ManageEngine
Log360

Establishing a least privilege

environment in healthcare organizations: The right access control policies to thwart security breaches

https://www.manageengine.com/log-management/healthcare-security-compliance.html

Table of Contents

The clear and present cyber risk in healthcare

With valuable data containing patients' medical history, prescription details, scan reports, and test results, the healthcare industry is arguably more at risk from security breaches than any other industry. One study suggests that health records can be sold for up to $1,000 on the dark web, as opposed to financial records, which can be sold for only a few dollars.1 The gravity of the problem is apparent when considering that more than 13 million healthcare records were breached in 2018.2 The risks will only continue to grow due to an increasing number of connected medical devices and an ever-evolving threat landscape filled with sophisticated attack techniques.

As things currently stand, healthcare organizations should do a lot more to improve their security posture. According to the Cost of a Data Breach report by Ponemon Institute, it takes 358 days on average to identify and contain a data breach in the healthcare industry.3 This means that attackers can lurk in the network for as long as one year, gradually escalating privileges, moving laterally, and exfiltrating sensitive data before they're stopped. Only the entertainment industry faces a bigger challenge when it comes to identifying and containing a breach.4

To mitigate the risk of a security breach, healthcare organizations must take the necessary steps and implement the correct processes to deter attackers. This includes having the right technology in place to detect the telltale signs of a breach at the reconnaissance stage; using tools to respond in case a breach occurs; being able to perform forensic and root cause analysis to go back in time, trace different actions, and learn how the breach occurred; and finally, organizations must address and fix the discovered vulnerabilities to improve their security posture. There is another major step healthcare organizations can take to thwart attackers, and that is establishing least privilege security. Figure 1 shows what actions healthcare organizations must take to secure themselves from security attacks.

Figure 1: What healthcare organizations must do to protect themselves against attacks.

In this e-book, we'll address how to thwart attackers—both malicious insiders and external hackers—by establishing a least privilege environment. We'll see what this means for a healthcare organization, and how they can go about implementing least privilege.

What is an environment of least privilege, and what are the benefits?

An environment of least privilege is one in which all users, programs, systems, or processes in an organization receive only the minimum privileges needed to perform their job or function. For example, a front-end employee at a hospital shouldn't have access to patients' X-rays. Similarly, a third-party medical supplies vendor shouldn't have access to insurance details. Establishing a least privilege environment goes a long way in safeguarding stakeholders' privacy and the security of the organization as a whole.

Here are the benefits of following the principle of least privilege:

- **Maximizes business productivity:** Many end users may feel that an environment of least privilege curtails their productivity; there could be times when a user is in the middle of some critical work, and they face a disruption due to not being able to access a particular application. However, if least privilege is implemented and enforced properly, such disruptions would never occur.

  In fact, by improving security, least privilege ensures that all business-critical applications are always up and running and employees can focus on their work, leading to happier employees and increased business productivity.

- **Improves adherence to compliance regulations:** There are several industry standards and regulations that organizations need to adhere to; in the healthcare industry, these include the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These regulations clearly establish protocols for the sharing and accessing of sensitive information, and protect consumers in case their data falls into the wrong hands. Failure to protect electronic protected health information (ePHI) can lead to huge fines.

By adopting least privilege security, organizations can establish policies to define who has access to what resources. They can also go one step further and define whether users have read-only access, or if they can modify, copy, and delete information. In this way, companies can minimize network communications to only what is necessary, and decrease the number of negative audit findings.

- **Deters attackers:** The best way to stop a cyberattack is to prevent it from ever happening. Attackers are always on the lookout for over-privileged users whose accounts can be compromised. Least privilege eliminates users and systems with privileges they don't need. For example, does a cardiologist require local admin privileges on their laptop? Is there a risk of an attacker performing a local admin rights takeover, and stealing sensitive information through this route?

  In today's era of digital transformation, an organization's perimeter extends beyond the brick and mortar, widening the attack field. Least privilege security makes it harder for criminals to infiltrate the extended perimeter. Anytime a workload fails to match the privileges given, its communication with the rest of the system is halted. Any alteration, whether from an accident, misuse, or adversarial activity, is a signal for automatic distrust by the system until the situation is corrected with prescribed policies. This goes a long way in deterring attackers.

