

Streamline your healthcare IT to improve patient care



www.manageengine.com/healthcare

Table of Contents

Navigating the digital transformation in the healthcare industry	3
Common healthcare sector challenges	4
How IT can help your organization	7
Solving real-world healthcare related IT problems with ManageEngine	13
Use-case 1: Ensure seamless patient care and staff experience	13
Use case 2: Leverage predictive analysis to make informed decisions	18
Use-case 3: Protecting critical patient data	19
Use-case 4: Facilitate streamlined hospital management	24
Use-case 5: Securing the cyber infrastructure	28
About ManageEngine	33

Navigating the digital transformation in the healthcare industry

The healthcare industry is undergoing a profound digital transformation, marked by the integration of cutting-edge technologies such as health monitoring wearables, networked medical devices, robotic-assisted surgical procedures, and comprehensive electronic health records. In parallel, there is a concerted effort to create a more integrated healthcare ecosystem and enhance connectivity and collaboration between various stakeholders, including pharmaceutical suppliers, insurance companies, and medical practitioners.

As this technological evolution unfolds, the industry faces the dual challenge of ensuring seamless operational efficiency and robust security measures to protect sensitive data, all without compromising the quality of patient care. Addressing these challenges head-on, there is an urgent need for advanced IT management strategies and state-of-the-art security solutions tailored to the unique demands of the healthcare sector.



Common healthcare sector challenges

Cyberattackers are more inclined to target the healthcare sector because they are well aware of the vulnerabilities that exist within the industry. Hospitals and healthcare providers cannot afford to prolong negotiations and take risks when patient health and safety are at stake. This makes them prime targets for cybercriminals seeking to exploit their weaknesses. The healthcare sector faces numerous concerns in striking a balance between providing quality medical care and ensuring the security of patient data.

Here are the most common challenges:

Cybersecurity threats

The healthcare industry is a prime target for cyberattacks due to valuable medical data. In the past five years, large breaches in the United States have increased, with a 141% rise in affected individuals in 2023 for which hacking and ransomware acted as main culprits. These attacks harm operations and patient privacy. The trend is expected to continue, with a focus on targeting healthcare systems. Al-based attacks using bots are on the rise, making updated cybersecurity solutions crucial, including Al tools. Employee awareness is a major weakness, with social engineering and insider threats being common methods used to steal data. A recent report found that 70% of healthcare data breaches globally are caused by insider threats.

Interoperability

Interoperability is a major challenge in healthcare technology as organizations must securely share patient data with care teams and other providers to comply with federal mandates. This involves the ability to access, exchange, and integrate data across different systems and boundaries with the goal of improving the health of individuals and populations globally. A <u>Deloitte survey</u> shows that U.S. based physicians expect this interoperability to become a standard practice in care delivery within the next decade.

The BYOD dilemma

The rapid growth of the BYOD trend in healthcare is a major challenge, as more institutions are allowing employees to use their own devices for work. While this trend offers increased functionality and efficiency, it also comes with risks such as data theft and cybersecurity vulnerabilities. Implementing strong security measures is crucial to mitigate these risks and ensure smooth operations in the healthcare IT sector.

Big data analysis

Doctors expect interoperability to include data from wearables and apps, adding to the already large amount they handle. Storing and securing large data can be a hassle if not accomplished properly. The high volume of real-time patient data from sensors and devices makes it hard to process. The variety of data also presents interoperability and accuracy challenges. Overall, managing this information is a major challenge.

Inadequate handling and organization of data

In the past year, almost 60% of healthcare organizations have experienced a cyberattack. Disorganized data increases the risk of hackers infiltrating systems, accessing confidential patient information, and committing identity theft. The consequences can be severe for patients and hospitals, leading to financial penalties and damaged trust. Strict data management is essential to ensure the safety of all individuals and organizations involved.

Data privacy regulations

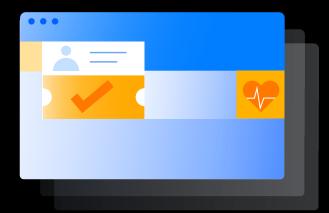
It is essential for healthcare providers to adhere to regulations like HIPAA in the U.S. and the GDPR in Europe to safeguard patient data privacy as cybersecurity threats evolve. Non-compliance can result in hefty fines and harm to its reputation, putting pressure on small healthcare organizations to follow regulations to prevent penalties. However, their lack of resources and cybersecurity expertise makes it difficult for them to manage compliance effectively and implement best practices.



