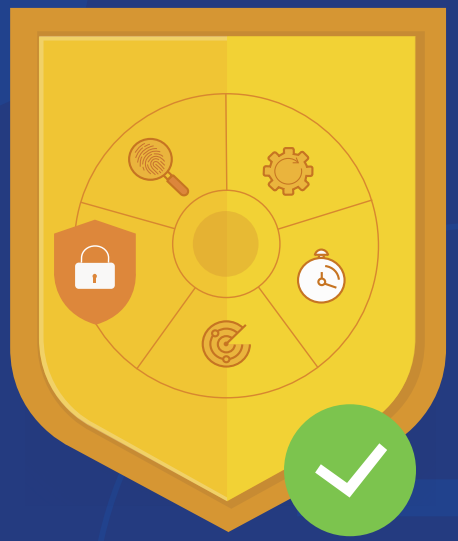
ManageEngine's guide to implement the NIST Cybersecurity Framework



ManageEngine

Table of content

Disclaimer

This material and its contents are intended, among other things, to present a general overview of how you can use ManageEngine's products and services to implement the NIST Cybersecurity Framework in your organization. Full implementation of the NIST Cybersecurity Framework requires a variety of solutions, processes, people, and technologies. The solutions mentioned in this material are some of the ways in which IT management tools can help with some of the NIST Cybersecurity Framework implementation.

Coupled with other appropriate solutions, processes, and people, ManageEngine's solutions help organizations implement the NIST Cybersecurity Framework. This material is provided for informational purposes only and should not be considered as legal advice for implementing the NIST Cybersecurity Framework. ManageEngine makes no warranties, express, implied, or statutory, and assumes no responsibility or liability as to the information in this material.

The NIST Cybersecurity Framework

With the evolving cybersecurity threat landscape, organizations are racing to find and implement effective cybersecurity solutions that help them manage and mitigate security risks preemptively.

The National Institute of Standards and Technology (NIST) developed a framework that could bolster the critical infrastructure of the US, as per the Cybersecurity Enhancement Act of 2014. The framework was originally imagined as a cybersecurity risk management system for the critical infrastructures of the US.

Today, it has been widely implemented in private and public sectors across organizational departments and around the globe. Organizations, regardless of their size and industry, can leverage the best practices outlined in the framework to understand, manage, and mitigate the cybersecurity risks associated with their data and networks.

The NIST Cybersecurity Framework offers guidelines and standards to manage cybersecurity risks across an entire organization or its critical infrastructures. The framework offers organizations a flexible, repeatable, and cost-effective approach towards managing their unique cybersecurity risks on a voluntary basis.

The benefits of implementing the NIST Cybersecurity Framework

- **Strengthen cybersecurity posture:**
  Organizations can discover their current security posture and prioritize opportunities to strengthen it by taking guidance from the informative references outlined in the framework.

- **Measure organizational risks:**
  Assess risks objectively and formulate an action plan considering the budget and resources available to bring risks within tolerance levels.

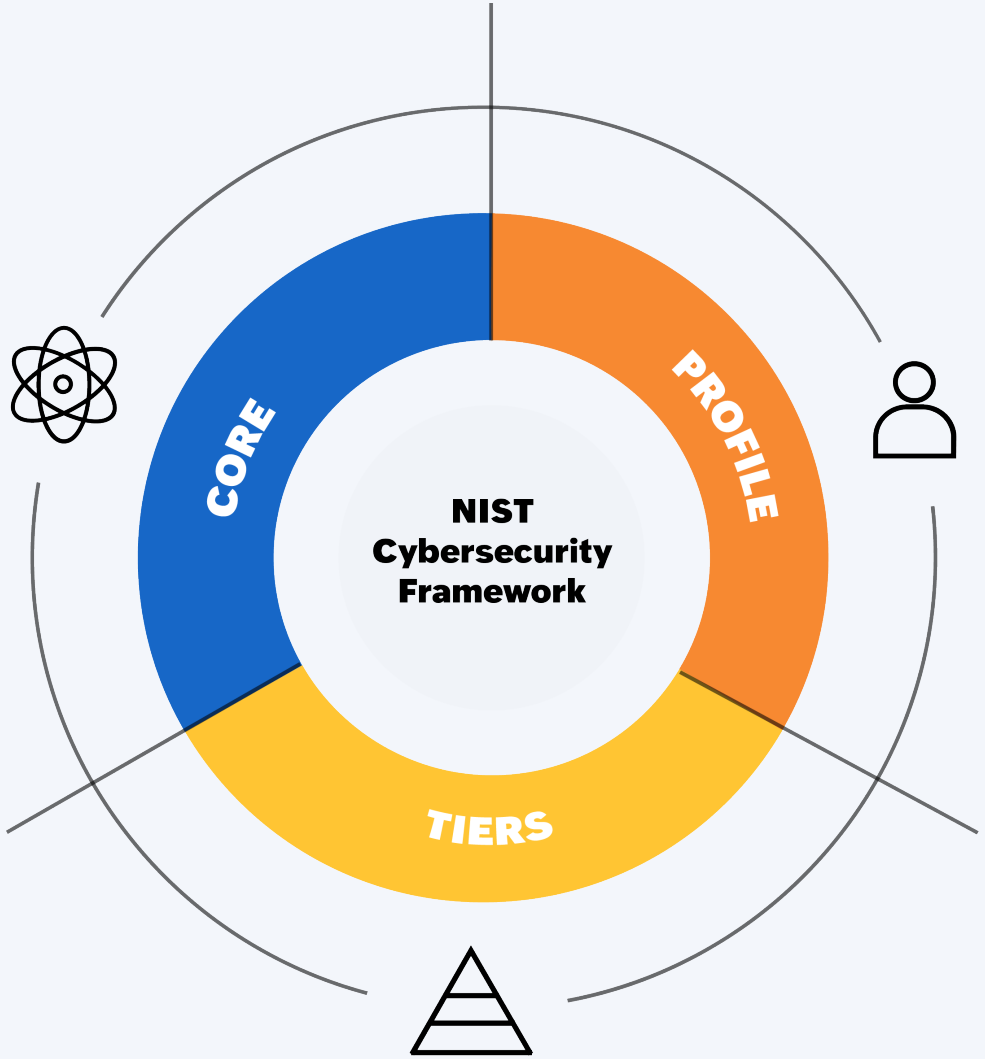
- **Comply with global standards:**
  Comply with other existing global standards and mandates easily, as the framework references multiple standards for its implementation.

