ManageEngine

ManageEngine's cybersecurity solutions guide

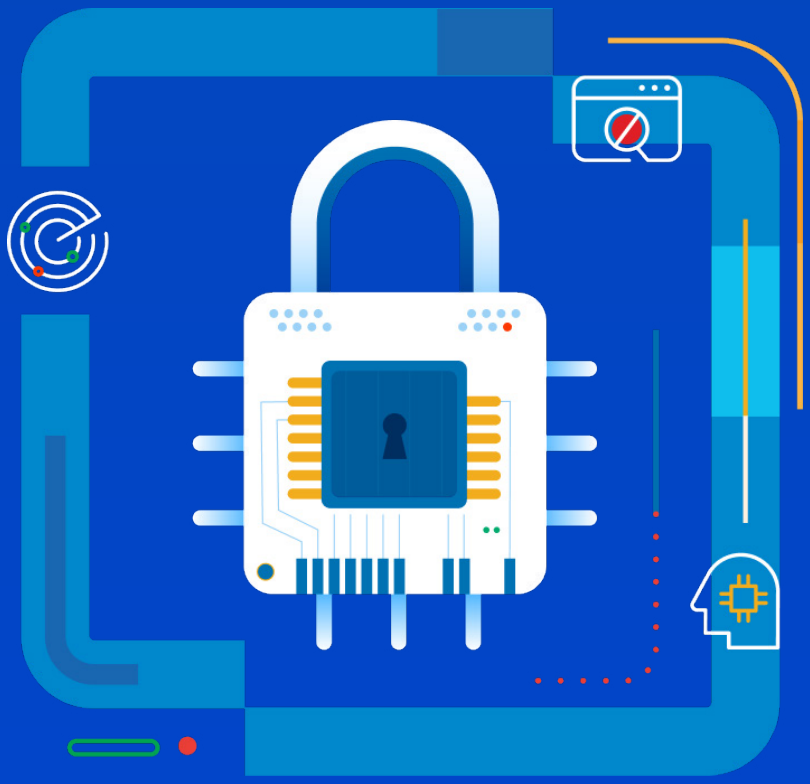


Table of Contents

Today's cybersecurity landscape

The widespread adoption of the internet, cloud computing, and remote work has transformed the way modern businesses operate. But with every new connected device, user, and application, the attack surface and imminent threat grow exponentially.

Modern threat actors aren't lone hackers—they're part of organized, well-funded groups using automation, AI, and social engineering to breach organizations at scale. Phishing, ransomware, data exfiltration, and privilege misuse are just a few of the tactics being deployed with alarming precision.

This guide explores the modern threat landscape; the business impact of attacks; and how organizations can build layered, proactive defenses with ManageEngine's unified cybersecurity platform solutions. If you want to think like an attacker and stop them before they strike, start here.

A nuanced glance into cybersecurity

Cybersecurity refers to the set of strategies, processes, and technologies used to protect systems, networks, and data from unauthorized access, disruption, or destruction. While the core objective has remained the same—to ensure the confidentiality, integrity, and availability of information—cybersecurity has evolved significantly in both scope and complexity.

In its early days, cybersecurity was mostly concerned with securing mainframes and localized networks. Today, with the rise of cloud computing, remote work, IoT, and SaaS, organizations are forced to defend a far more fragmented and dynamic attack surface. Threat actors have also evolved from amateur hackers and opportunists to well-resourced nation-state groups, ransomware cartels, and insiders with privileged access.

Modern cybersecurity demands a proactive, layered approach. This includes:

- **Preventive controls** (e.g., authentication, patching, and encryption)
- **Detective controls** (e.g., log correlation and threat intelligence)
- **Responsive measures** (e.g., containment, recovery, and forensics)

However, people, processes, and technology do not operate in silos. They require a structured foundation that aligns with organizational risk goals. That's where cybersecurity frameworks and standards laid down by organizations like the NIST, the ISO, and the IEC become essential, which we'll cover later in this guide.

Why cybersecurity can't be an afterthought anymore

Data is the new gold, and just like the highwaymen of the past, cybercriminals are always looking to plunder it. And for threat actors, breaching an organization's digital vault for its identities, devices, and systems can deliver an enormous payday.

The consequences of a cyberattack go far beyond technical disruption. A single breach can spiral into operational paralysis, legal consequences, and long-term brand damage.

→ Protects business continuity and revenue

Modern businesses run on digital infrastructure. A breach can halt operations; disrupt service delivery; and result in significant costs from downtime, data loss, and recovery. This makes cybersecurity essential to maintaining daily continuity.

→ Guards against legal, regulatory, and financial fallout

With frameworks like the GDPR, HIPAA, and DORA, compliance is now mandatory. Violations can result in steep fines, lawsuits, and loss of certifications, impacting everything from investor confidence to customer contracts.

→ **Preserves brand trust and market credibility**

A publicized breach can damage reputation beyond repair. Customer churn, media backlash, and lost deals often outlast the technical aftermath, forcing organizations into costly brand repair initiatives.

