (EDR) services.

Email Security Protection

Quest's Email Security Suite (powered by Proofpoint) helps you protect your people, data, and brand. This 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 ad hoc 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.

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).

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.

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.

Quest presents a holistic approach to IT security, encompassing advanced features ranging from Network and Service Device Patching to SIEM (Security Information and Event Management) solutions. We integrate robust tools for device monitoring, mobile device management, and penetration testing. Moreover, our offerings extend to server monitoring, comprehensive patching solutions, and dedicated services for backup and disaster recovery. All these are bolstered by our state-of-the-art Firewall/IPS/IDS platforms.

Managed Detection & Response Services

Prevent security threats from becoming security incidents by leveraging Quest's advanced analytics, threat intelligence, and human expertise to deepen your monitoring protocols and turbocharge your response capabilities.

Quest's Cybersecurity Experts Are Your Cybersecurity Experts

As cybersecurity threats multiply, it has become virtually impossible for most organizations to adequately provide security with in-house teams. Few have the staffing, expertise, or security tools on hand to smoothly manage their monitoring and alerting operations, much less provide timely response when an intrusion occurs.

With Quest's Managed Detection and Response (MDR) Services, our experts will protect your data and assets even if a threat manages to get past your organizational security controls. It's a next-level, 24/7 security control platform that is ideal for organizations that either can't or prefer not to maintain their own security operations center.

While it can normally take months and even longer for an organization to stand up a security team capable of handling today's threats, Quest's MDR services provide immediate protection.

Experience Advanced Cybersecurity Technologies

Machine-learning technology provides the first layer of a deep view of advanced analytics. Quest's detection tools then provide the necessary visibility into security events and deliver solid endpoint telemetry, forensic data, and threat intelligence. Quest's global network of hardened data centers further offers redundancies that guarantee the minimum of disruption should a threat become a breach.

Round-the-clock surveillance by a team of experts is essential for real security, ensuring the proactive approach that is essential to protecting your organization. Quest's Managed Detection and Response Services Agreement puts an experienced team of security experts at your disposal 24/7.

Real Security Experts Work Directly With Your Team

Regardless of how sophisticated your layers of automated defenses are, today's armies of highly motivated bad actors can overwhelm them. Aided by artificial intelligence (AI) and machine learning, Quest's human threat hunters have extensive experience identifying and thwarting the most evasive threats that arise.

Benefits of Quest's MDR Services

- AI plus 24/7 human monitoring ensures immediate detection.
- Triaging alerts deliver prioritized reports.
- Cybersecurity experts with machine-learning tools perform real-time analysis.
- Focused investigation yields actionable threat intelligence for rapid response.
- Immediate response isolates endpoints and blocks persistent modules that are pinpointed as root-cause, stopping attackers and preventing catastrophic incident.
- Zero-trust threat hunting tools protect entire enterprise.

Leverage Your Cybersecurity Investment

It's likely that you have over-invested in automated cybersecurity that is not delivering sufficient returns. There are almost certainly tools in your toolkit that have not been fully deployed because of a lack of time or resources. Quest's MDR services can maximize your current effort and take it to the level you require.

Quick & Decisive: Tracking Threats, Correlating Data, & Facilitating Remediation

Unless you have a full contingent of cybersecurity experts on staff, you're not able to act on whatever actionable information you are able to uncover. But with our experts on your side, you'll be ready. Managed Detection and Response Services ensure that you are prepared to respond quickly and decisively to any threat.

Optimize Your Resources With a Trusted Cybersecurity Partner

As endpoints increase with remote workers and their numerous devices, along with the proliferation of the Internet of Things (IoT), the security that protects these endpoints has grown exponentially. That has resulted in tidal waves of security alerts that swamp your own IT team. Quest's Managed Detection and Response Services can free your IT team from dealing with reactive and time-consuming incident response, allowing them to do more strategic work. That's why, in addition to protecting their organizations from potential catastrophe, many find that the benefits of MDR services accrue to their core business and bottom line.

MDR Services Tailored to Your Cybersecurity Needs

The first step towards true cybersecurity is a thorough assessment of your organization's security position. Your security needs and vulnerabilities will vary depending on your industry and the scale of your operation, which is why we tailor your agreement according to your specific requirements.

Incident Response

Reliable & Trustworthy Critical Incident Response Team

Experiencing an active threat? Contact Quest at any time. Our Incident Response Team takes quick, effective, and orderly action to address incidents such as:

- Virus infections
- Hacker attempts and break-ins
- Improper disclosure of confidential information to others
- System service interruptions
- Breach of personal information
- Other events with serious information security implications

Quest IR Support Is Available 24/7, Responding to Threats Within 60 Minutes

Our IR Team is ready to act immediately, effectively, and skillfully in the event of computer system, network, or database threats. Our IR team can help minimize cybersecurity incidents and reduce the costs associated with recovery. And, if you have a cyber liability policy, Quest will work with your insurance company to meet the coverage requirements.

Don’t Wait to Be Attacked. Get Your Strategic Incident Response Plan in Place.

Even the best security infrastructure won't prevent all intrusions or malicious acts. Technological advancements make it possible for hackers to employ sophisticated methods of attack at an alarming rate. The speed with which your company recognizes, analyzes, and responds to a data breach and other computer security incidents makes all the difference in your survivability.