How IT can help your organization

Healthcare organizations can achieve business goals by aligning IT with specific objectives. Thanks to the digital revolution in the healthcare industry, IT is now crucial for delivering efficient, high-quality patient care. IT management plays a crucial role in the smooth functioning and advancement of the healthcare industry. Here's how:

Modernize your healthcare operations



The industry faces pressure to upgrade due to patients' expectations of better digital experiences and the need to enable interoperability with modern healthcare wearables. Modernizing IT in healthcare is essential for enhancing security and efficiency. It can cut costs, simplify scaling, and reduce cybersecurity risks. Upgrading from legacy systems helps manage cybersecurity threats, with recent data showing a rise in healthcare breaches. Modern IT can improve data interoperability and help in infrastructure upgrades, process streamlining, and application development.

How IT helps:

- IT management solutions can facilitate modernizing by managing the update of hardware, software, and networks.
- Moving to the cloud is considered part of the modernization process, and this gives organizations the flexibility to scale at a lower cost.
- Healthcare applications can be developed in very little time with the help of low code app development technology.

Enhanced staff and patient experience



In recent times, patients are well-versed in technology and rely heavily on online services. As a result, they anticipate healthcare services to provide the same level of efficiency and convenience as other online platforms. Customers prioritize seamless assistance, prompt patient intake, and tailored services.

Healthcare professionals must also receive top-notch support to enhance their ability to care for patients effectively. This involves creating a conducive work environment that allows employees to concentrate on their duties without unnecessary interruptions. Equipping employees with resources to aid in decision-making and streamline tasks will improve overall efficiency.

How IT helps:

- Operations can be streamlined by optimizing repetitive processes with the help of workflow automation and AI.
- IT systems help track equipment availability, staff schedules, and medication inventory, optimizing resource allocation, and reducing costs.
- Patient portals provide self-service options for scheduling appointments, accessing medical records, requesting prescription refills, and learning about conditions.
- Through IT predictive analysis, vast healthcare data is analyzed to offer actionable insights, evidence-based recommendations, and alerts for diagnoses, treatment, and medication.
- Website and applications monitoring solutions can ensure seamless access to patient portals.
- All based chatbots can be used to provide quick answers to queries.

Improved compliance management



Cybercriminals often attack medical records to access demographic data, social security numbers, financial information, health insurance information, and medical and clinical data. These data can be used to commit identity theft. Medical records can also provide the essential information for submitting fake tax returns to claim refunds. Regulatory boards and countries have implemented rules to prevent breaches and protect patient privacy, with strict guidelines and measures for legal operation. Healthcare organizations must comply with regulations like HIPAA, HITECH, HITRUST, CCPA, POPIA, the GDPR, and others.

How IT helps:

- IT management solutions safeguard ePHI by helping implement robust cybersecurity measures, ensuring compliance with data privacy regulations like HIPAA.
- IT plans and implements disaster recovery protocols to ensure continued operation and data security in case of emergencies.
- Automated solutions for monitoring, auditing, and reporting can assess the effectiveness of IT security controls, uncover discrepancies, and provide evidence of compliance.
- Data security solutions aid in risk assessment, file analysis, and monitoring sensitive data flow through data leak prevention capabilities.

Build secure and efficient medical systems



The healthcare industry is vulnerable to cyberattacks due to valuable patient data, outdated data security technology, insufficient cybersecurity awareness and resources among staff, among other factors. Creating secure and effective medical systems is crucial for protecting patient privacy and safety, ensuring the accuracy of critical data, and enhancing healthcare delivery by streamlining processes and focusing on better health outcomes for patients.

How IT helps:

- Security solutions assist in detecting, investigating, and mitigating cyberthreat that may compromise the network.
- Identity management and privileged access management tools can be utilized to restrict access to sensitive patient data to only authorized medical personnel.
- Automated endpoint and network security management solutions can patch network and device vulnerabilities.

Elevate healthcare operations with ManageEngine's advanced IT management solutions

With novel and improved technologies continuously emerging, the healthcare sector must prioritize strengthening its IT infrastructure to ensure the protection of patient care. Managing comprehensive IT solutions becomes crucial in this pursuit.

