FORTRA™

SOLUTION BRIEF (ALERT LOGIC)

Achieving NIST 800-171 Compliance

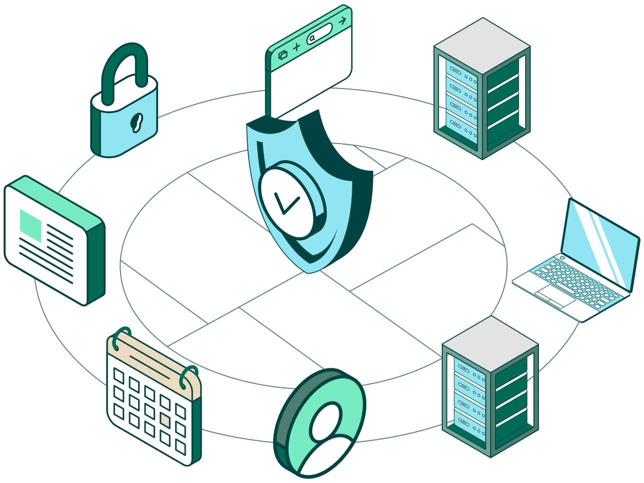
Like many compliance mandates, ensuring your organization meets NIST 800-171 guidelines can be a heavy lift for experienced security professionals and an overwhelming responsibility for those businesses with limited staff with minimal security experience.

The National Institute of Standards and Technology Special Publication 800-171 – known by most as NIST 800-171 – is a set of standards and guidelines that all organizations that work with a U.S. federal agency must follow in order to be considered for government contracts as set by the Federal Information Security Management Act (FISMA). With NIST 800-171, the standards and processes protects information that is sensitive but not categorized as "classified." If your organization processes, stores, or transmits Controlled Unclassified Information (CUI) data for most federal and even state agencies, NIST 800-171 compliance is non-negotiable.

Even if your organization is not required to comply with NIST 800-171, it provides a solid blueprint for establishing an IT cybersecurity program with the framework for addressing: access control, audit and accountability, configuration management, identification and authentication, incident response, risk assessment, security assessment, and system integrity.

A proactive compliance strategy for NIST 800-171 ensures your organization is ready for any potential audit and can answer current or future customers' questions. With Fortra's Alert Logic MDR, meeting NIST 800-171 compliance is within reach through our cost-effective, managed solution that provides asset discovery, vulnerability assessment, and threat detection. Our team of experts will quickly help you understand your current state of compliance and help you map to NIST 800-171 standards. With Alert Logic MDR, you can:

- Support your NIST 800-171 compliance program with a team who are highly experienced in implementing security controls
- Protect customer data from network and OWASP Top 10 attacks with a robust vulnerability library and access to security consultants 24/7 to keep data safe
- Prepare for audits, anytime with audit-ready guidance and preparedness reporting that helps your IT staff stay one step ahead of requirements, mandates, and auditors
- Implement NIST 800-171 best practices with informed advice and remediation steps from our security experts
- Free up internal resources with comprehensive log review and threat monitoring from our 24/7 Security Operations Center
- Improve your organization's security posture, and reduce attack surface and risk of data breach



Alert Logic NIST 800-171 Solutions Mapping

Alert Logic’s integrated services address a broad range of NIST 800-171 to help you prevent incidents that threaten the security, availability, integrity, and privacy of your customer’s data.

FORTRA’S ALERT LOGIC MDR SOLUTIONS	NIST 800-171
Fortra’s Alert Logic MDR Essentials **Vulnerability & Asset Visibility** • Asset Discovery • Vulnerability Scanning • Cloud Configuration Checks • Endpoint Detection • Threat Risk Index • Compliance Scanning & Reporting	• Audit & Accountability • Configuration Management • Risk Assessment • Security Assessment • Systems & Communications Protection • Systems & Information Integrity
Fortra’s Alert Logic MDR Professional (includes Essentials) **24/7 Managed Threat Detection & Incident Management** • 24/7 Incident Monitoring & Management • Security Analytics & Threat Intelligence • Log Collection & Monitoring • Intrusion Detection • Security Event Insights & Analysis • Office 365 Log Collection & Search • Cloud Vendor Security Integrations • AWS User Behavior Anomaly Detection • Anti-virus Integration • File Integrity Monitoring	• Access Control • Audit & Accountability • Configuration Management • Identification & Authentication • Incident Response • Risk Assessment • Security Assessment • Systems & Communications Protection • Systems & Information Integrity
Fortra’s Alert Logic MDR Enterprize (includes Professional) **Designated Security Expert** • Continuous Threat Hunting • Proactive Tuning & Sensor Optimization • Security Review	

NIST 800-171	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE
3.1 Access Control			
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.		●	●
3.1.8 Limit unsuccessful logon attempts.		●	●
3.1.11 Terminate (automatically) a user session after a defined condition.		●	●
3.1.12 Monitor and control remote access sessions.		●	●
3.3 Audit and Accountability			
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	●	●	●
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	●	●	●
3.3.3 Review and update audited events.		●	●
3.3.4 Alert in the event of an audit process failure.		●	●
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.		●	●
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.		●	●
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.		●	●
3.4 Configuration Management			
3.4.3 Track, review, approve/disapprove, and audit changes to information systems.	●	●	●
3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	●	●	●
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	●	●	●

NIST 800-171	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE
3.5 Identification and Authentification			
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.		●	●
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.		●	●
3.6 Incident Response			
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.		●	●
3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.		●	●
3.11 Risk Assessment			
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	●	●	●
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	●	●	●
3.12 Security Assessment			
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	●	●	●
3.13 System and Communications Protection			
3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	●	●	●
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).		●	●

NIST 800-171	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE
3.14 System and Information Integrity			
3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	●	●	●
3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.	●	●	●
3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.	●	●	●
3.14.4 Update malicious code protection mechanisms when new releases are available.	●	●	●
3.14.5 Perform periodic scans of the information system, and real-time scans of files from external sources as files are downloaded, opened, or executed.	●	●	●
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		●	●
3.14.7 Identify unauthorized use of the information system.		●	●

Alert Logic maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including PCI DSS 3.2 Level 2 Audit, AICPA SOC 2, Type 2 Audit, and ISO 27001-2013 certification for UK operations.

For more information, please visit **AlertLogic.com**

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.