Our goal is to help prevent your company from experiencing the potential financial, professional, and legal damages associated with these breaches. Because we believe that a successful response plan requires comprehensive threat intelligence, our cyber incident response services always begin with a thorough incident response capability assessment.

Quest’s Comprehensive Incident Response Approach

Hackers and bad actors constantly try to find new and devastating ways of infiltrating your network traffic and compromising your data. But Quest’s proactive Incident Response services and emergency services help you prepare for, respond to, and recover from a data breach. We have access to a constantly updated set of cyber incident response tools. Our specialists will work with you to evaluate your existing plan, develop a new one, and provide an organized and rapid response when you need it.

1. Proactive Planning

- IR Readiness Assessment and Playbook

2. Service Level Agreement

- Retainers and Bundled Response Packages
- Support Remediation Efforts
- Deploy Quest's Managed Security Service Provider (MSSP) Containment Tools

3. 24/7 Emergency Response Team

- Identify
- Detect
- Contain
- Eradicate
- Recover

Incident Response Workshop & Service Options

Identify	Detect	Contain	Eradicate	Recover
Event Type	Access Control	Minimize Threat Recovery	Validate Removal Tactics	Identify Priorities and Map Recovery Plan
Business and Employee Impact	Threat Path	Reduce Threat Paths	Analysis Recovery Options—Backups	Communicate Risk
Stakeholders and Decision Makers	Logs	Apply Containment Tools	Start with Minimal Impact	Prioritize Recovery
Source	Alerts	Blocking	Removal	Protect for Future Incidents

Quest's IR Readiness Assessment & Playbook

Prepare for the eventuality of a cyberattack with a customized IR playbook. Quest's cyberdefense specialists will help create your IR Playbook, describing the available resources in your organization, the individuals with decision-making authority, the scope of that authority, and the consequences of any decisions they may have to make. This information is vital in the event of an attack.

As one of the most recognized cyber incident response companies, Quest's Readiness Assessment operates using a strategic 4-phased approach:

1 Assessment

- Security operations
- IR policies and procedures
- Logging
- Intelligence

2 Environment Prep

- Tailored to the organization
- Focus on tools and data/logs
- Review of current alerts
- Tuning and clean-up

3 Tabletop Exercise

- Focused on goals of the organization
- Tests existing capabilities
- Customized for your organization
- Identifies gaps and strengths

4 Foundation

- Findings and recommendations report
- Assistance with prioritization
- Defined interface with Quest IR team
- Assigned IR resource

Improve Incident Response Times

Quest's multi-tiered, strategic IR program enables you to improve security incident response times, effectiveness, and costs. In the chart below, you can find a list of the available tiers with a range of options and features suitable for your company.

Feature	IR T&M	IR Retainer	Readiness & Retainer	TOC
Service Level Agreements	Best Effort	1 hour by phone; 24 hours on-site	1 hour by phone; 24 hours on-site	4 hours by phone; 48 hours on-site
Service Model	T&M	12 month retainer	12 month retainer	12 month contract
Included IR Hours	Ad hoc per Rate Sheet	160 hours annual	160 hours annual	T&M
24/7/365 Access to Incident Responders	✓	✓	✓	✓
Needed Response Tools (Quest EPS, SIEM, DNS Security)	✓*	✓	✓	✓*
Incident Coordination, Containment, and Investigation	Per Incident (T&M)	✓	✓	Per Incident (T&M)
Log, Host, and Network-based Forensics as needed	Per Incident (T&M)	✓	✓	Per Incident (T&M)
Network Edge Vulnerability Scan	Per Incident (T&M)	Per Incident (T&M)	✓	Per Incident (T&M)
Annual 4-point Incident Response Readiness Assessment			✓	
I. Readiness Assessment			✓	
II. Environment Prep			✓	
III. Tabletop Exercise			✓	
IV. Final Report			✓	
Proactive Threat Hunting/Compromise Assessment	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)
Internal IR, SOC, and Forensic Team Builds/ Stand-up	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)
System Backup and Recovery	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)

* *SLA per Incident Response Time*

Endpoint Protection (EPaaS)

The surge in mobile device usage, coupled with bring-your-own-device (BYOD) policies and an increasing remote workforce, has amplified vulnerabilities in endpoints like desktops, laptops, smartphones, and tablets. Furthermore, the emergence of trends like the Internet of Things (IoT) has carved new pathways for cybercriminals to initiate advanced attacks on individuals and businesses. With an ever-expanding range of targets, the incessant wave of cyber threats has transcended what humans can manage alone.

Keep Your Devices Safe with Quest's Endpoint Protection as a Service

Quest's Endpoint Protection as a Service (EPaaS) uses artificial intelligence and machine learning to monitor your endpoints for threats. It maintains surveillance of events generated at each of your endpoints, looking for suspicious activity and addressing it immediately. Quest's EPaaS provides you with malware and virus protection and reliable security intelligence in real-time, shortening response times and delivering continuous threat monitoring. EPaaS allows your team to retain the tools they use to be productive while you protect your enterprise by keeping their devices safe.

AI & Machine Learning Deliver Fast Responses

Endpoint intrusions can operate at machine speed on the host device, outpacing the efforts of human defenders. To deal with this problem, Quest harnesses the latest technology to improve the efficacy of EPaaS. Predictive AI, machine learning, and Next-Generation Antivirus (NGAV) solutions increase speed, strengthen security operations, and improve your overall network safety. We deploy lightweight, ultra-fast artificial intelligence (AI) directly on client devices. Intrusions trigger fully automated security playbooks, which result in rapid, coordinated responses that stop malicious processes before they multiply.