- **Maximize ROI:**
  Focus on critical service delivery components to make the implementation process cost-effective by rethinking the prioritization of resources.

- **Communicate effectively:**
  The framework provides common language to convey cybersecurity risks and requirements to the stakeholders inside and outside the organization.

- **Expand the scope of risk management:**
  Ensure the products and services from external stakeholders meet critical security outcomes.

Components of the framework



Framework core

The framework core consists of key risk management activities that pave the way for organizations to realize cybersecurity outcomes that align with their business objectives and priorities. This outcome-driven approach allows for tailor-made action plans to meet business requirements.

The core is comprised of six concurrent functions and offers a holistic strategy to understand potential security threats, mitigate their impact, and recover from any business disruptions.

- **Govern:** Establish and communicate the organization's risk management strategy and policy.
- **Identify:** Understand and identify important systems, people, assets, and data and their associated risks to manage cybersecurity.
- **Protect:** Implement appropriate safeguards to protect the critical infrastructure and resources of an organization.
- **Detect:** Monitor systems continuously to discover the occurrence of a cybersecurity incident or anomaly promptly and analyze it.
- **Respond:** Take actions against a detected cybersecurity attack and limit its impact.
- **Recover:** Ensure business continuity and undertake recovery activities to restore affected business operations.

Functions are not meant to be a serial path to a desired state but to be performed concurrently and continuously to develop an organizational culture that addresses emerging cybersecurity risks.

Framework
implementation tiers

The implementation tiers illustrate the degree to which an organization's established cybersecurity program reflects the characteristics outlined in the framework. It helps in understanding the scope of cybersecurity practices established to manage risks.

The tiers are not maturity levels. Organizations should move towards a higher tier if the desired tier level aligns with their business goals and when they have the resources and budget to reduce their cybersecurity risks.

Tier 1: Partial	Tier 2: Risk informed	Tier 3: Repeatable	Tier 4: Adaptive
Irregular, reactive risk management practices with limited awareness of cybersecurity risks	Some awareness of cybersecurity risks but limited establishment of a risk management program at an organizational level	A consistent cybersecurity risk management program across an organization with processes to respond based on changes in the threat landscape	An advanced response system capable of effectively improving its risk management program based on previous incidents and predictive indicators

Framework profile

The framework profile represents an organization's desired target cybersecurity posture. An organization can develop its profile by selecting all the most important outcomes based on its business goals, risk tolerances, and resources from the categories and subcategories of the framework core.

By creating a current profile and comparing it with the target profile, organizations can identify opportunities to improve their cybersecurity program. Based on the priority and estimated cost of the corrective efforts, organizations can plan for cybersecurity improvement measures.

Organizations can use the framework profile to communicate the cybersecurity requirements that their partners and external stakeholders, who deliver critical products and services, need to meet in order to keep their supply chain secure.

How can ManageEngine help you implement the NIST Cybersecurity Framework?

While the NIST Cybersecurity Framework consists of technical and non-technical controls to manage cybersecurity risks, we can help you implement the technical aspects of it.

Govern:

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Category	Description	How ManageEngine solutions can help you
Organizational Context (GV.OC): The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood.	**GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed.	**Log360:** Simplify compliance management with audit-ready report templates for the PCI DSS, HIPAA, FISMA, the CCPA, the GDPR, and more. **AD360:** Meet compliance requirements with exclusive compliance reports for SOX, HIPAA, the PCI DSS and more. **PAM360:** Generate compliance reports periodically or on-demand based on pre-built templates for the PCI DSS, the ISO/IEC 27001, NERC-CIP, and the GDPR to assist in compliance audits. **Endpoint Central:** Generate custom reports on users, computers, groups, OUs, and domains. Schedule predefined reports, query reports, and custom reports in specific formats like CSV, XLS, and PDF for various compliance audits like HIPAA, the CIS, the GDPR, the DPDPA, and more.
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	**ServiceDesk Plus:** Set SLAs and OLAs with the accountable stakeholders for business critical services.

Category	Description	How ManageEngine solutions can help you
Risk management strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.	**GV.RM-06:** A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	**Endpoint Central:** Prioritize patches strategically with customizable risk profiles and automated assessment, ensuring effective risk management.
Roles, responsibilities, and authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	**GV.RR-02:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	**PAM360:** Allow the workforce, third-party stakeholders, and external vendors to access organizational resources securely. **Endpoint Central:** Map users to customizable roles with a prescribed set of activities and access permissions based on the requirements.
	GV.RR-04: Cybersecurity is included in human resources practices.	**AD360:** Streamline deprovisioning of user accounts and mailboxes through automatic approval workflows once the employee status changes.
Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced.	**GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	**Endpoint Central:** Enforce cybersecurity policies effectively with robust mechanisms, including comprehensive compliance monitoring and audit processes.