ManageEngine solutions provide a range of cutting-edge tools that can contribute to the enhancement of healthcare operations. By leveraging AI-powered analytics, automation, hybrid cloud infrastructure, and IT management solutions, healthcare organizations can achieve numerous benefits.

Solving real-world healthcare related IT problems with ManageEngine

We have compiled some practical examples to assist organizations in determining which solutions can support their IT departments in addressing the challenges they encounter.

Use-case 1:

Ensure seamless patient care and staff experience

A healthcare group wants its patients and staff to have uninterrupted access to resources. They also want to provide a uniform experience at every location and swiftly resolve any potential performance concerns.

They plan to create an application for simpler patient data access. As the software contains private patient information, employee logins should be protected with authentication. The entire app experience should be convenient, enabling users to sign in securely and access various health apps without re-entering their credentials. The users should also be able to report issues and requests for service quickly via a self-service portal and have access to the necessary knowledge base to facilitate their resolution.

The healthcare group also intends to develop a patient portal providing users, the patients, with secure access to manage their health information, schedule appointments, fill or refill prescriptions, and enhance their overall healthcare experience. A comprehensive resource database is planned to provide assistance in areas such as preventive care, first aid, and self-medication techniques.

Healthcare Industry Guide

Additionally, many of the healthcare group's operational processes are manual, causing errors and delays. It plans to develop its own app to create a dedicated CRM and build modules for a quality management system, vendor management, and sales rep management.

How ManageEngine products can help

ManageEngine products	How they help
Applications Manager	Boost your app developers' ability to detect and resolve code issues swiftly. Provide valuable insights on response times, transaction traces, slow queries, memory leaks, and exceptions for Java, Dot Net, Ruby, PHP, and node.js apps.
	Monitor server health and availability for optimal performance of hosted applications. Receive instant notifications and take corrective action for seamless performance.
	Utilize synthetic transactions to mimic and track user experiences in your healthcare application. Keep a close eye on important transactions with screenshots and detailed breakdowns of page elements and load times.
OpManager Plus	Monitor the performance, health, and resource usage of web servers, web applications, maintain and update inventory management, and shield your organization from downtime.
	Observe and analyze live user activity data and discover the functionality of your healthcare apps across various regions with RUM.

Healthcare Industry Guide

Site24x7

Manage and enhance the efficiency of IT resources to enable physicians and specialists to obtain patient information rapidly for examination.

Whether it is a CT scan machine or a patient administration system, receive immediate notifications about downtime via text messages or use the mobile app for monitoring.

Observe REST APIs, as they facilitate interaction among applications and devices and enable the exchange of patient data for efficient analysis.

AD360 (on-premises) Identity360 (cloud)

Deploy MFA-protected SSO to enable users to securely access apps and prevent password overload with its single user, single identity feature. They can also easily access numerous business applications from a central console via the integrated SSO dashboard.

SupportCenter Plus

Create a personalized customer portal for each of your hospital divisions. Give customers access to the knowledge base (KB) in the customer portal. Suggest KB articles when a request is being logged. Enable patients, doctors, and staff with easy access to relevant information while submitting a request or searching for solutions.

Organize and integrate computer telephony with your customer support to provide better service to your patients, doctors, and staff. Keep the doctors and staff informed about the various things in the hospital.

Direct calls to the appropriate department or doctor based on predefined rules to ensure patients connect with the right person promptly.

ServiceDesk Plus

Empower your employees and patients by providing essential information at their fingertips. Launch an omni-channel service platform with a self-service portal featuring healthcare-specific categories and resources for easy access to patients.

Streamline communication between staff members and other departments by providing a centralized ticketing system to log and resolve IT and non-IT related issues.

Build comprehensive knowledge bases to keep your end users informed about relevant contact information, preventive care, standard procedures, and more.

Set up automated workflows to escalate critical issues to the right personnel based on urgency and expertise.

Integrate with IT monitoring and observability solutions like Site24x7 to convert anomalies and alarms into incident tickets and trigger automated incident response workflows.

Utilize Zia, an Al-driven smart chatbot, to provide round-the-clock conversational assistance to your staff. By using Zia, medical facilities can create comprehensive conversation workflows for common issues and frequently asked questions.