Additionally, our EPaaS provides analysts with actionable information and corroborating evidence, which helps security operations analysts identify, investigate, and remediate. We can collect telemetry data on suspicious activity and enrich that data with information from related events. Through such functions, Quest's EPaaS can be instrumental in shortening incident response times and serve as the first step toward proactive, continuous threat hunting.

Quest's EPaaS Provides:

- AI-driven malware and virus protection
- 24/7 monitoring and alert notification
- Managed detection and response (MDR)
- Enterprise-wide threat hunting
- Memory exploitation prevention
- Device policy enforcement
- Script management
- Application control for fixed-function devices
- Context-driven threat detection
- On-demand root cause analysis
- Automated playbook-driven response
- Remote investigation and remediation

Flexibility Tailored to Your Operational Demands

At Quest, our Endpoint Protection as a Service (EPaaS) offering is more than just a service — it's a solution built with the dynamic needs of businesses in mind. Recognizing that no two enterprises have the same requirements, we've made our EPaaS as adaptable as possible. Whether you prefer deploying the service within your own infrastructure or wish to harness the capabilities of Quest's Service Delivery Centers, we have you covered. Choose between dedicated servers, ideal for businesses seeking unparalleled performance and security, or shared servers, perfect for those looking for efficient and cost-effective options. We're committed to ensuring that our EPaaS aligns perfectly with your business needs, ensuring a seamless integration into your existing workflow.

Monitoring & Alerting

It’s crucial to be able to trust that your company's IT infrastructure is protected and watched. Quest's 24/7 Monitoring and Alerting Services cover essential network maintenance and ensure continual updating, monitoring, and analysis to keep your organization's productivity at optimum levels.

Quest will monitor your environment in real-time and around the clock. With Quest's expert resources and sophisticated tools employed on your organization's behalf, you can trust in uninterrupted business operations and fast alerts.

We offer five categories of Monitoring and Alerting Services:

1. Server/Virtual Server Monitoring & Support

(24/7 Server/Virtual Server Monitoring & Support)

- Perform monitoring of server hardware and OS
- Automated patch monitoring, alerting, and support (OS)
- Minor configuration changes
- Remote HW/OS troubleshooting/remediation

2. Hypervisor Monitoring & Support

(24/7 Server/Virtual Server Monitoring & Support)

- 24/7 alert/performance monitoring of Hypervisor (per physical host)
- Automated patch monitoring, alerting, and support (Hypervisor)
- Minor platform point release installation
- Configuration changes
- Remote Hypervisor troubleshooting/remediation

3. Switch/WAN Monitoring & Patching

(24/7 Switch/WAN Monitoring & Patching)

- Perform monitoring of hardware and software environment
- Configuration backup
- Minor platform point release/patch installation
- Configuration changes
- Remote HW/SW troubleshooting remediation

4. Firewall/IPS Monitoring & Patching

(24/7 Firewall/IPS Monitoring & Patching)

- Perform monitoring of hardware and software environment
- Perform IPS event and UTM event monitoring
- Signature updates to IPS
- Configuration backup
- Minor platform point release/patch installation
- Configuration changes
- Remote HW/SW troubleshooting, remediation (security breach remediation not included)

5. UPS Monitoring & Patching

(24/7 UPS Monitoring & Patching)

- Perform monitoring of UPS hardware and OS
- Automated patch monitoring, alerting, and support (OS)
- Remote HW/OS troubleshooting/remediation

With Quest on the job, you can relax knowing your infrastructure is secure and your IT resources are positioned to help your business realize its financial and strategic objectives. Reinforce your workforce with Quest's cybersecurity expertise and sophisticated tools for network alerting, monitoring, and support on your side.

Patch Management (PMaaS)

Patching is a critical part of cybersecurity. It limits your firm's exposure to vulnerabilities, which minimizes risk and makes a world of difference in your defenses. Failure to patch your technologies and endpoints can lead to a security breach, creating legal liabilities, regulatory fines, and reputational damage.

However, an effective enterprise patching process requires intimate knowledge of your existing environment, as well as the flexibility to continuously evolve with your IT infrastructure. And each time something changes in your IT environment (such as new virtual machines, applications, or devices) you have a new set of patches to identify, evaluate, and deploy in a timely fashion.

As a result, it can be easy to find the patching process overwhelming, causing you to overlook it altogether — a choice that can lead to devastating consequences as cybercriminals take advantage of unpatched security gaps. Quest's Patch Management as a Service (PMaaS) can be the solution you need. It manages the cyclical patching process for you so you can focus on other critical business activities. With Quest's PMaaS, you'll have a team of experienced security experts on your side, reducing vulnerabilities one patch at a time.

Password Management as a Service (PWMaaS)

Reduce the risk of weak or compromised passwords with Password Management as a Service (PWMaaS), an innovative new addition to Quest's CyberDefense Suite. The cloud-based platform implements encryption and two-factor authentication (2FA) to safeguard password information, providing you with the essential tools to effectively manage organization-wide credentials and proactively increase security.