Category	Description	How ManageEngine solutions can help you
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	**GV.OV-03:** Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments as needed.	**Log360:** View the risk posture of Active Directory and SQL Server. Assess the degree of risk to help adjust the strategy. **ServiceDesk Plus:** Set up security incident management dashboards to add more context to risk management performance evaluations.
Cybersecurity supply chain risk management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.	**GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	**ServiceDesk Plus:** Map roles with granular permissions across various stages of the security incident resolution process.
	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	**ServiceDesk Plus:** Collaborate with both internal and external stakeholders during incident management.
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.	**Log360:** Set up alert profiles to get instantly notified when a string of events that are indicative of a supply chain attack occur and automate incident response with custom workflows

Identify:

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Category	Description	How ManageEngine solutions can help you
Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-01:** Inventories of hardware managed by the organization are maintained.	**Asset Explorer:** Discover IP-based devices within the organization with agent-based (Windows, Linux, and macOS) and agentless mechanisms. **Endpoint Central:** Manually enroll, automate the process, or allow users to self-enroll their mobile devices. Control corporate network access by ensuring only enrolled devices are granted permissions. Maintain full visibility with a comprehensive inventory of all managed endpoints in the network. **Network Configuration Manager:** Keep track of devices in the network and their device specifics, such as serial numbers, interface details, port configurations, and hardware specifics. **Analytics Plus:** Correlate data from asset and endpoint management applications to create a single source of truth that provides extensive insights into every resource's overall health, patch status, password compliance, associated users, license status, and any associated risk.
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	**Asset Explorer:** Get complete visibility into the software installed in your network, and keep track of purchased software licenses. **Endpoint Central:** can networks periodically to fetch the installed software details.
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	**Asset Explorer:** Establish and map data flows between assets, applications, documents, and people with the help of a CMDB.

Category	Description	How ManageEngine solutions can help you
		ServiceDesk Plus: Map pending requests, issues, and changes raised to their respective configuration items using a CMDB. **DataSecurity Plus:** Locate sensitive personal data within files and catalog it.
	ID.AM-04: Inventories of services provided by suppliers are maintained.	**DataSecurity Plus:** Monitor internal and external cloud applications and gain visibility into the encrypted network traffic of your organization. Catalog and analyze the browsers used to access cloud applications. **Cloud Security Plus:** Gain visibility into your AWS, Azure, and GCP cloud infrastructures through comprehensive reports and customizable alerts.
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	**PAM360:** Access business-critical resources securely as per assigned privilege level. Classify critical and business-value resources using a CMDB. **AD360:** Identify user record changes in the HRMS database and automatically modify corresponding user data in Active Directory. **Endpoint Central:** Streamline policy enforcement by configuring policy settings to restrict user actions and application access. Restrict access based on assigned user privileges tailored to specific departments or roles.

Category	Description	How ManageEngine solutions can help you
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles.	**PAM360:** Gain complete visibility and control over the life cycle of enterprise SSL and TLS. Discover, consolidate, create, deploy, renew, and manage digital keys and certificates within the enterprise network. **ServiceDesk Plus:** Build visual asset life cycles to automate the entire asset journey from procurement to expiration. **Endpoint Central:** Automate the entire management life cycle of digital assets from deployment to decommissioning with real-time asset tracking, automated patch management, and compliance audits.
Risk assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization.	**ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded.	**AD360:** Detect and analyze security risks in AD and M365 environments, such as failed logon attempts, file access, role changes, and license modifications. **Vulnerability Manager Plus:** Discover, assess, and prioritize vulnerable endpoints in your network. **Cloud Security Plus:** Monitor the log data from AWS, Azure, and GCP cloud infrastructures to identify security threats. **PAM360:** Detect certificates that are susceptible to SSL/TLS vulnerabilities, such as POODLE, Heartbleed, etc.

Category	Description	How ManageEngine solutions can help you
	ID.RA-02: Cyberthreat intelligence is received from information-sharing forums and sources.	**Log360:** TAXII, and AlienVault Open Threat Exchange (OTX) threat feeds to discover malicious IPs, domains, and URLs. **Vulnerability Manager Plus:** Prioritize vulnerabilities and respond to threats based on current exploits reported in the latest news feeds.
	ID.RA-03: Internal and external threats to the organization are identified and recorded.	**Log360:** Detect malicious software, services, and processes on endpoints and servers. Mitigate insider threats and account compromise with UEBA. Maintain a tamper-proof log archive to ensure log data from Windows, syslogs, and other applications is secured for future forensic analysis and audits. Log360 provides an advanced threat detection and incident response (TDIR) engine known as Vigil IQ that help organizations identify, navigate, and investigate threats. **Vulnerability Manager Plus:** Identify all the assets in the network and perform agent-based scans periodically to uncover emerging vulnerabilities, network misconfigurations, high-risk software, active ports, and more. **Firewall Analyzer:** Analyze firewall security logs to identify network breach attempts and attacks such as viruses, a Trojans, and denial-of-service attacks. **PAM360:** Allow administrators to shadow remote sessions of privileged users and detect abnormal behavior. Access recordings and audit logs of previous remote sessions to analyze and detect anomalous behavior.