→ **Addresses the expanding threat and attack surface**

The rise of remote work, cloud sprawl, and insider risks has created more entry points than ever. Attackers exploit these through phishing, ransomware, and supply chain vulnerabilities, making layered, adaptive defense critical.

→ **Influences strategic decisions and risk posture**

Security is now a board-level metric. It shapes insurance premiums, vendor risk assessments, and regulatory audits, directly impacting an organization's long-term viability and ability to scale securely.

Anatomy of a cyberattack—and how ManageEngine helps you defend against one

Modern cyberattacks rarely unfold in linear, predictable stages. Threat actors blend tactics like phishing, stolen credentials, ransomware, supply chain compromise, or insider abuse, sometimes skipping steps or executing them in parallel. Each move is designed to deepen access, expand control, or extract value.

Understanding these patterns is critical to building layered defenses. In the sections below, we break down the common phases of an attack, highlight where organizations are most vulnerable, and show how ManageEngine's platforms disrupt adversaries at every turn.

Reconnaissance and entry

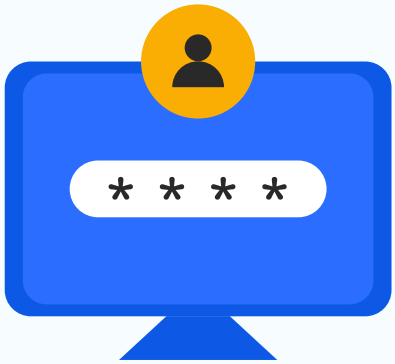
Before any payload is delivered or credentials exploited, many attackers begin with reconnaissance, quietly probing the organization's external surface. They identify exposed services, harvest credentials from data breaches or phishing, and analyze infrastructure for weaknesses. These early moves are methodical and often invisible to conventional defenses, setting the stage for a breach with precision.

Reconnaissance typically blends seamlessly into the attacker's initial access stage. Once an exploitable vector is discovered, whether it's an unpatched public-facing application, a misconfigured endpoint, or a low-privilege user account, threat actors move quickly to establish their initial foothold. In some cases, attackers bypass reconnaissance altogether, relying on opportunistic exploits or direct credential theft to gain an immediate foothold.

Common tactics

Attackers employ open-source intelligence and automated tools to identify and fingerprint vulnerable assets. Techniques include:

- **Port scanning and service enumeration:** Used to identify open RDP or SSH services, vulnerable VPNs, or exposed APIs.
- **Credential harvesting:** Attackers may use phishing, employ infostealers, or leverage leaked credentials from previous breaches.
- **Software version mapping:** Helps adversaries find systems running outdated software with known CVEs.
- **Social engineering:** Attackers impersonate IT admins or partners to trick users into granting access or clicking malicious payloads.



Why traditional defenses fail

Perimeter-based security models often assume that internal systems and authenticated users are trustworthy. This assumption fails in hybrid, decentralized environments where:

- Endpoint visibility is fragmented across BYOD and remote assets.
- Legacy VPNs provide implicit trust to any authenticated session.
- Patch management is inconsistent, especially on roaming or niche systems.
- Alerting is siloed; firewall, identity, and endpoint events are rarely correlated in real time.
- Attackers thrive in this visibility gap, leveraging low-noise techniques that evade signature-based detection and relying on misconfigured or excessive privileges to scale access.

How ManageEngine disrupts this phase

ManageEngine applies a layered, Zero-Trust-aligned defense that eliminates implicit trust and focuses on continuous verification.

- Our IAM suite enforces adaptive MFA, conditional access, and continuous risk-based verification, detecting dormant accounts, password reuse, and privilege anomalies before they become entry points.
- Endpoint protection hardens every device—including BYOD—through patching, configuration enforcement, and continuous monitoring. Attack surface reduction and behavioral analysis proactively stop phishing payloads, rogue applications, and malicious footholds.
- With SIEM, logs from endpoints, firewalls, and scanners are correlated to flag failed logins, port scans, and abnormal queries. Integrated threat intelligence highlights IoC-driven reconnaissance attempts in real time.
- The observability suite adds automated asset and network discovery, surfacing unauthorized access points while firmware vulnerability management pulls CVE data and severity scores to accelerate remediation.

Lateral movement

If attackers successfully bypass authentication—through stolen credentials, exploited vulnerabilities, or insider help—they often pivot quickly, targeting privileged accounts, poorly segmented systems, or high-value resources. This quiet expansion across the network sets the stage for privilege escalation or further compromise, making early detection of unusual movement and access patterns critical.

Common tactics

- Credential harvesting through tools like Mimikatz
- Pass-the-hash or pass-the-ticket attacks
- Exploiting remote management services like RDP
- Using legitimate admin tools
- Pivoting across systems using shared credentials

Attackers leverage poorly secured internal services and weak privilege boundaries to move sideways. Their goal is to find high-value accounts or assets without setting off alarms. Tools like PsExec, PowerShell, and built-in admin interfaces help them blend in with legitimate traffic.