Quest's PWMaaS includes the following features:

- Encrypted Password Vaults
- Administrator Console
- Auto-Generated Complex Passwords
- Zero Trust Environment
- Real-Time Security Audits
- BreachWatch

Encrypted Password Vaults

Implement a separate, fully encrypted vault for each employee for secure password storage, protected by 2FA. The cloud-based platform is OS and device independent, ensuring that authorized individuals can access essential information whenever necessary.

Administrator Console

Reporting, auditing, and analytics/MDR integration capabilities are intuitively organized in a user-friendly console, streamlining security procedures and putting a proactive approach within easy reach.

Auto-Generated Complex Passwords

A single weak password can put your organization's most valuable data in danger. Password Keeper automatically generates appropriately complex passwords quickly and effectively, preventing the common mistakes that can be exploited by threat actors.

Zero Trust Environment

Lock down the internal control environment with strict enforcement policies and event reporting.

Real-Time Security Audits

Harness the power of data analytics via security audits that provide details of the password strength and date of the last password change for every relevant site. Receive an overall score to inform improvement efforts, using your knowledge of existing password issues to target critical areas.

Breachwatch

See exactly where your organization's biggest risks are located, including specific information about data breaches and each user's weak points. Benefit from clear, actionable steps to rapidly resolve at-risk records, eliminating vulnerabilities before cybercriminals can exploit them.

Security Information & Event Management (SIEM)

Long-term, low-key siphoning of sensitive information can indefinitely stay below the radar of IT and security teams. Your business could be suffering from a data breach without knowing it. Fortunately, there is a solution: SIEM. SIEM software continuously monitors the organization to collect and aggregate log data, then identifies, categorizes, and analyzes incidents and events. The software delivers on two main objectives: report on security-related incidents and events and send alerts if any activity violates established rulesets (meaning it might be a security issue).

SIEM systems have proven to be very useful in helping companies protect against advanced and persistent threats and remain compliant. The technology detects threats, attacks, and breaches early, allowing you to analyze security event data in real-time. SIEM has become one of the go-to cybersecurity solutions in recent years. However, it can be cost-prohibitive and overwhelming to stand up the infrastructure and resources needed to implement, monitor, and manage logs effectively.

Quest SIEM as a Service

Quest's managed SIEM as a Service (SIEMaaS) saves you from that infrastructure expense while improving the speed and accuracy of incident detection and response time to targeted attacks and breaches. You have no software to purchase and no need to hire cybersecurity professionals or provide any additional training to bring your staff up to speed.

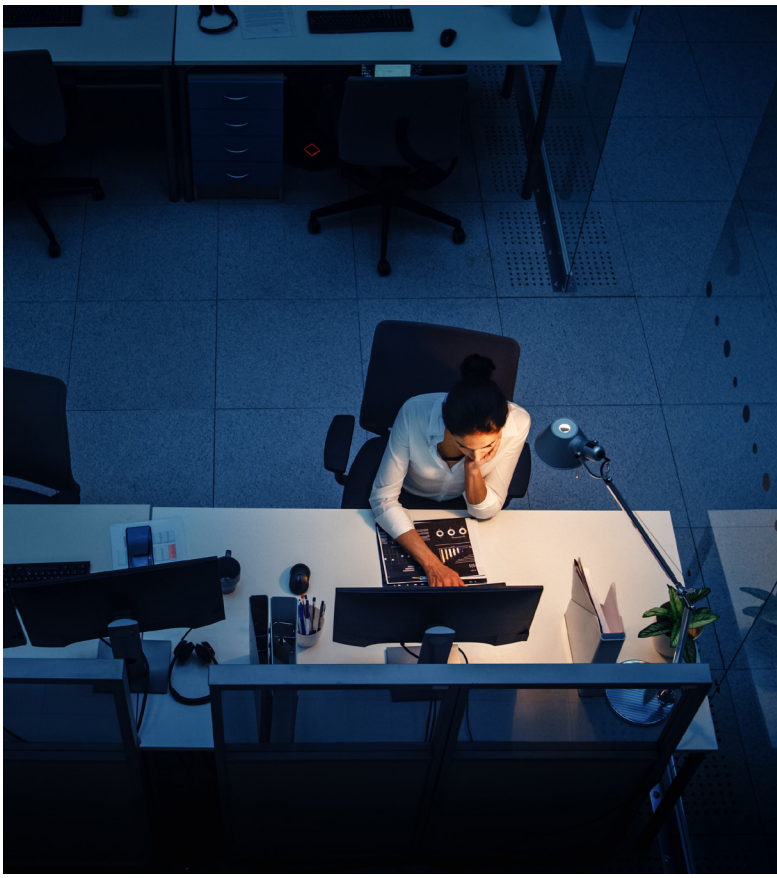
Quest experts handle the large-ticket items and the day-to-day SIEM operations on a subscription basis. The Quest team adapts to your environments and delivers the genuine actionable intelligence necessary to understand your threat posture and prioritize response quickly.