Category	Description	How ManageEngine solutions can help you
	ID.RA-04: Potential impact and likelihood of threats exploiting vulnerabilities are identified and recorded.	**Site24x7:** Predict outages for critical infrastructures and discover their business impact with the help of AI and ML. **OpManager:** Gain insights and predict resource utilization on your network devices through forecast reports. **Vulnerability Manager Plus:** Identify vulnerabilities along with their context, such as CVSS and severity scores, to ascertain priority, urgency, and impact. Utilize built-in patching to remediate vulnerabilities instantly.
	ID.RA-05: Threats, vulnerabilities, likelihood, and impact are used to understand inherent risk and inform risk response prioritization.	**Vulnerability Manager Plus:** Scan the assets in your networks to identify OS, third-party application, and zero-day vulnerabilities. Understand the impact of the threats through the severity ranking dashboard.
	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	**PAM360:** Assign trust scores to users and devices based on their security compliance, and use policy-based access controls to process requests automatically and take custom actions as per organization policies. **Endpoint Central:** Scan the network assets to detect OS vulnerabilities, third-party applications, and zero-day threats. Assess the potential impact using the severity ranking dashboard.

Category	Description	How ManageEngine solutions can help you
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	**ServiceDesk Plus:** Manage IT changes from submission to closure, including recording all necessary parameters such as the risk involved. **Endpoint Central:** Automatically record and monitor events, and manage and track changes by assessing their risk impact in real time using endpoint analytics and reporting capabilities.
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF functions.	**ID.IM-01:** Improvements are identified from evaluations.	**Endpoint Central:** Continuously assess cybersecurity posture and simplify compliance evaluations using automated compliance reporting capabilities.
	ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	**Analytics Plus:** Gather insights from anomaly patterns and drill down to specific metrics to identify areas that need improvement. **Endpoint Central:** Test and approve patches to assess changes in a controlled setting.
	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	**Vulnerability Manager Plus:** Remedy web server security flaws by acquiring details on the incident cause and impact. Prioritize vulnerable areas susceptible to exploitation by using attacker-based analytics.

Protect:

Develop and implement appropriate safeguards to ensure delivery of critical services.

Category	Description	How ManageEngine solutions can help you
Identity management, authentication, and access control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.	**PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization.	**AD360:** Automate authorization of user access to resources based on their organization role. **PAM360:** Identify and authorize access to business-critical resources, and spot unusual privileged activities. **FileAnalysis:** Prevent privilege abuse by analyzing users' access permissions. **Endpoint Central:** Leverage conditional access policies to validate authorized users to access business-critical systems and data.
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.	**PAM360:** Onboard privileged user accounts into a secure vault mechanism that offers role-based access to the critical assets in the network.
	PR.AA-03: Users, services, and hardware are authenticated.	**AD360:** Implement MFA techniques such as biometrics and QR codes to authenticate user identity. Centrally manage application access and usage, and provide SSO for your end users. **Endpoint Central:** Implement MFA techniques, including biometrics and OTPs, to authenticate digital assets.

Category	Description	How ManageEngine solutions can help you
	PR.AA-04: Identity assertions are protected, conveyed, and verified.	**PAM360:** Allow privileged users to access remote hosts without any endpoint agents. Provision secure access to critical data center components through SSH, Telnet, and RDP connections. **Endpoint Central:** Establish a secure, web-based connection to remote computers in the LAN and WAN through a VPN or the internet.
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	**PAM360:** Establish strict governance over privileged access pathways and critical infrastructure. Assign just-in-time controls and provision higher privileges only when required by users. Adopt a Zero Trust security approach to reduce security risks by using least privilege workflows for access provisioning. **AD360:** Streamline identity access management tasks by imposing least privilege access policies to users based on their roles and responsibilities. Automate periodic access reviews with customizable access certification campaigns. **Application Control Plus:** Limit malware intrusions by blocklisting malicious executables. **DataSecurity Plus:** Detect ransomware with threshold-based alerts by inspecting sudden spikes in file rename and other change events. Shut down infected devices to contain the ransomware spread in your network quickly. **Log360:** Detect threats to both users and devices. Monitor all successful and non-successful accesses. Trigger response workflows to log off the associate user or entity.

Category	Description	How ManageEngine solutions can help you
		Device Control Plus: Create and fine-tune file access control policies for peripheral devices based on the specific departments and employee functions within your organization. **Endpoint DLP Plus:** Deploy policies to detect all structured and unstructured sensitive items. **Browser Security Plus:** Exercise control over installation and usage of browser extensions and plugins.
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	**Endpoint Central:** Configure stringent passcode and device lock policies to protect corporate assets. **Mobile Device Manger Plus:** Configure device settings and functions on corporate mobile devices based on assigned groups. Set up alerts and schedule custom reports to gain visibility into compliance violations.

Category	Description	How ManageEngine solutions can help you
Data security (PR.DS): Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-01:** The confidentiality, integrity, and availability of data at rest are protected.	**Endpoint Central:** Protect data by managing BitLocker encryption in endpoints. Secure sensitive information from theft by using advanced data loss prevention strategies. **DataSecurity Plus:** Secure and control access to USBs, selectively block file copy actions for business-critical information, and prevent leakage of confidential files via email attachments. **Endpoint DLP Plus:** Automate detection and classification of personal data, audit file access, and establish policies to ensure secure usage. **Log360:** Avoid data exposure by blocking high-risk file copy activities to USB devices and across local and network shares. Log360 also monitors file servers by tracking and recording a complete audit trail of all files copied by auditing your clipboard for Ctr+C and right-click copy actions.
	PR.DS-02: The confidentiality, integrity, and availability of data in transit are protected.	**Endpoint Central:** Identify emails containing sensitive information using fingerprinting and keyword search, and block emails as per the policy. Block the transfer of sensitive information via unauthorized USB devices. Control the download and printing limit for trusted devices. **Network Configuration Manager:** Back up incremental versions of network configurations and choose the most stable version as the baseline configuration. **Key Manager Plus:** Manage SSH keys and digital certificates to ensure secure, encrypted data communication.