Why traditional defenses fail

- Lack of privilege auditing or enforcement of least privilege
- Inadequate monitoring of new account creation or privilege elevation
- Gaps in visibility into service accounts or scheduled tasks
- Reactive security models that don't correlate intent with access behavior

Traditional identity controls often fail to validate the legitimacy of privilege changes. Persistence indicators like backdoor account creation or registry tampering can go unnoticed without baseline tracking or correlation with user intent.

How ManageEngine disrupts this phase

- PAM platforms enforce just-in-time (JIT) elevation and remove standing privileges. IAM tools monitor for unauthorized account creation and group changes. AD360 strengthens identity governance by detecting unauthorized account creation, group membership changes, and privilege escalation attempts in real time.
- Log360 correlates privilege modifications with behavioral anomalies, exposing hidden backdoors or misuse before persistence takes hold.
- Endpoint Central stops registry edits, script injections, and rogue local admin creation at the endpoint level, ensuring privilege creep is contained.
- Network observability monitors abnormal device traffic and network anomalies that could indicate persistence through hidden channels.
- from SIEM and IAM systems ensure internal threats don't go undetected.

By combining privilege access controls with continuous behavior monitoring, ManageEngine ensures that access elevation is both rare and tightly scrutinized. When suspicious privilege activity is detected, access is revoked in real time, preventing attackers from consolidating control.

Privilege escalation and persistence

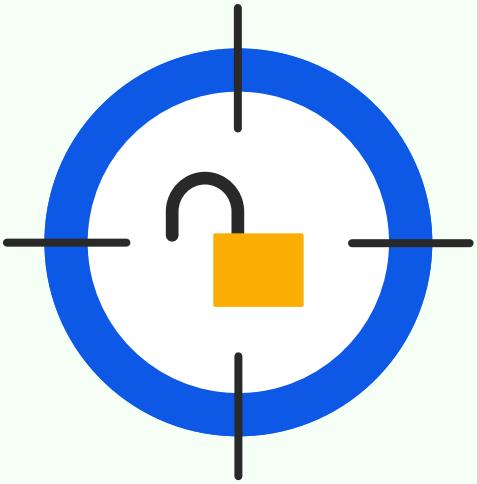
After gaining any level of access, attackers often race to deepen control—sometimes immediately—by abusing misconfigurations, stolen credentials, or planted backdoors. Escalation and persistence can occur in parallel with other activity (or even as a stand-alone objective), allowing adversaries to entrench themselves quietly and withstand resets, reboots, or password resets.

Insider threats are especially dangerous here. Malicious insiders already operate past authentication layers and may know of overlooked vulnerabilities or unused accounts to exploit. Even well-intentioned insiders can inadvertently pose a great risk if their elevated privileges are misused or left standing longer than necessary.

Common tactics

- Exploiting misconfigured group memberships or GPOs
- Creating rogue admin or service accounts
- Harvesting cached credentials or tokens
- Installing remote access tools
- Using scheduled tasks, registry changes, or startup scripts for persistence

Attackers often blend into normal administrative operations, leveraging over-permissioned accounts, legacy service dependencies, or rarely audited settings to entrench themselves. Persistence ensures they can return even after partial cleanup efforts.



Why traditional defenses fail

- Lack of traffic visibility
- Flat network architecture without segmentation
- Over-permissioned user accounts across departments
- Infrequent privilege audits and blind spots in Active Directory (AD) visibility
- Limited context in alerts, leading to detection gaps

Most organizations rely heavily on perimeter defenses and miss the internal recon and privilege abuse happening post-compromise. Without strong identity governance and behavioral context, lateral movement often goes unnoticed for weeks.

How ManageEngine disrupts this phase

- The IAM suite enforces least-privilege access and applies risk-based controls to detect anomalies in login behavior or privilege use, reducing attacker opportunities for lateral escalation.
- UEMS continuously monitors endpoint activity, blocking unauthorized remote connections and isolating compromised devices to prevent further spread. Suspicious movements, unauthorized applications, and abnormal session activity are surfaced in real time.
- SIEM correlates logins, account escalations, and cross-system access, exposing coordinated attempts that would otherwise blend into normal activity. UEBA enhances this by flagging deviations in user and host behavior.
- OpManager Plus delivers deep visibility into internal traffic with one-minute granularity. Its stream-mining engine detects anomalous east-west flows, zero-day intrusions, and threats that bypass traditional firewalls.

ManageEngine applies layered defense mechanisms across identity and network telemetry. Behavioral baselines help distinguish benign admin behavior from potential attacker movement, and correlated insights from SIEM and IAM systems ensure internal threats don’t go undetected.