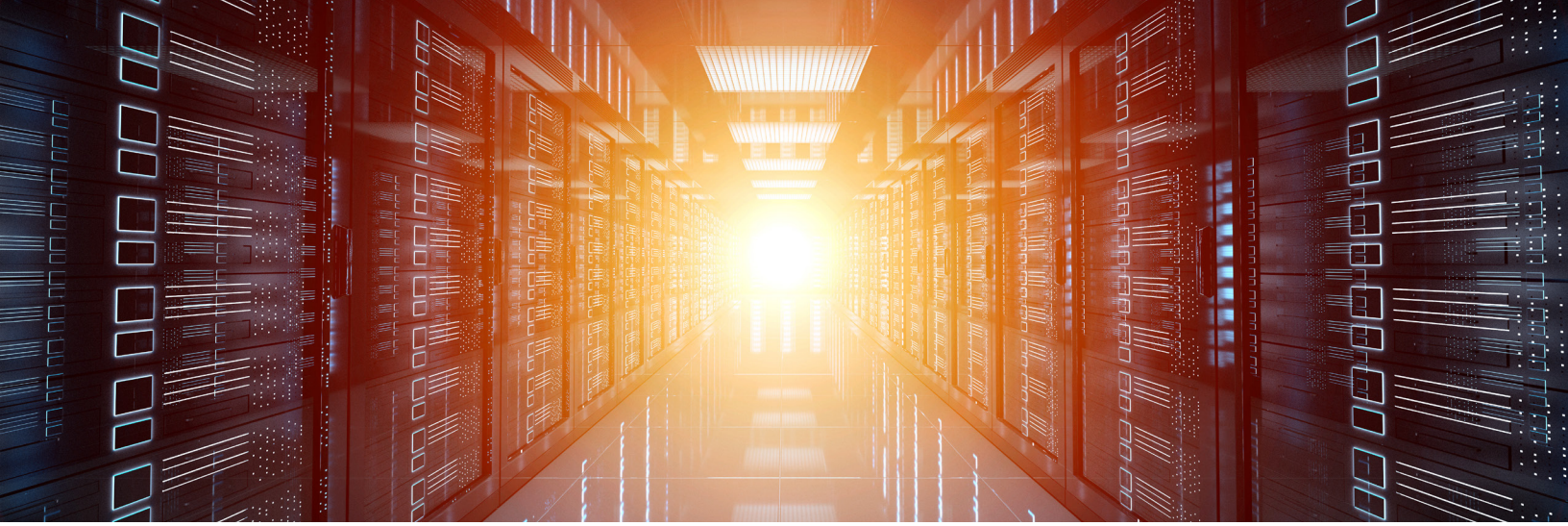
Quest's SIEM as a Service Features:

- Quick and easy detection of new threats
- Real-time event log correlation
- Integrated compliance management
- Augmented threat intelligence
- Network device auditing
- In-depth application auditing

Quest Can Also Customize Your SIEMaaS Solution With These Options:

- Log storage services beyond the 1 TB that is included
- Data replication (second copy) services
- Configuration of backups and endpoints
- Security, firewall, and ACL configuration review
- Incident Response (IR) and remediation services
- Data and/or application migration services





Data Protection (Immutable Storage)

Quest Offers Enterprise DPaaS: Without the Complexity

Even a single data loss incident can have devastating results, causing your business to suffer from monetary loss, negative publicity, and legal liability. To protect your business from breaches, exfiltration, and destruction of sensitive data, it is essential to put a data protection solution in place. You need to be able to discover, monitor, control, and secure sensitive data throughout the environment in real-time. To do this, you can use Data Protection as a Service (DPaaS).

As a complete enterprise-class cloud disaster recovery service, our DPaaS gives you full visibility into file and device activity on endpoints, along with email encryption that integrates with a broad range of encryption services. Quest's DPaaS can be deployed quickly and with no dedicated resources, and will provide the deepest data visibility and control to block suspicious insider activity or outsider attacks. We use the principle of zero trust and secure your data transparently and continuously, encrypting it at rest, in transit, or in use. Plus, we are agnostic to file type, data size, or application.

Transform your application access and achieve consistent data protection with Quest's next-generation DPaaS.

Cloud Zero Trust Network Access

Zero Trust: Secure Access: Anywhere, Anytime

An overwhelming 97% of employees say they want to continue to work remotely to some degree. Remote work introduces security concerns, though, as you can no longer be certain that every device that connects to your network is authenticated and behind a firewall. Traditional security approaches take advantage of your organization's firewall, filters, and other security measures by sending all data via a backhaul connection through a Virtual Private Network (VPN). With remote employees, partners, suppliers, and third-party contractors needing secure access to applications, the traditional approach doesn't work anymore.

What you need is Zero Trust Network Access (ZTNA), a cloud-based, multi-level security model that falls under the highly effective Secure Access Service Edge (SASE) security model. Quest's Cloud Zero Trust Network Access (Cloud ZTNA) services give you a smarter way to grant private application access to your users, whenever and wherever they need it. With Cloud ZTNA, you get a solution that is easy to use and manage, and is able to secure every endpoint in your network.

Quest's Cloud ZTNA services ensure frustration-free, uninterrupted, cloud-based access across your enterprise—all with a single login. It can mitigate security risks, reduce costs, eliminate delays, and keep your users productive. Policies are managed from a single hub, and can be continuously adapted based on external threats, user context, device posture, and more. Plus, you can easily grant access to third-party contractors, suppliers, and partners anytime. Even better, constant analysis of user behavior and application access opens a window into new insights for data-driven innovation.

Quest's Cloud ZTNA was engineered by experts who understand what your needs are—and how to address them. Quest Technology Management is well-equipped with the skill and expertise necessary to guarantee the total reliability, exceptional performance, and flexibility you need to move your business into the future.