Category	Description	How ManageEngine solutions can help you
		DataSecurity Plus: Audit the usage of removable storage media and the respective data transfer activities. Implement read-only access to suspicious devices to prevent executables running on USBs. **Endpoint Central:** Block the transfer of sensitive information via unauthorized USB devices. Control the download and printing limit for trusted devices. **Log360:** Prevent files containing highly sensitive data from being shared via email as attachments. Log360 also allows the tracking of data-sharing patterns via web apps like SharePoint, Exchange, OneDrive, DropBox, Box, and more with details on who made the request, when, and from where. Leverage Log360 to secure your data in transit by monitoring workstations, file servers, cloud applications, and more.
	PR.DS-10: The confidentiality, integrity, and availability of data in use are protected.	**DataSecurity Plus:** Maintain file integrity by monitoring permission changes, file creation, and move and modify events. **Network Configuration Manager:** Identify potential firmware security vulnerabilities in your network and perform corrective measures periodically. **Vulnerability Manager Plus:** Monitor network endpoints to detect peer-to-peer apps and remote-sharing tools. Eliminate the associated security risks by uninstalling unsafe software.

Category	Description	How ManageEngine solutions can help you
		Log360: Leverage Log360 to monitor and report on a wide range of file activities, including create, delete, modify, overwrite, rename, move, read, etc. in real time. Also gather details on all file activities via browsers, such as potential upload and download actions by employees. It also allows you to classify files based on their sensitivity into categories, i.e., public, private, confidential, or restricted to help secure at-risk confidential files.
	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	**AD360**: Back up your AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments. **Network Configuration Manager:** Automate network device configuration backups and reduce downtime.
Platform security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.	**PR.PS-01:** Configuration management practices are established and applied.	**Network Configuration Manager:** Configure the network configlets and maintain control over change workflows and changes within network infrastructure. Back up incremental versions of network configurations and choose the most stable version as the baseline configuration. **Endpoint Central:** Centralize and manage user-based and computer-based configurations for improved efficiency.

Category	Description	How ManageEngine solutions can help you
	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.	**Endpoint Central:** Schedule software deployments and perform pre and post-deployment activities. Allow users to install software themselves using the self-service portal. **Application Control Plus:** Discover all installed applications and executables, and categorize them as authorized or unauthorized based on their digital signatures. Create application allowlists, and associate them only to chosen users to ensure complete security.
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	**Asset Explorer:** Handle the complete life cycle of every asset from procurement to disposal. **Endpoint Central:** Control corporate network access by ensuring only enrolled devices are granted permissions. Maintain full visibility with a comprehensive inventory of all managed endpoints in the network.
	PR.PS-04: Log records are generated and made available for continuous monitoring.	**Log360:** Collect logs from devices, servers, network devices, firewalls, and more. Encrypt the log data for future forensic analysis, compliance, and internal audits. Log360 automatically discovers the Windows and syslog devices on your network and ingests log data. With features such as custom log parsing, real-time analytics, secure log archival, and automated workflows, Log360 bolsters your organization's cybersecurity. **Firewall Analyzer:** Collect and analyze log data from firewalls and other security devices to discover security threat attempts and perform bandwidth management. Firewall Analyzer generates detailed log-based reports for in-depth visibility into traffic and attacks.

Category	Description	How ManageEngine solutions can help you
	PR.PS-05: Installation and execution of unauthorized software are prevented.	**Log360:** With its complex log collection capabilities, Log360 uses both agent-based and agentless log collection methods ensure no entity or abnormal behavior goes unnoticed. UEBA also provides insights into unauthorized or abnormal software installations or executions within your network. **PAM360:** Provide endpoints access to only RemoteApp, thus limiting users from executing unauthorized applications. **Endpoint Central:** Blocklist or allowlist applications and stand-alone EXEs to prevent unauthorized application usage.
Technology infrastructure resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage.	**OpManager Plus:** Secure your network with the Advanced Security Analytics module to detect zero-day network intrusions, firewall rule anomalies, and rogue devices. **Log360:** Log360 tracks malicious IP addresses attempting to access your company's vital resources and assists with the analysis of users accessing unsafe and banned websites to help in both detection and mitigation of cyberattacks. Log360 will also help you gain more insights about the attack techniques, IP reputation scores, and the geolocations of hostile actors trying to infiltrate your network. **Endpoint Central:** Regulate user permissions and strict access control policies to ensure only authorized individuals and devices can connect to your network.