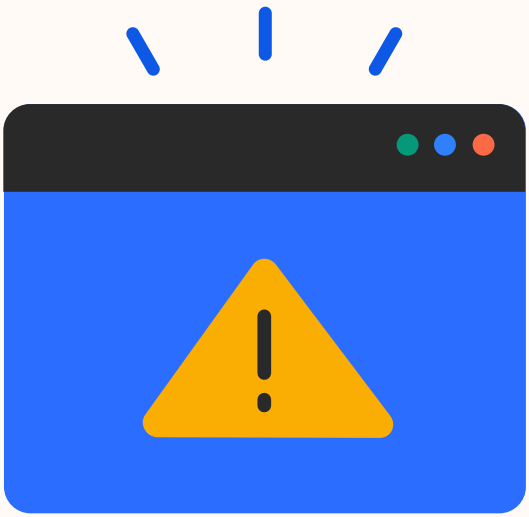
Attack execution

When attackers move from positioning to active harm, they deploy ransomware, use destructive scripts, or tamper with processes to disrupt operations or seize control. Some campaigns execute instantly upon delivery (for example, a drive-by download or an accidentally run malicious binary), while others combine immediate sabotage with simultaneous data theft or system manipulation, making the event noisy, fast, and potentially hard to contain.

Common tactics

- Launching ransomware to encrypt critical data
- Modifying configurations or deleting backups
- Deploying logic bombs or destructive scripts
- Tampering with critical services or bootloaders
- Creating diversionary events (e.g., DDoS attacks) to mask true objectives

Attack execution marks the culmination of earlier stages. With sufficient privileges and access, attackers often act fast, disrupting operations, erasing forensic traces, or triggering ransom payloads across multiple endpoints in parallel.



Why traditional defenses fail

- Inability to correlate pre-execution behavior with impending attacks
- Delayed or incomplete threat detection across endpoints
- Lack of containment capabilities to halt execution midstream
- Poor visibility into remote or unmanaged assets

Legacy antivirus tools and siloed detection systems may miss low-and-slow execution techniques or fail to respond quickly enough to limit blast radius. Without centralized control and behavioral correlation, threat execution can unfold unchecked.

How ManageEngine disrupts this phase

- Our endpoint management and security solution's built-in threat detection and device control capabilities stop malicious processes and isolate compromised endpoints before ransomware or destructive payloads propagate.
- PAM tools terminate elevated sessions and revoke access if abnormal behavior is detected.
- Log360 UEBA identifies coordinated attack patterns—privilege changes, suspicious host activity, and lateral escalation attempts—surfacing early execution signals.
- Security orchestration automates containment, isolating infected systems, reverting unauthorized changes, and triggering incident response workflows.
- With role-based access control in Network Configuration Manager, admins can restrict device access so only assigned users can modify configurations. Even then, changes cannot go live directly—they first require admin approval, ensuring unauthorized modifications are blocked. Additionally, backup deletion is not permitted, adding another layer of security.

ManageEngine solutions are engineered for rapid response. Behavioral analytics detect malicious intent before payloads launch, while integrated response tools isolate threats and roll back changes—turning destructive attacks into containable incidents.

Data exfiltration and cover-up

After gaining access—or even before any visible sabotage—attackers frequently move to steal sensitive data, using encrypted tunnels, cloud syncing, removable media, or covert APIs to siphon information without detection. Exfiltration can occur as a stand-alone objective, be run in parallel with destructive actions, or serve as leverage for extortion; attackers also manipulate or erase logs and metadata to hide their tracks, complicating detection and forensic response.

Common tactics

- Compressing and exfiltrating sensitive data via encrypted channels (HTTPS, DNS tunneling, etc.)
- Using legitimate cloud storage or collaboration apps to evade detection
- Transferring data via removable media or unmanaged endpoints
- Deleting logs, modifying timestamps, and disabling security agents
- Creating or backdating fake admin accounts for long-term access

Attackers often rely on living-off-the-land techniques, abusing legitimate tools like PowerShell, scheduled tasks, or cloud sync to quietly siphon data. Simultaneously, they attempt to erase logs and signatures that could trigger investigations.

Why traditional defenses fail

- Data security policies are often poorly configured or absent on unmanaged assets.
- Network monitoring fails to inspect encrypted outbound traffic or sanctioned cloud apps.
- A lack of immutable logging or offsite audit trails allows tampering to go unnoticed.
- SIEM solutions without behavioral correlation miss subtle data theft patterns.
- Delayed detection enables attackers to clean up evidence before response teams engage.

Conventional tools may alert on specific exfiltration attempts but struggle to stitch together the full picture, especially when data leaves slowly, stealthily, or through trusted channels.

How ManageEngine disrupts this phase

- Endpoint Central's DLP and protection capabilities classify sensitive data; block transfers to unapproved cloud apps, domains, or USB devices; and restrict suspicious file actions.
- SIEM and UEBA correlate anomalies across users, devices, and traffic flows to detect stealthy exfiltration channels, maintain tamper-proof audit trails, and issue alerts on file integrity violations or log manipulation attempts, preserving forensic evidence.
- OpManager Plus delivers real-time monitoring of outbound flows, firewall policies, and anomalous data transfers, surfacing hidden exfiltration attempts that bypass endpoint defenses.
- AD360 ensures fast rollback of AD and Exchange assets if attackers attempt to destroy evidence or backups.