Distributed Denial of Service (DDoS) Protection

DDoS attacks occur when multiple compromised devices are used to simultaneously flood a business or Internet Service Providers' (ISPs) network with traffic or server requests, rendering the system inoperable. DDoS cyberattacks cause significant damage to the finances, operations, and reputations of businesses worldwide. And because more devices are connecting to the internet every day, there is an increasing number of endpoints that cybercriminals can weaponize. In fact, **DDoS attacks are projected to rise to 15.4 million per year by 2023**. The majority of attacks last up to four hours and, according to Gartner, the average cost of IT downtime is $5,600 per minute. Add it up and a DDoS attack could cost a business as much as $336,000 for every hour of downtime.

To protect yourself against this threat, call on Quest's DDoS Protection Services.

Quest DDoS Protection Services

Quest can detect and mitigate DDoS attacks of any size and kind at the network edge, closest to the source of origin. This helps ISPs and businesses ensure that the performance of legitimate traffic is not impacted, which increases uptime and performance. Quest has a reliable infrastructure and an extremely competent and responsive team that is well-positioned to deflect even the largest of attacks. This offering is available from every Quest data center, using our global network and two fundamental networking protocols (BGP and GRE) for routing and encapsulation. Plus, it can be used for on-premise, cloud-hosted, and hybrid networks alike.

We inspect all customer traffic and can immediately apply advanced and automated mitigation techniques. Additional functions such as load balancing, next-gen firewall, content caching, and serverless compute are also delivered as a service.

Key Features

- Over 42 Tbps of network capacity
- Mitigate most attacks in under 10 seconds
- Sub-second threat detection
- Integrate via BGP routing and GRE encapsulation
- Native integration with L7 services (CDN, WAF, Bot Management, etc.)
- Always-on and on-demand options
- Support for all IP services (TCP, UDP, IPSec, VoIP, custom protocols)
- Advanced analytics

Email Security Suite

Quest Email Security Suite

Email is still the favorite attack vector for today's cybercriminals, and attacks are becoming increasingly sophisticated, fooling even the most cautious users. Protecting your organization means taking your email security to the next level.

That is where Quest's Email Security Suite comes in, strengthening your defenses against threats like imposter email, phishing, malware, spam, and bulk mail. Email Security Suite works with even the most complex enterprise deployments, including cloud, hybrid cloud, and on-premises installations with virtual or physical machines.

This is an easy-to-use, cloud-based solution that helps you secure and control both inbound and outbound emails. It uses multiple layers of technology to accurately detect threats, and can meet the needs of even the most complex enterprise deployments; Quest can support cloud, hybrid, and on-premises installations with virtual or physical appliances. Features include dynamic reputation analysis, multilingual analysis, quarantine options, granular control, big data analysis, flexible policy creation, email continuity and sync, message tracing, reporting, and end user controls.

Quest Email Security Suite Packages

Quest offers three tailored packages to meet the needs and budget of your organization.

Features	Business	Advance	Professional
SECURITY			
Antivirus	✓	✓	✓
Spam Filtering	✓	✓	✓
Reporting	✓	✓	✓
Content Filtering	✓	✓	✓
Outbound Filtering	✓	✓	✓
Imposter Email Protection	✓	✓	✓
Data Loss Prevention	✓	✓	✓
URL Defense (Sandboxing)	✓	✓	✓
Attachment Defense (Reputation)	✓	✓	✓
Attachment Defense (Sandboxing)		✓	✓
Email Encryption		✓	✓
Social Media Account Protection		✓	✓
CONTINUITY			
Emergency Inbox	30 days	30 days	30 days
Email Spooling	30 days	30 days	30 days
Instant Replay	30 days	30 days	30 days
EMAIL ARCHIVE			
Unlimited Storage			✓
Configurable Retention (up to 10 years) and Legal Hold			✓
Powerful Search and Discovery Tools			✓
End-user Search Access			✓
EMAIL THREAT EDUCATION — ADDITIONAL			
Unlimited Phishing Security Tests			
Security "Hints and Tips"			
Assessments			
Phishing Reply Tracking			
Email Integration			
Industry Benchmarking			
MANAGEMENT — ADDITIONAL			
Multi-level Logins			
Domain Management			
Email Logs			
Active Directory Sync			
Azure Active Directory Sync			

Cyber Risk Monitoring & Management

From top-level executives to IT leaders, the concern for maintaining a company's good standing is universal. If you want to protect yourself against cyber threats and preserve your brand's credibility, Quest is ready to help by offering cyber risk monitoring and management. This is a strategic, ongoing approach that combines visibility with action, keeping a close eye on your public perception while minimizing threats (such as data breaches) that could compromise your integrity and trustworthiness. Our expert team performs an in-depth risk assessment to identify potential vulnerabilities in your cybersecurity systems and processes, letting you make informed decisions about where to focus your risk mitigation efforts.

Cyber risk monitoring and management has evolved into a comprehensive, in-depth process that encompasses many components, including monitoring, reporting, risk management, vulnerability management, and threat response. Quest can provide all these services, helping you feel confident in your reputation and security.

Why Do You Need Cyber Risk Monitoring & Management Services?

Cyber risk monitoring and management services protect your business from the financial consequences of cyber security threats. Organizations must prioritize visibility regarding risks. You must identify and promptly address any significant changes that may arise to ensure their continued success.