Stay audit-ready compliance by accounting for every IT and non-IT asset that powers up your digital infrastructure. Track granular software license usage and compliance with license agreements and contracts.

PAM360

Authorize privileged doctors to access sensitive patient records through secure, validated remote access based on multi-level approval from authorized personnel. Grant scrutinized access to help view sensitive patient records in a time-restricted manner.

Endpoint Central

Manage a wide range of devices, including desktops, laptops, and mobile devices used by staff to ensure consistent configuration, security policies, and application deployment across locations.

Monitor device health and performance, enable IT staff to remotely identify and resolve issues affecting critical healthcare applications, minimize downtime and disruptions, and ensure seamless productivity.

Enable staff from different shifts to use the same set of devices by setting up shared tablets to allow each employee to access their own session on the device during their shift.

Create a self-service portal where staff can download and install applications and patches on their own to reduce the need for IT support. This portal lets users schedule updates and reboots during non-peak hours and helps focus on installing critical patches first and delay less important ones.

AppCreator

Create a dedicated CRM for your organization.

Maintain up-to-date patient data and set up online portals to create and track appointments and to access reports and metrics for daily analysis.

Empower stakeholders to develop applications using a compartmentalized approach with drag-and-drop builders. These builders also eliminate the need for programming applications and automations from scratch.

Identify and automate repetitive tasks and increase your overall operational efficiency. If-then conditions, loops, ready-to-use field actions, integrations, and other built-in features help automate processes across departments.

Use-case 2:

Leverage predictive analysis to make informed decisions

An esteemed healthcare organization wants to cut operational costs, improve coordination, and deliver better outcomes. They aim to leverage their existing data to extract meaningful insights to make informed decisions about equipment shortages, patient care demands, and utilize predictive analytics to optimize its operations, improve customer experience, reduce risk, and more.

How ManageEngine products can help

ManageEngine products	How they help
Analytics Plus	Utilize AI-enabled healthcare analytics to unify large volumes of data and generate key insights, improving patient care quality, and ensuring seamless service availability.
	Leverage built-in predictive models to forecast equipment and personnel requirements based on patient inflow. Use this information to plan IT budget proposals for the future.
	Correlate data from application, network, server, and configuration management to pinpoint systems at risk of failure. Mitigate risk efficiently, transfer workloads to backup servers, and maintain 24/7 availability of hospital services.
	Utilize APIs and data connectors to access any application or data source for enhanced insights into patient data. Provide personalized services and solutions to patients, including medication recommendations, disease prevention tips, and self-treatment advice to foster loyalty and trust.

Use-case 3:

Protecting critical patient data

A multinational hospital network, with facilities worldwide, is grappling with the challenge of securing its patient data amidst an escalating number of data breaches, intricate industry regulations, and privacy mandates.

The hospital is associated with numerous laboratories, third-party vendors for medical supplies, and insurance agencies, all of which are essential for its operations. But these affiliations further expose the hospital network's data to risks and highlight the need for stringent access controls and measures to prevent unauthorized data transmission and leaks.

Due to the global nature of its operations, this organization must adhere to mandates like HIPAA, HITRUST, and HITECH, as well as comply with POPIA, the CCPA, and the GDPR.

As a result, in order to assess the success of its data protection strategies and guarantee compliance with these various regulatory requirements, the organization must periodically conduct data audits and produce customized reports.



How ManageEngine products fit

ManageEngine products	How they help
ServiceDesk Plus	Utilize HIPAA-compliant help desk to mark sensitive data fields as electronic protected health information (ePHI) and protect sensitive data by encrypting data collected and stored in any additional fields.
	Delete or anonymize the sensitive data marked as ePHI individually or collectively.
	Password-protect the data that is being exported from reports or any module in a password-protected ZIP file.
	Log any actions performed around ePHI fields automatically to simplify audits.
Data Security Plus	Perform context analysis to discover important files related to healthcare operations and classify them based on vulnerabilities.
	Continuously monitor the access and modifications made to these sensitive files and automate immediate responses to security incidents like ransomware attacks, data exfiltration attempts, file transfer anomalies, and more.
Endpoint DLP Plus	Automate in-depth content inspection to pinpoint the locations of all structured and unstructured sensitive data including ePHI.
	Once sensitive data has been identified, rules can be defined to dictate exactly which cloud applications can be used to upload data. Endpoint DLP Plus automatically stops sensitive content from being exported via unsanctioned web browsers to various third-party cloud storage applications.