ManageEngine closes the window for silent theft. With multi-layered visibility across endpoints, identity, and data channels, organizations can catch exfiltration before damage is done and ensure attackers leave fingerprints they can't scrub.

Real-world cybersecurity in action: How ManageEngine secures modern IT

Whether you're a growing business or a global enterprise, today's cybersecurity challenges demand more than point tools and reactive fixes. The following scenarios explore how real-world organizations strengthen their defenses, from securing hybrid identities to ensuring compliance across diverse environments. These use cases demonstrate how ManageEngine's unified cybersecurity portfolio adapts to different scales, infrastructures, and risk profiles, delivering practical, layered protection against modern threats.

Scenario 1: Securing identities and access in complex hybrid environments

In a mid-sized enterprise undergoing rapid digital transformation, the IT security team is grappling with growing identity-related risks. As remote work expands and cloud adoption accelerates, user identities are scattered across on-premises AD, Microsoft 365, and multiple cloud apps. The security team is tasked with ensuring that employees, contractors, and third-party vendors have the right access—no more, no less—to corporate resources at all times.

The problem is multifaceted. There are gaps in visibility across identity stores, making it difficult to enforce unified access policies. The HR team frequently forgets to deprovision access when employees exit. Contractors are granted persistent privileges even after their engagement ends. Inactive admin accounts are piling up. The compliance officer flags repeated violations of least-privilege policies, and audit logs across systems are disjointed.

To bring order to this sprawl, the team begins by consolidating identity life cycle processes. Using AD360, they automate provisioning and deprovisioning for AD, Exchange, and Microsoft 365 accounts based on HR triggers and policy rules. Access is granted based on role templates, with scheduled reviews to detect excessive privileges. AD360 also helps enforce adaptive MFA for the organization.

But managing identities isn't enough; the team must also control privileged access. To avoid always-on admin rights, they introduce JIT access via PAM360, ensuring elevated privileges are granted only for the duration needed and are automatically revoked. All privileged sessions are monitored, recorded, and audited. To enable secure remote access for external vendors, the team leverages Access Manager Plus, which allows browser-based session access to internal systems without exposing credentials.

Throughout this process, the security team uses ADAudit Plus to continuously monitor changes to user accounts, group memberships, and access rights. Any anomalous privilege escalation, lateral movement, or suspicious logon activity is flagged in real time, helping to preempt internal abuse or account compromise.

By implementing a layered identity architecture powered by ManageEngine solutions, the organization moves closer to Zero Trust maturity. Identity becomes the foundation for control; well-governed, tightly monitored, and aligned with the principle of least privilege.

Scenario 2:
Fortifying the endpoint perimeter against emerging threats

The security operations team at a mid-sized enterprise is tasked with keeping the organization safe from threats across endpoints, users, cloud services, and the network. But growing attack surfaces and limited staff make it difficult to maintain visibility, let alone proactively hunt for risks.

One major concern is blind spots across hybrid infrastructure. Many legacy tools don't monitor cloud events or correlate logs across disparate systems. As a result, incidents go undetected until damage is already done. They also struggle with alert fatigue. Too many irrelevant alerts mean critical incidents get missed or buried. Meanwhile, compliance teams are pushing for better log retention and audit trails.

Endpoint Central consolidates endpoint protection into a single platform, giving teams end-to-end visibility and control. It enforces hardened security baselines, automates patching for OSs and third-party apps, and continuously mitigates vulnerabilities before attackers exploit them. Integrated application allowlisting, browser isolation, and device control stop phishing payloads, drive-by downloads, and rogue USB activity at the source.

To centralize visibility, the organization deploys Log360, which aggregates logs from servers, endpoints, firewalls, and cloud apps. Its built-in correlation rules and behavioral analytics detect anomalies that previously went unnoticed, like a sudden privilege escalation followed by unusual file access. Log360's MITRE ATT&CK mapping helps the

team align alerts with known adversary tactics, accelerating triage and investigation.

For deeper user behavior insights, they layer in ADAudit Plus to track AD changes and logon activity across the environment. Any lateral movement or privilege abuse is flagged in real time and correlated with endpoint signals. With EventLog Analyzer, they're also able to retain logs for long-term forensics and compliance needs, including prebuilt reports for standards like HIPAA and SOX.

Over time, the team builds out threat hunting playbooks and response workflows. Alerts are prioritized based on risk, thereby reducing noise. Incident timelines stitched across multiple sources help analysts resolve threats faster, slashing their mean time to detect and mean time to respond.

Scenario 3: Detecting and responding to insider threats before they escalate

Not all threats originate outside the perimeter. Organizations today are just as likely to face security risks from within, like disgruntled employees, negligent insiders, or contractors with excessive access. These insiders may not trip traditional perimeter defenses, but their actions can be just as devastating: tampering with sensitive files, exfiltrating data, or abusing legitimate access to cause operational disruption.

The challenge for IT and security teams lies in distinguishing routine activity from subtle misuse, especially in distributed environments where thousands of user actions take place daily. Traditional rule-based

monitoring tools fail to detect unusual access that technically appears valid. And when anomalies do surface, they're often buried in alert noise or surfaced too late to act.