Category	Description	How ManageEngine solutions can help you
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	**ServiceDesk Plus:** Streamline major incident management by configuring multiple criteria to execute custom actions. Reduce repeat incidents by defining closure rules. **Endpoint Central:** Distribute tasks and workloads across multiple servers to maintain continuous endpoint security operations and prevent service disruptions, ensuring optimal performance under varying conditions. **Vulnerability Manager Plus:** Orchestrate patch management to test, approve, and deploy OS and third-party application patches. Configure deployment policies to determine when and how patches should be deployed to user endpoints. **Log360:** With Log360's intuitive correlation dashboard, you can view a summary of all detected security threats, including ransomware attacks, file integrity threats, database and web server threats, malicious use of command line tools, suspicious process spawning, and exploitation of built-in binary tools and utilities. With Log360's UEBA console, you can analyze all anomaly trends and get insights on the number of detected anomalies, anomaly report statistics, and risk levels for users and entities in your network.
	PR.IR-04: Adequate resource capacity to ensure availability is maintained.	**OpManger Plus:** Monitor and optimize your network bandwidth and the performance of critical network devices, including firewalls and servers. **Site24x7:** Ensure availability by monitoring the performance of your DevOps and IT operations.

Detect:

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Category	Description	How ManageEngine solutions can help you
Continuous monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.	**DE.CM-01:** Networks and network services are monitored to find potentially adverse events.	**Log360:** Gain insights into your security incidents by monitoring and collecting extensive audit data from servers, firewalls, applications, and endpoints. **OpUtils:** Scan routers and subnets periodically to detect rogue devices in the network and block their access. **NetFlow Analyzer:** Leverage the network behavior anomaly detection system to analyze server traffic, diagnose network anomalies, and identify any threats in the network.
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.	**Log360:** Group users in the network based on their behaviors and establish a baseline for their group. Use the baseline as a reference to flag any deviations as anomalies and raise alerts. Monitor privileged user activities, data access, and network access, and receive real-time alerts for incidents. **DataSecurity Plus:** Monitor file activities, data transfers, and application usage to spot anomalous activities. **AD360:** Monitor user and admin activities for suspicious behavior. Receive real-time alerts for any unusual data patterns and keep an eye on application access in your organization with a detailed report. **Endpoint Central:** Leverage AI-driven behavior-based detection and advanced deep-learning antivirus to safeguard against both online and offline malware threats. Proactively identify, block, and address emerging threats with next-gen antivirus.

Category	Description	How ManageEngine solutions can help you
	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events.	**NetFlow Analyzer:** Utilize flow technologies to aid in network forensics and security analysis to discover internal or external security threats, zero-day vulnerabilities, and network anomalies. **Log360:** Collect and analyze logs from various sources in your environment, including third-party software, external services, and end-user devices, and get insights in the form of graphs and intuitive reports that help spot security threats.
	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	**OpUtils:** Identify rogue device intrusions in the network and block access. **Endpoint Central:** Limit cyberattacks by blocking non-business applications and malicious executables. **Log360:** Gain insights into your security incidents by monitoring and collecting extensive audit data from servers, firewalls, applications, and endpoints.
Adverse event analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.	**DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities.	**Log360:** Collect and analyze event logs from the endpoints, servers, network devices, and firewalls in your environment to spot security threats. Analyze and correlate logs with visual dashboards to discover security incidents, attacks, and suspicious or malicious user behavior. **Analytics Plus:** Run comprehensive postmortem reports to identify loopholes and anomalies leading up to a cybersecurity event. Detect indicators of compromise, and trigger alerts to relevant security personnel.

Category	Description	How ManageEngine solutions can help you
	DE.AE-03: Information is correlated from multiple sources.	**Log360:** Collect and analyze event logs from the endpoints, servers, network devices, and firewalls in your environment to spot security threats. Analyze and correlate logs with visual dashboards to discover security incidents, attacks, and suspicious or malicious user behavior.
	DE.AE-04: The estimated impact and scope of adverse events are understood.	**Log360:** Understand the impact of incidents by conducting post-attack analysis and identify patterns to stop attacks through log forensics.
	DE.AE-06: Information on adverse events is provided to authorized staff and tools.	**Endpoint Central:** Deliver real-time alerts for suspicious activity, security incidents, and potential threats on managed endpoints. **Log360:** Gain meaningful security context from collected log data to identify security events quickly and streamline incident management by integrating with external ticketing tools.
	DE.AE-07: Cyberthreat intelligence and other contextual information are integrated into the analysis.	**Log360:** Leverage STIX, TAXII, and AlienVault OTX format threat feeds to discover malicious IPs, domains, and URLs.

Category	Description	How ManageEngine solutions can help you
	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.	**Log360:** Configure alert thresholds by selecting the number of anomalies, intervals, and time ranges that would trigger the alert. **ServiceDesk Plus:** Trigger automated incident management workflows based on alerts from monitoring devices. **Endpoint Central:** Automate workflows to initiate incident response procedures, notify security teams, and escalate critical events.

Respond:

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Category	Description	How ManageEngine solutions can help you
Incident management (RS.MA): Responses to detected cybersecurity incidents are managed.	**RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared.	**Vulnerability Manager Plus:** Remediate threats and vulnerabilities by automating the deployment of patches to operating systems and third-party applications. **AD360:** Modify or revoke NTFS permissions to limit the exposure of sensitive files. **Log360:** Automate and accelerate threat response through standard workflows, and streamline incident management by integrating with ticketing tools. **ServiceDesk Plus:** Automate major incident workflows to improve resolution time and streamline major incident management.
	RS.MA-02: Incident reports are triaged and validated.	**NetFlow Analyzer:** Detect security threats using a continuous stream mining engine technology. Track network anomalies that infiltrate your firewall and identify context-sensitive anomalies by analyzing traffic patterns. **Log360:** Mitigate internal and external threats by collecting and analyzing real-time data from all critical resources. Conduct forensic analysis by identifying network and system anomalies. **Endpoint Central:** Identify zero-days within the software and network infrastructure by leveraging real-time threat monitoring and detection capabilities. Streamline the mitigation of zero-days by promptly deploying the patches and configurations.