Log360

Utilize integrated DLP and CASB capabilities to detect threats across the enterprise network, covering endpoints, firewalls, web servers, databases, switches, routers, and cloud sources.

Automate monitoring log data from firewalls, routers, switches, workstations, servers, and critical applications, and get notified whenever there is a compliance violation, suspicious activity, or signs of a data breach or exfiltration.

Unify data collection from all your devices for centralized healthcare log management and analysis. Gain a complete picture of your security by correlating diverse logs. Receive instant alerts on suspicious activity that might endanger patient information. Leverage advanced behavioral analytics to uncover insider threats that could breach patient privacy.

Use out-of-the-box compliance reports as evidence for your adherence to requirements stated in the regulations, which simplifies your security auditing.

EventLog Analyzer

Collect, monitor, and analyze log data for compliance management.

Export comprehensive compliance reports in any format, tweak the existing compliance auditing report templates, or create custom compliance reports to meet the requirement of the regulations.

Additionally, archive log data for custom time periods to meet crucial log archival requirements.



AD360 (on-premises) Identity360 (cloud)

Control access to critical healthcare documents and applications through single sign-on (SSO) using advanced authentication methods such as biometrics or RSA SecurID.

Keep tabs on data access rights by monitoring folder owner and permission changes, and get alerted on changes to critical files and folders via email and SMS.

Prevent inappropriate access to patient data by leveraging ML capabilities to spot unusual volumes of file changes and changes occurring at unusual times.

Protect confidential patient data by applying different authentication factors for different users based on risk factors such as IP address, time of access, device, and geolocation with risk-based automated access control.

Enhance user access security for cloud and on-premises applications by integrating SSO with MFA. Quickly identify and respond to potential threats by detecting unusual activity in user logins, account lockouts, and permission modifications through automated incident responses.

Endpoint Central

Secure hospital staff data without affecting user privacy by containerizing on mobile devices, ensuring workrelated apps are encrypted and isolated from personal applications.

Prevent patient data from falling into the wrong hands by remotely locking misplaced devices, putting them in Lost Mode, and performing a data wipe if needed.

Ensure compliance with HIPAA and generate comprehensive reports for auditing.

Ensure healthcare staff use only approved browsers and monitor all add-ons, extensions, and plug-ins to prevent unauthorized or malicious software from compromising sensitive data.

Use real-time threat monitoring to detect and fix vulnerabilities. Understand the root cause of ransomware attacks, respond immediately, and prevent future incidents.

Get notified about zero-day vulnerabilities and deploy pretested mitigation scripts before official fixes are released, ensuring immediate protection for healthcare systems.

PAM360

Efficiently detect, enroll, store, and oversee privileged users, accounts, and resources—utilized by both individuals and software—from a centralized dashboard.

Mitigate security threats stemming from persistent privileges by implementing just-in-time privilege escalation and least privilege protocols for access provisioning.

Supervise privileged user activity with session shadowing capabilities and achieve dual control on privileged access. Capture sessions and archive them as video files to support investigative audits.

Analytics Plus

Track patterns in data access, sharing, and privileged account use, and gain early warning signs of changes in patient record access patterns.

Calculate the real-time risk scores of healthcare personnel's corporate and BYOD devices, and seal security gaps with effective patching.



Use-case 4:

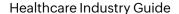
Facilitate streamlined hospital management

A multi-specialty hospital is struggling to manage its operations due to outdated IT infrastructure. It intends to modernize its systems by adopting advanced technologies to support modern healthcare.

As part of its modernization drive, it has adopted new e-health applications and upgraded its core medical systems. However, its IT team does not have complete insights into the performance of these applications, which could lead to unplanned application outages that impact patient care.

The IT team also needs to track of licensing compliance, IT expenditures, and asset depreciation to manage its healthcare IT infrastructure effectively and streamline the management of IT assets through the entire life cycle, from acquisition to disposal.