ManageEngine's security platforms focus on detecting intent, not just activity. With behavioral baselines powered by UEBA in Log360, you can spot unusual access patterns, like a finance user suddenly accessing engineering file shares or logging in from atypical locations. AD360 tracks file integrity violations, group membership changes, and privilege escalations, which are common early signs of insider compromise.

For endpoints, the UEMS suite proactively blocks malicious activity before damage occurs. Rogue executables, scripts, and unsanctioned admin tools are automatically stopped, while ransomware and malware protection layers ensure insiders cannot deploy destructive payloads. Integrated DLP prevents sensitive files from being copied to USB drives, personal cloud apps, or unauthorized email—closing common exfiltration paths.

These controls work together to detect misuse early, automate response actions, and generate tamper-proof audit trails, vital for compliance and forensics. And by integrating into a single SIEM view with Log360, your SOC team can correlate alerts across endpoints, file servers, and user accounts for faster resolution.

Scenario 4:
Centralizing compliance visibility across multi-regulated IT environments

For many enterprises, compliance is no longer tied to a single framework. Finance teams must answer to SOX, HR to HIPAA, and IT to the PCI DSS or ISO 27001, while business units expand into regions with their own laws like the GDPR, NIS2, or DORA. Each regulation demands a different flavor of access control, log retention, data handling, or incident response. The result? Fragmented efforts, duplicated audits, and growing blind spots across teams and systems.

Security and compliance teams need a way to unify visibility without reinventing the wheel for each regulation. Manual mapping of controls, siloed audit logs, and reactive compliance reporting just don't scale, especially when non-compliance now carries steep penalties and reputational risk.

ManageEngine's cybersecurity platform brings control standardization and audit visibility across hybrid IT. Log360 offers prebuilt report packs for frameworks like the GDPR, SOX, HIPAA, and the PCI DSS, aggregating logs across devices, users, and cloud services into centralized dashboards. AD360 and PAM360 help enforce and document role-based access, privilege management, and MFA adoption, critical for least-privilege mandates in most regulations.

Endpoint Central consolidates compliance enforcement across endpoints by unifying patching, vulnerability management, application and device control, and data protection into one platform.

It continuously validates security baselines against CIS, NIST, and regulatory standards; automates remediation of non-compliant systems; and generates audit-ready reports to simplify regulatory assessments across HIPAA, the PCI DSS, and the GDPR.
By correlating these efforts under a single platform, security leaders can maintain a real-time pulse on compliance posture, reduce audit fatigue, and prove control effectiveness without chasing siloed evidence trails.

Scenario 5: Building resilience with attack surface monitoring and recovery readiness

Modern attack surfaces are sprawling and dynamic including cloud apps, VPN tunnels, mobile endpoints, and supply chain integrations. And while preventing intrusions is critical, resilient organizations focus equally on limiting the blast radius and restoring operations swiftly when defenses fail. Recovery readiness, asset observability, and response planning are now just as vital as perimeter controls.

Unfortunately, most organizations discover their weaknesses post incident. Incomplete asset inventories delay containment. Weak credential recovery stalls incident response. Unmonitored misconfigurations open the door to repeat exploits.

ManageEngine's cybersecurity portfolio supports continuous surface monitoring and rapid recovery orchestration. OpManager Plus, Site24x7, and Cloud Security Plus continuously scan on-premises and cloud environments for rogue devices, risky configurations, or unauthorized exposure. AD360 enables granular restoration of AD objects and Microsoft 365 mailboxes, helping organizations recover accounts,

policies, and email access after compromise. It also ensures users can securely reset credentials post incident without overloading IT desks.

The UEMS suite maintains continuous endpoint visibility, detects configuration drift, and automates remediation of risky settings to reduce exploitable gaps. Integrated ransomware and malware protection stop destructive payloads before they spread. Patented single-click rollback and recovery ensure business continuity, while vulnerability scanning and CIS and NIST benchmark alignment prevent repeat exposure.

Meanwhile, Firewall Analyzer audits changes in firewall rules and VPN configurations, alerting teams about unauthorized access paths. These layers ensure that organizations can detect surface changes quickly, lock down blast zones during an attack, and recover identities and services with minimal downtime.

Together, these tools build operational resilience, not just by reacting faster but by reducing the long-term consequences of breach events.

Why compliance isn't optional—and how ManageEngine helps you gets it right

Today's regulatory climate is more complex than ever. Governments, industry bodies, and consumer protection authorities have rolled out hundreds of cybersecurity and data privacy regulations across sectors and geographies. From the GDPR in Europe to HIPAA in healthcare and the PCI DSS for payment systems, each framework imposes its own set of mandates on how organizations must handle, secure, and monitor their data and systems.

But with compliance comes complexity. Most organizations must simultaneously adhere to multiple standards, each with different control requirements, reporting expectations, and enforcement models. Staying on top of all this is no longer optional.

Non-compliance can lead to crippling fines, operational shutdowns, and reputational damage, especially in breach scenarios. And proving compliance isn't always straightforward; it requires continuous monitoring, audit readiness, and demonstrable security controls.