- Cybersecurity insurance costs have increased significantly by 50-100%. It is crucial to prioritize optimal protection as investments in insurance continue to rise.
- Insurance companies have clear expectations for coverage to organizations. They require detailed information that demonstrates the proper precautions have been taken.
- The immense amount of data shared across various channels, directly and through third parties, increases vulnerabilities.

Besides these issues, the threat of ransomware deserves special mention. These attacks have been growing more popular, and can set you back $4-5 million, which poses serious financial risks for your business. Even worse, "ransomware as a service" (RaaS) is now available, making it even easier for cybercriminals to strike. To effectively counter this kind of evolving and devastating threat, cybersecurity strategies must be dynamic alert, and comprehensive. Taking proactive measures to safeguard your data and ensure uninterrupted business operations is imperative — and reputation monitoring is a part of this strategy, thanks to the way it improves your visibility and enhances your response efforts.

Cyber Risk Monitoring & Management Services

Security is never one-size-fits-all, which is why we make it simple to customize services based on your key objectives. Options include:

- 24/7 monitoring, monthly reports, or one-time assessments
- Optional tracking for competitors, suppliers, partners, and/or potential acquisitions
- Personalized technical resources
- Industry-based comparisons
- Tailored security recommendations, including specific action steps for remediation

Next, let's take a closer look at Quest's service offerings:

Third Party Risk Management (TPRM)

Ensuring the security of your business should always be a top priority. It is imperative to remain vigilant and proactively identify potential security threats among partners, consultants, vendors, and customers. You can safeguard your business from these risks by taking necessary precautions and implementing robust security measures.

Security Rating Services (SRS)

You need a clear understanding of your cybersecurity stance, particularly compared to competitors. This knowledge will help you identify potential vulnerabilities or weaknesses in your systems and take necessary measures to strengthen them. Assessing and improving your cybersecurity measures helps you to stay ahead of the competition and protect your data from threats.

Risk Management

An exemplary security rating and a proactive approach to reputation management services can help with client relationships. This will nurture your current client base and attract potential clients to develop long-lasting and fruitful partnerships.

Reputation Monitoring

As a leader, you should understand how stakeholders view and interact with your organization. This includes your competitors, partners, customers, and threat actors so you understand vulnerabilities.

Online reputation monitoring services include:

- Monitoring
- Reporting
- Risk Management
- Vulnerability Management
- Threat Response
- Mapping to specific partners
- Managing risk with all internal and external partners

To protect your organization effectively, you need a holistic approach to cyber risk monitoring and management. Without it, your company becomes significantly vulnerable when other organizations strengthen security measures.

Assessing Cyber Insurance Protection

Part of our cyber risk monitoring and management services includes reviewing your cyber insurance policy, letting you ascertain your exact level of coverage, understand whether it aligns with your current risk profile, and maintain compliance with policy conditions. Complying with the policy and ensuring sufficient coverage during a cyberattack is essential, so we want to make sure coverage aligns perfectly with your unique risk profile. We offer valuable guidance for staying compliant, including conducting regular security assessments, implementing necessary security measures, and promptly reporting incidents. Taking these steps will help protect your business from potential financial losses and mitigate the damage caused by such incidents.

Info Collection for Monitoring & Assessments

Quest uses open-source intelligence (OSINT) techniques to conduct non-intrusive scans. False positives are no longer a problem, thanks to standard scoring models such as the MITRE Cyber Threat Susceptibility Assessment (CTSA), Common Weakness Risk Analysis Framework (CWRAF), and Common Vulnerability Scoring Systems (CVSS). With access to massive IP & Domain Whois databases, as well as an authorized IP zone transferer, our system can utilize over a billion historical items, as well as every company-related domain name and IP address. All this data is assessed and compiled into an easy-to-read report, using a letter-grade approach to determine potential risks and translate technical information into relevant business concepts.

Safeguard Your Reputation Today & Tomorrow

Navigating the ever-evolving complexities of cybersecurity can be challenging, but with Quest's cyber risk monitoring and management services, you do not have to face them alone. We provide the expertise and tools necessary to identify, assess, and mitigate your cybersecurity risks. Our expert team diligently conducts risk assessments to thoroughly analyze all potential threats to your business, including ransomware, phishing, insider attacks, and any other hazards specific to your industry. With our comprehensive analyses of vulnerabilities in your cybersecurity infrastructure, you'll learn about potential threats and your level of preparedness to handle them, helping you make informed decisions about risk mitigation strategies. Do not leave your organization's reputation and financial stability to chance — be proactive, understand your risk landscape, and secure your peace of mind with our help.

Ransomware Assessment

Ransomware attacks are an especially dangerous type of attack. They lock your data away and demand the payment of a ransom in order to unlock everything. Without proper precautions, you may be forced to pay this ransom—but there is no guarantee the attackers will uphold their end of the deal. Making matters worse, these kinds of attacks are growing more common at an alarming rate, and each one can pose a unique risk and require a different approach.

To protect yourself against these kinds of attacks, call on Quest. We offer comprehensive ransomware assessments that cover multiple areas, providing you with the info you need to set up strong defenses and know how to recover from ransomware attacks.