The IT team is struggling to manually update and deploy patches to its fleet of endpoints and Medicare applications, leading to slow and incomplete patching, and leaving them vulnerable to attacks. The hospital is looking for ways to automate the deployment of patches to protect against vulnerabilities and create a secure operational environment.



How ManageEngine products can help

ManageEngine products	How they help
ServiceDesk Plus	Implement an asset management strategy that works well with the other ITSM processes. Keep track of licensing compliance, IT expenditures, and asset depreciation to manage your IT infrastructure effectively. Build a central inventory for all your IT and non-IT assets. Provide real-time statuses on your entire asset inventory with live dashboards. Keep workplace service delivery and operations running smoothly. Optimally utilize your organization's campuses while keeping workplace amenities and services in check.
Asset Explorer	Monitor the complete asset life cycle from procurement to disposal. Auto-discovery and management of all hardware and software inventory deployed in your network. Scan Windows, Linux, and MacOS devices with the unified agent for asset discovery. Map business relationships among staff, assets, and services in your organization with a configuration management database.
PAM360	Ensure that the vast number of SSL/TLS certificates in enterprise IT environments are properly managed or renewed which helps avoid business outages and cyberthreats. Provide complete certificate life cycle management capabilities to help users discover all their certificates, create, renew, and deploy new certificates, and generate custom alerts for certificate expiry. Ensure that an enterprise's critical systems are encrypted and secure.

Endpoint Central

Track hospital IT assets, such as software and hardware, licenses, and warranties. Provide alerts for any changes and monitor location, condition, and usage to prevent unnecessary expenses and losses.

Seamlessly onboard and manage devices with ABM, Knox, and Google Zero Touch integration. Provide an app catalog for easy installations, reducing the need for IT support. Ensure compliance with industry regulations and data protection by allowing only approved applications for the medical team.

Conduct regular scans to gather information on IT assets within your network and create dashboards to gain insights and visualize the status of your IT infrastructure across various devices and operating systems.

Secure your network by automating patch deployment for Windows, Mac, Linux, and third-party applications. Automate patch deployment to save time and resources, with customizable scheduling for different applications and departments. Provide automatic notifications, pre-test and approve patches to avoid downtime, and implement flexible compliance policies.

OpManager

Gain immediate insight into the status, accessibility, and efficiency of your network elements, such as hospital servers, applications, and databases, to address problems before they impact patients and staff.

Create and streamline processes to address network problems. Implement automated rules and initiate processes in response to network occurrences, in line with a proactive observability strategy.

Applications Manager

Monitor the health and availability of your servers, VMs, converged or container infrastructure to ensure optimal performance for critical applications.

Site24x7

Gain comprehensive insight into the status and efficiency of your primary healthcare and e-hospital software, servers, data storage systems, networks, and websites through a single dashboard.

Analytics Plus

Build consolidated dashboards that provide a single pane of view into every healthcare application, asset, infrastructure, endpoint, and more.

Attain prebuilt dashboards combining data from the service desk and endpoint applications to view assets' entire life cycle, associated users, patch compliance, licenses, and warranties from one pane.

AppCreator

Drag-and-drop over 30 types of form fields to collect data like names, email addresses, and customer feedback.

Establish a customized CRM for your company. By implementing a healthcare CRM, you can maintain current patient information, such as medical history, appointment details, and billing records, and establish online portals for scheduling appointments and analyzing daily reports.

Utilize AppCreator's online portals to manage suppliers. This involves uploading new orders, monitoring shipments, managing payments, and submitting support requests from a single dashboard.

Monitor the number of visits made by your field sales team to physicians and other clients.

Provide sales managers with a centralized dashboard to manage team expenses, review meeting reports, access support requests, and more.



Use-case 5:

Securing the cyber infrastructure

A hospital is concerned about the increasing risks of cyberattacks, with attacks already compromising patient information within the industry. As a proactive measure to enhance its defenses and lower risks, the hospital is updating its cybersecurity approach, adopting security frameworks like the NIST Cybersecurity Framework and Zero Trust.

While analyzing its security practices, one major issue identified was the lack of proper access control, which threatens the security and privacy of patient data.