That's where a platform like ManageEngine makes the difference—consolidating monitoring, reporting, access control, and audit capabilities to help organizations meet evolving compliance demands without drowning in complexity.protection against modern threats.

NIS2 Directive

The NIS2 Directive introduces stricter cybersecurity expectations for European Union (EU) member states and critical sectors—broadening scope, increasing accountability, and imposing stronger enforcement. Organizations deemed essential or important must now prove structured cybersecurity governance, including board-level oversight and accountability.

NIS2 places particular emphasis on third-party risk, real-time threat visibility, and prompt incident reporting. Compliance requires more than periodic audits—it demands ongoing risk assessment, endpoint and identity monitoring, and clear response plans.

ManageEngine helps organizations align with NIS2 by integrating detection, response, and governance across IT layers:

- Enforce access control and identity governance with IAM tools like AD360 and PAM360.
- Detect threats and respond swiftly using Log360's SIEM, UEBA, and alerting.
- Automate endpoint hardening by enforcing CIS- and NIST-aligned configurations with Endpoint Central.
- Preserve audit trails and enable post-incident forensics with comprehensive log retention.
- Firewall Analyzer's integrated compliance management function automates firewall compliance audits with its out-of-the-box firewall security standards reports.

Explore how ManageEngine equips you with the controls, reports, and oversight mechanisms needed to operationalize NIS2 across your IT and security landscape.

NIS2 →

Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) establishes a unified EU-wide standard for managing ICT risks in the financial sector. It extends beyond banks and insurers to cover FinTech firms, crypto providers, and third-party ICT vendors—placing broad digital ecosystems under regulatory oversight.

DORA goes deeper than breach prevention—it mandates operational resilience. Financial entities must prove they can detect, withstand, and recover from disruptions. This includes testing business continuity plans, reporting incidents promptly, and managing vendor-related risks.

To comply, organizations need full visibility into their digital infrastructure, clear dependency mapping, and immutable audit trails of security and recovery events.

ManageEngine helps streamline DORA readiness through layered resilience and risk control:

- Maintain ICT visibility and configuration hygiene with OpManager Plus and Vulnerability Manager Plus. Monitor device health, encryption status, and antivirus compliance with Endpoint Central to align with ICT resilience requirements.
- Strengthen threat detection and speed up response with Log360's UEBA and tamper-proof audit trails.
- Control identity and access with AD360 and PAM360 for JIT access and secure authentication.
- Ensure fast recovery with RecoveryManager Plus for backup and restoration across AD and Exchange.

ManageEngine's cybersecurity platforms help operationalize DORA with layered protection, built-in incident forensics, and audit-ready compliance reporting across all critical systems and endpoints.

DORA →

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) defines how healthcare entities in the United States (US) must protect electronic protected health information (ePHI). It applies to hospitals, insurers, and business associates, with strict mandates for data security, access control, and breach accountability.

What makes HIPAA unique is its focus on auditability and access justification. Organizations must log and justify every interaction with patient data—and a single unauthorized access can trigger steep penalties and loss of public trust.

Compliance isn't a one-time exercise. It requires continuous risk assessments, real-time monitoring, strong encryption practices, and granular access enforcement.

ManageEngine helps healthcare providers meet HIPAA requirements with unified controls for identity, activity, and endpoint security:

- Enforce role-based access and MFA with IAM solutions like AD360 and PAM360.
- Monitor and audit user access to ePHI using Log360 and ADAudit Plus.
- Scan vendor domains, drill deep with the detailed assertion check results on various risk factors, obtain a security rating score, and analyze the state of security with the Digital Risk Analyzer.
- Block unauthorized data transfers using Endpoint DLP Plus and Browser Security Plus.
- With Endpoint Central, block ePHI transfers via unapproved apps or devices, automate patching and configuration baselines to ensure devices meet HIPAA technical safeguards, ask for end-user permission before initiating remote sessions, and mask PII data in reports.

ManageEngine's security suite empowers healthcare organizations to operationalize HIPAA by enforcing data protection across devices and users—backed by compliance-ready reports and breach response capabilities.

HIPAA →

PCI DSS compliance

The PCI DSS is a globally recognized framework designed to protect cardholder data and ensure secure payment processing. It applies to any organization that stores, processes, or transmits credit card information—across retail, finance, healthcare, and beyond.

PCI DSS v4.0 raises the bar with stricter authentication requirements, ongoing risk assessments, and a focus on continuous compliance—not just annual audits. Organizations must implement encryption, access controls, activity monitoring, and detailed audit logs across all cardholder data environments.

ManageEngine supports PCI DSS readiness through integrated access governance, data protection, and security observability:

- Enforce role-based access, MFA, and least privilege with IAM solutions like **AD360** and **PAM360.**
- Ensure complete auditability with **Log360** and **ADAudit Plus,** which offer real-time log analysis, session tracking, and tampering alerts.
- Protect endpoints and data flows using **Endpoint Central** and **Endpoint DLP Plus** to harden systems, prevent leaks, and control device usage.
- Generate prebuilt PCI DSS compliance reports for audits and internal reviews.
- Ensure that configurations align with regulatory standards, reducing vulnerabilities and ensuring uninterrupted service.