Category	Description	How ManageEngine solutions can help you
	RS.MA-03: Incidents are categorized and prioritized.	**ServiceDesk Plus:** Classify incidents based on their urgency and the severity of their impact on users or the business. **Log360:** Prioritize threats that occur earlier in the attack chain by using MITRE ATT&CK framework in Log360. **Endpoint Central:** Prioritize incidents effectively using the vulnerability severity capability, which helps assess and rank threats based on their potential impact.
	RS.MA-04: Incidents are escalated or elevated as needed.	**Log360:** Automate and accelerate threat response through standard workflows, and streamline incident management by integrating with ticketing tools. **ServiceDesk Plus:** Configure multiple escalation levels for incidents when the response or resolution SLA is breached. **Endpoint Central:** Define workflows to trigger automatic notifications and escalations based on predefined criteria, ensuring timely intervention for high-priority incidents. Track and validate the status of all ongoing incidents.
Incident analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities.	**RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	**Log360:** Understand the impact of incidents by conducting post-attack analysis and identify patterns to stop attacks through log forensics. **Endpoint Central:** With anti-ransomware capabilities, analyze system logs, memory dumps, and registry entries to track down the source of the vulnerability.

Category	Description	How ManageEngine solutions can help you
Incident management (RS.MA): Responses to detected cybersecurity incidents are managed.	**RS.AN-06:** Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	**Log360:** Tamper-proof log archive files to ensure the log data is secured for future forensic analysis, compliance, and internal audits. **ServiceDesk Plus:** Record, assign, and track the tasks performed during the incident resolution process.
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.	**Log360:** Mitigate internal and external threats by collecting and analyzing real-time data from all critical resources.
	RS.AN-08: An incident's magnitude is estimated and validated.	**ServiceDesk Plus:** Record the level, impact, urgency, and priority of an incident.
Incident response reporting and communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.	**RS.CO-02:** Internal and external stakeholders are notified of incidents.	**ServiceDesk Plus:** Automate custom notifications to various relevant stakeholders through email when high priority tickets are created. **Log360:** Correlate log data to detect attack patterns, conduct root cause analysis, and automate immediate notifications via email and SMS. **AD360:** Set up alert profiles to notify security personnel via email and SMS on detection of suspicious user activity with UBA.

Category	Description	How ManageEngine solutions can help you
		Firewall Analyzer: Send security alerts to admins through email or SMS on detection of anomalous traffic behavior.
	RS.CO-03: Information is shared with designated internal and external stakeholders.	**Site24x7 StatusIQ:** Keep all stakeholders in the loop about an incident by posting on your status page or sending out notifications via SMS or email.
Incident mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects.	**RS.MI-01:** Incidents are contained.	**ServiceDesk Plus:** Reduce repeat incidents through root cause analysis. **Endpoint Central:** Proactively contain security incidents with real-time threat detection and rapid response capabilities. **Log360:** Automate incident response and create incident workflows triggered by alerts. Reduce the mean time to detect (MTTD) and the mean time to resolve (MTTR) an incident by quickly detecting, categorizing, analyzing, and resolving an incident accurately with a centralized console.
	RS.MI-02: Incidents are eradicated.	**Vulnerability Manager Plus:** Mitigate the exploitation of security loopholes in your network and prevent further loopholes from developing.

Recover:

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Category	Description	How ManageEngine solutions can help you
Incident recovery plan execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.	**RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process.	**AD360:** Automate incremental or complete backups of AD, virtual machines, and Windows Server to restore affected files in case of any cyberattacks. **Network Configuration Manager:** Restore network functions in case of a misconfiguration disaster by implementing a rollback mechanism to a trusted network configuration version. **Log360:** Terminate or initiate processes, change firewall rules, and effect AD changes automatically after an incident to enable recovery.
Incident mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects.	**RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	**Site24x7 StatusIQ:** Keep all stakeholders in the loop about an incident by posting on your status page or sending out notifications via SMS or email.

Step1: Prioritize and define the scope

By defining their business objectives and priorities clearly, organizations can understand the underlying support systems and assets that need to be safeguarded from cyberthreats. Establishing a consensus on what the acceptable risk tolerance levels are is the first chasm to cross and will require complete collaboration between upper management and IT.

How can you establish or improve a cybersecurity program?

This framework offers organizations a repeatable set of actions that can be performed to design their cybersecurity practices from scratch or build on their existing program to tackle the evolving cyberthreat landscape.

Step 2: Orient

The identified support systems and assets can be used to understand applicable threats and vulnerabilities. This helps in drafting an overall risk approach.

Step 3: Create a current profile

Organizations can understand their current cybersecurity posture by creating a profile that illustrates the outcomes of categories and subcategories that are being achieved.

Step 4: Perform a risk assessment

To build a resilient cybersecurity management program, organizations must assess the likelihood of a cybersecurity event and the consequential impact on business.

Step 5: Create a target profile

Based on their current profile and the possibility of cybersecurity risks, organizations can determine their weak links. By focusing on the area of vulnerability, the respective outcomes under categories and subcategories are noted down to manage risks.

Step 6: Identify and prioritize gaps

By comparing the current and target profiles, organizations can determine the efforts necessary to bridge the gap. By formulating an action plan to address the gap by outlining the budget, risks, benefits, mission drivers, and resources, a cost-effective approach can be spelled out with informed decisions.