To safeguard its IT infrastructure, the hospital plans to:

- Gain full visibility over all identities, devices, data, and applications accessing the network.
- Ensure that medical staff, like doctors, nurses, and health insurance executives, have only the necessary access to patient health information relevant to their duties.
- Monitor all network activity and entities, identifying and flagging any suspicious behavior or threats.
- Respond to potential threats by enforcing additional authorization and authentication, restricting user privileges, isolating devices, ending sessions, and providing just in time access if needed.
- Take preventative actions and enhance security for endpoints and accounts, such as resetting credentials and fixing vulnerabilities.
- Develop an incident management plan to ensure business continuity and data backup in case of an attack.

Healthcare Industry Guide 28

How ManageEngine products can help

ManageEngine products	How they help
AD360	Assign appropriate access levels to patient health information for doctors, nurses, health insurance executives, and other relevant personnel. Monitor for signs of privilege abuse, such as excessive file modifications and unauthorized attempts to access critical files. Detect privilege escalation attacks by tracking and
	reviewing changes to security groups.Track folder ownership and permissions to monitor data access rights.
	Receive email and SMS alerts for file and folder changes. Apply ML to detect unusual file activity and unauthorized access to patient data. Improve security for sensitive health information by customizing authentication methods based on risk factors like IP address, access time, device, and location.
	Back up AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments. Ensure unprecedented resilience during disasters by restoring your entire environment or just part of it from a backup.
PAM360	Grant trusted, authorized entities secure remote access to medical systems on a role-based, least privilege basis. Assign just-in-time controls for your domain accounts and provision them with higher privileges only when required by your users. Automatically revoke account permissions after a set period and reset passwords for tighter security.

Data Security Plus

Identify critical files related to healthcare operations associated with discover, assess their vulnerabilities, and categorize them accordingly. Monitor access and changes to these sensitive files and automate responses to security incidents such as ransomware attacks, data exfiltration attempts, abnormal file transfers, and other threats.

Endpoint DLP Plus

Automate content analysis to locate sensitive data, including intellectual property and PII-like patient accounts and ePHI. Set rules for allowed cloud applications and block unauthorized transfers through web browsers to third-party storage.

Log360

Automate the monitoring of log data from firewalls, routers, switches, workstations, servers, and critical applications. Provide notifications for any compliance requirement violations or suspicious data breach activities. Utilize prebuilt compliance reports as proof of adherence to compliance requirements, streamlining security auditing processes.

Use real-time security monitoring to track your VPN connections and look for suspicious remote logons.

Detect suspicious software and service installations in your network by utilizing the rule-based correlation engine.

Utilize advanced threat analytics (ATA) technology and MITRE ATT&CK capabilities to detect internal and external threats.

Spot signs of insider threats and account compromise by monitoring activities like unusual system accesses, unusual access times, unusual file accesses or modifications, excessive authentication failures, unusual software installations, and more. Utilize automated incident workflows and the ticketing module to enable faster threat response and remediation.

EventLog Analyzer

Track and review log data for compliance purposes.
Easily generate detailed reports in any format, customize templates, and store data for specific time periods to meet regulations.

OpManager Plus

Obtain real-time insights and a comprehensive view of the health, availability, and performance of your entire network components, including routers, switches, firewalls, and resolve potential issues before they impact patient care.

Investigate specific security incidents by analyzing firewall logs. Security teams can use the search and filter options to identify potential attack patterns or anomalous behavior.

Endpoint Central

Provide secure, role-based access to protect patient privacy. Set installation permissions, monitor privileges, and ensure Zero Trust security with role-based and time-based privileges.

Define staff roles and responsibilities clearly, and assign appropriate privileges based on these roles. Provide access permissions to temporary accounts, such as consultants, contractors, and temporary healthcare staff, to ensure they can access necessary medical and administrative systems within the specified time frame.

Regularly assess and manage access levels for contractors and temporary healthcare staff, ensuring they have appropriate system entry to perform their duties effectively while maintaining the security and confidentiality of patient data, and efficiently handling access provisioning and deprovisioning processes.

Use application-centric privileges to control staff access to specific applications. Permit only approved applications and block any suspicious ones.

Allow staff to use personal devices for work while ensuring they are secure and compliant with industry guidelines for handling PHI. When an employee leaves, remotely wipe corporate data from their device to protect sensitive information.

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, Active Directory, 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.



Trusted by



















For more information:

www.manageengine.com | sales@manageengine.com