Cybersecurity Awareness Training & Workshops

Today, ensuring security goes beyond technology alone; organizations must also confront the human element of risk. The people in your company can make or break your cybersecurity efforts: those who lack training and knowledge of cybersecurity can become weak links in the “human firewall”, potentially allowing cyberattacks to occur by accident. In fact, over 90% of successful hacks and data breaches start with phishing scams, a type of attack that preys on untrained people who are not well-informed of cyber threats.

Education is the answer to this problem, and Quest can give your people the training they need. Powered by KnowBe4, Quest’s SaaS-based Cybersecurity Awareness Training provides your employees with focused security awareness training and messaging that teaches them to recognize and avoid cyber threats. Employees who undergo regular training learn to make smarter security decisions every day. Engaging Quest to provide your company with cybersecurity awareness training is a critical step in protection—and you can count on Quest to handle every detail of your training program so you can focus on your business. You will finally have a platform to better manage the urgent IT security problems of social engineering, spear- phishing, and ransomware attacks and at the same time stay compliant with industry regulations.

The training program includes:

- Baseline testing using mock attacks
- Engaging interactive web-based training
- Continuous assessment through simulated phishing, vishing (video), and smishing (SMS) attacks
- Actionable metrics and insight into the effectiveness of your awareness training program through advanced reporting using machine learning technology

Subscription Levels

Quest offers four levels to meet the needs of your organization and the depth of information you would like to deliver:

Silver: Includes the Kevin Mitnick Security Awareness Training module and unlimited simulated phishing tests, assessments, and enterprise-strength reporting.

Gold: Includes all Silver level features plus industry regulation compliance training modules. Gold also includes monthly email exposure check reports and vishing security tests using IVR attacks over the phone.

Platinum: Includes all features of Silver and Gold, plus advanced phishing features: Smart Groups, reporting APIs, user event API, security roles, and landing page social engineering indicators.

Diamond: Includes all features of Silver, Gold, and Platinum plus full access to the extensive library of interactive modules, videos, games, posters, and newsletters. In addition, access to AI-driven simulated multi-faceted social engineering attack using email, phone, and SMS messaging.

In addition to these four levels of cybersecurity awareness training, Quest offers KnowBe4's PhishER and KCM GRC. PhishER can be a stand-alone product or an optional add-on, and includes a lightweight Security Orchestration, Automation, and Response (SOAR) platform that can automate your threat response and manage the high volume of potentially malicious messages reported by your users. Meanwhile, KCM GRC is a standalone product that helps cut down audit time and effectively manage risk, enabling organizations to comply with regulations like PCI-DSS, HIPAA, CCPA, FedRAMP, SOX, FFIEC, and GLBA.

These solutions are designed to fit your needs. Our team will get your training courses up and running quickly and provide expert guidance and support to help your team get the greatest ROI out of the experience.

Subscription Level Comparison

Features	Silver	Gold	Platinum	Diamond
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program (ASAP)	✓	✓	✓	✓
Security "Hints and Tips"	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Assessments	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration (ADI)	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Crypto-Ransom Guarantee	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓
Smart Groups			✓	✓
Reporting APIs			✓	✓
User Event API			✓	✓
Security Roles			✓	✓
Social Engineering Indicators (SEI)			✓	✓
USB Drive Test			✓	✓
Priority Level Support			✓	✓
Training Access Level III				✓
AIDA™ Artificial Intelligence-driven Agent				✓
PhishER™ — Optional Add-on	✓	✓	✓	✓

Cybersecurity Workshop

There are countless threats waiting to prey on your organization, including bad actors, viruses, ransomware, disgruntled employees, social engineers, phishing attempts, and more. To defend against all these hazards, you need to review your security concerns, assess your current security posture, and receive smart recommendations tailored to your organization. This is where Quest can help. In Quest's Cybersecurity Workshop, certified IT experts will gauge your level of vulnerability to these types of threats and others, giving you the information you need to defeat the cyber threats lurking around you.

Cybersecurity Workshop Overview

To determine your unique risk factors, Quest will assess your current security posture and review your existing security measures and/or compliance requirements. Since business risk extends beyond the IT department, your biggest threat could be from porous work processes, or even employees that are untrained in basic security measures like avoiding phishing emails. After our assessment, we will create recommendations that are specifically designed for you, addressing and prioritizing your security concerns, requirements, and goals. Recommendations may include topics such as tech configurations, security policies, compliance requirements, and resource optimization. In addition, we will provide an executive summary complete with documentation. Overall, our workshop will help you take the first step toward a more confident and secure business future.

Risk Management Workshop

With Quest's risk management workshop, you can identify your unique business risk factors and explore mitigation options. We'll take an executive look at your organization to uncover risk beyond the IT department, such as undocumented policies and processes or gaps between recovery expectations and capabilities. The workshop walks you through all the factors to identify key solutions that will help you mitigate risk, align with industry standards and compliance regulations, and streamline your business continuity. Plus, we will provide recommendations that are tailored to your organization.

Our experts will take a deep dive into the areas of your organization where you would like to focus and offer an expert business perspective that keeps your bottom line in mind. We can concentrate on any number of the following:

- Business Impact Analysis
- Business Continuity
- Security Management
- Mitigation Strategies
- Crisis Communication and Management
- Disaster Recovery
- Process Management

How can we help?®

www.questsys.com
1.800.326.4220

Quest TECHNOLOGY MANAGEMENT