Foundations for cyber resilience: Security frameworks explained

While regulations mandate what organizations must do to stay compliant, cybersecurity frameworks guide how to do it effectively. Developed by leading security collectives, these frameworks lay out structured, adaptable best practices for identifying, mitigating, and responding to cyber risks.

From risk-based models like the NIST CSF to control-driven systems like the CIS Controls, these frameworks are used by security leaders to benchmark their posture, design resilient architectures, and align with industry-proven defensive strategies.

Adopting a framework doesn't just improve security; it strengthens trust with stakeholders, accelerates compliance, and gives IT teams a common language to evaluate gaps and prioritize initiatives.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is one of the most widely adopted cybersecurity standards globally. Developed by the US National Institute of Standards and Technology (NIST), it provides a high-level, flexible framework for organizations to manage and reduce cybersecurity risk across critical infrastructure and digital operations. The framework is structured around five core functions: identify, protect, detect, respond, and recover.

Why It matters

The NIST CSF isn't just a compliance checklist—it's a risk-informed, outcome-based model that guides organizations in aligning

cybersecurity with business needs. The framework is scalable across industries and maturity levels, making it ideal for both small- and medium-sized businessess and large enterprises. It also serves as a foundation for other regulatory and standards bodies, including the CIS Controls, ISO 27001, and even sector-specific mandates like HIPAA and DORA.

How ManageEngine helps

ManageEngine enables practical implementation of the NIST CSF with integrated solutions across all five core functions:

- **Identify:** Asset inventory and risk visibility through OpManager Plus, Application Control Plus, and Vulnerability Manager Plus
- **Protect:** Identity and access governance via AD360 and PAM360; endpoint hardening with Endpoint Central
- **Detect:** Real-time vulnerability alarm, log correlation, threat detection, and UEBA via Log360, ADAudit Plus, and Network Configuration Manager
- **Respond:** Automated incident alerts, investigation workflows, and audit trails using Log360's security event correlation
- **Recover:** Rapid recovery of critical services and directory objects with AD360

Together, these solutions help operationalize the NIST CSF across IT layers—from users and devices to logs and privileges—while reducing tool fragmentation and manual effort.

Learn more →

CIS Controls®

Developed by the Center for Internet Security (CIS), the Critical Security Controls are a prioritized set of 18 cybersecurity best practices designed to help organizations prevent, detect, and respond to modern threats. These implementation-ready guidelines provide a practical foundation for securing IT systems, especially for resource-constrained teams.

Why it matters

Unlike broader frameworks, the CIS Controls are highly prescriptive—making them easier to operationalize. They address real-world threats like ransomware and phishing while aligning with broader standards like the NIST CSF and ISO 27001. Organizations adopting these controls often see measurable improvements in security posture and compliance readiness.

How ManageEngine helps

ManageEngine offers integrated support across all 18 CIS Controls, helping teams automate enforcement and demonstrate maturity with built-in reporting:

- **Endpoint Central** for continuous vulnerability assessment, secure configurations, and patch management
- **Log360** for centralized log monitoring and threat detection
- **AD360 and PAM360** for access control, resilient backup and recovery, and identity governance
- **Digital Risk Analyzer** to analyze third-party partner and vendor risks
- **Network Configuration Manager** includes CIS benchmarks by default, automatically checking device configurations against standard and flagging any non-compliant settings

Together, these tools streamline CIS Control adoption, enabling faster rollout and easier audits.

Learn more →

Essential Eight Maturity Model

The Essential Eight is a cybersecurity framework developed by the Australian Cyber Security Centre, offering eight prioritized mitigation strategies to defend against the most common cyberthreats. Though originally intended for the government and critical infrastructure sectors, its practical, maturity-based approach has seen global adoption.

Why it matters

The framework defines four implementation maturity levels (0 to 3), helping organizations benchmark progress and resilience. It focuses on high-impact areas like patching, access control, macro restrictions, and backup integrity—areas consistently exploited in real-world breaches. Essential Eight is valued for being actionable, scalable, and directly tied to improved security outcomes.

How ManageEngine helps

ManageEngine's platforms support Essential Eight implementation across all maturity levels:

- Streamline patching, application allowlisting, macro control, and privileged access auditing with **Endpoint Central.**
- **AD360** and **PAM360** manage privileged access, JIT elevation, and user activity audits. **AD360** also ensures reliable, granular backup and recovery.
- **Browser Security Plus** restricts Microsoft 365 macros, ActiveX, and legacy components.
- **Log360** detects threats with correlation, UEBA, and lateral movement analysis.

By consolidating these functions under a unified platform, ManageEngine helps teams operationalize the Essential Eight without complexity or tool sprawl.

Learn more →

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, 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 opportunities in the future.

ManageEngine

www.manageengine.com