Step 7: Implement an action plan

Organizations can move towards their desired target state with guidance from the informative references provided for the outcomes. Organizations have the leeway to choose which standards and guidelines better suit their industry and business requirements.

Parting thoughts

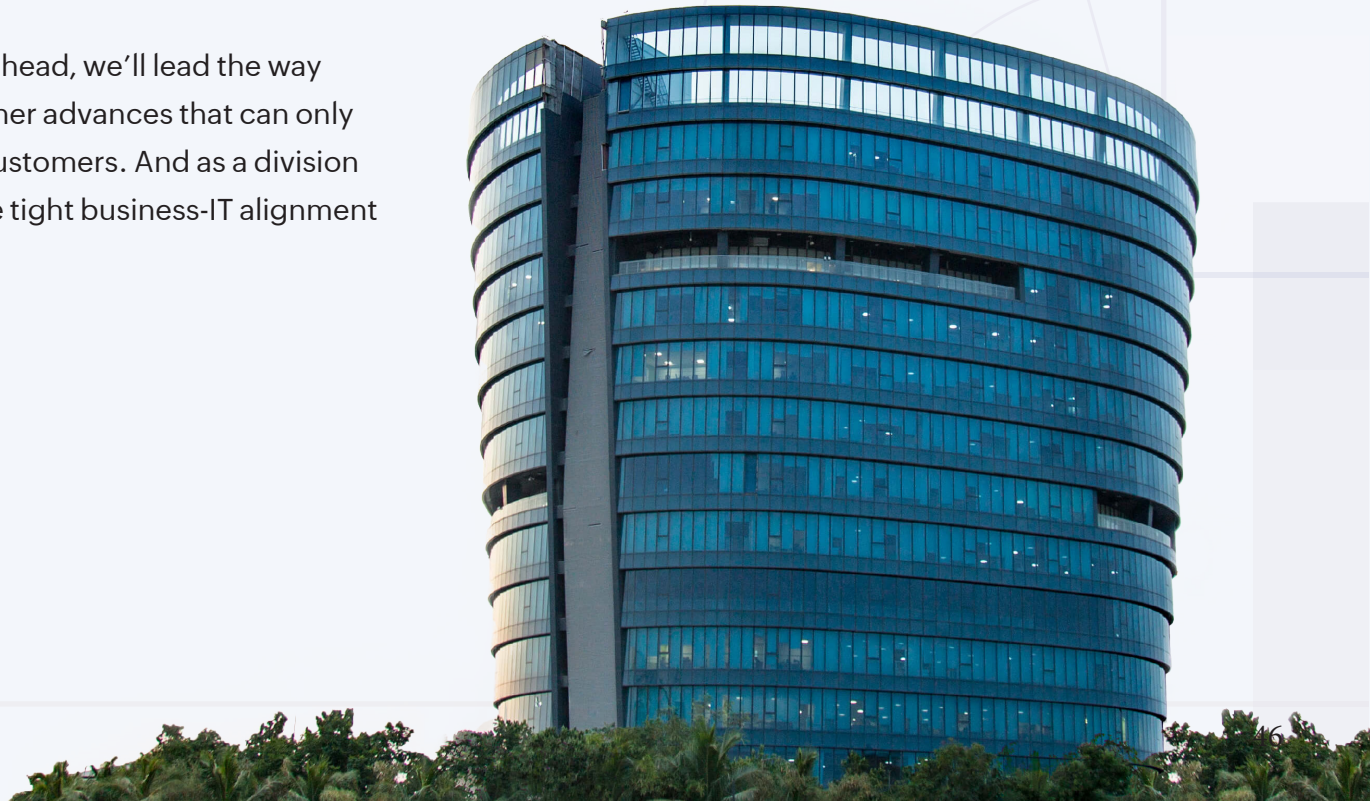
As with any worthy endeavor, the implementation of the NIST Cybersecurity Framework is more about improving your cybersecurity posture as evolving threats arise rather than racing towards a definite finish line. Keeping your organization secure is an enduring and iterative process that comprises risk assessment and implementation of best practices. The framework acts as a compass that guides organizations in the right direction to plan and prioritize their cybersecurity strategies.

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, your service desk, AD, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize future opportunities.



Take control of your IT.

Monitor, manage, and secure your digital enterprise with ManageEngine.

ManageEngine crafts comprehensive IT management software for your business needs

Available for
Enterprise IT | Managed service providers (MSPs)
As
Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

Unified service management
- Full-stack ITSM suite
- IT asset management with a CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Service management for all departments
- Reporting and analytics

Identity and access management
- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps, with MFA
- Password self-service and sync
- Microsoft 365 and Exchange management and auditing
- AD and Exchange backup and recovery
- SSH and SSL certificate management

Unified endpoint management and security
- Desktop and mobile device management
- Patch management
- Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices
- Endpoint data loss prevention
- Next-gen antivirus and ransomware protection

IT operations management and observability
- Network, server, and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change and configuration management
- Application discovery and dependency mapping
- Cloud cost and infrastructure monitoring
- End-user experience monitoring
- DNS management
- AIOps

Security information and event management
- Unified SIEM for cloud and on-premises
- AI-driven user and entity behavior analytics
- Firewall log analytics
- Data leak prevention and risk assessment
- Regulatory and privacy compliance

Advanced IT analytics
- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out-of-the-box support for multiple data sources

Low-code app development
- Custom solution builder

Trusted by


AT&T


BARCLAYS


SONY


NEC


SAINT-GOBAIN


ERICSSON


L'ORÉAL
PARIS


GE

www.manageengine.com