- **Optimizes identity management:** In an organization that enforces least privilege, each unique user is mapped to one single identity. In this way, it's simple to track which user performed which action.

  For example, in a physiotherapist's clinic, there could be multiple front-end employees who work different shifts. If all of them are provided with the same logon credentials, it would go against the principles of least privilege. In addition, it could be very cumbersome to track who did what, when, and on which server. It's always better to tie a digital identity to each user and track all of their actions within the organization's perimeter. This means that authentication and authorization have to happen at each step. Figure 2 below summarizes the discussion about the benefits of adopting least privilege.

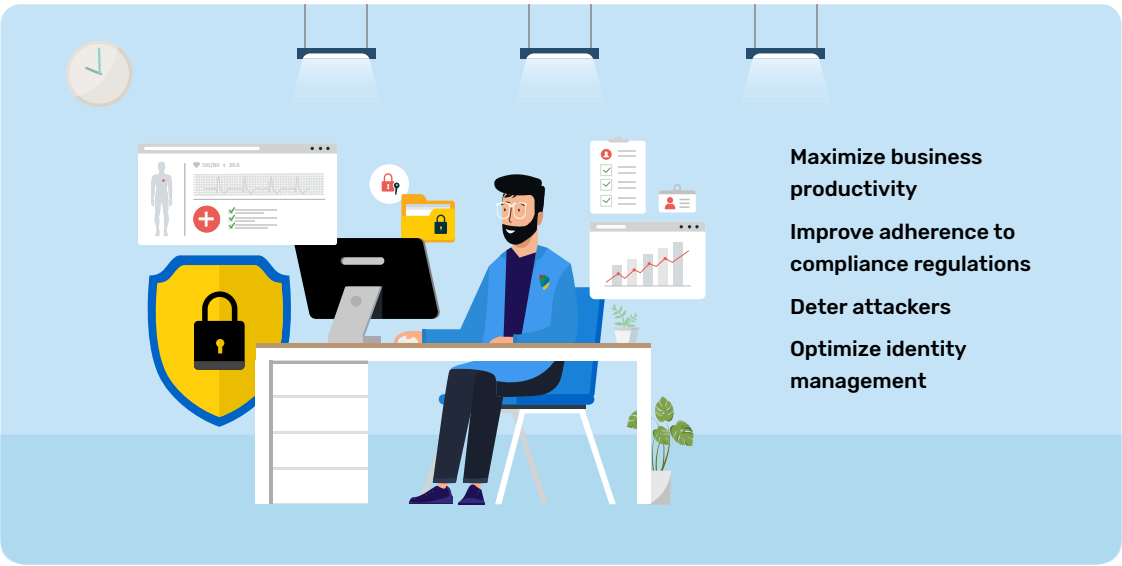


Figure 2: The benefits of implementing least privilege security.

What does least privilege mean for a healthcare organization?

Imagine a dubious situation for a moment: A hospital has only one employee, a doctor, who works the 9am to 5pm shift. Establishing an environment of least privilege becomes very simple in this situation. We'd need to ensure that this doctor gets physical access into the hospital, and is able to log on to their workstation, view the right files and folders, use specific connected medical devices, access certain applications, and view patient health records.

But in reality, a hospital is a complicated world. There are numerous departments like neurology, oncology, cardiology, psychiatry, and orthopedics. There are multiple types of users who are directly involved in healthcare like doctors, nurses, therapists, medical assistants, lab technicians, medical interns, and pharmacists. And then, there are also other users from departments like finance, human resources, marketing, IT, facilities, and administration. All of these users require access to different types of data to do their jobs effectively. At the same time, care must be taken to ensure that data is not unnecessarily and carelessly exposed to people who don't need it.

The hospital must also take into account employees who are transferred to a different department. For example, if a lab technician transfers from the oncology department to cardiology, they may require a completely different set of access privileges and permissions.

In this situation, there must be a process to revoke the older permissions and grant new ones. Just like transfers, hospitals must also account for users who leave the organization. The last thing any healthcare organization wants is an attacker compromising an ex-employee's account to access sensitive health records.

Least privilege security goes beyond just taking care of user accounts. In any healthcare organization, there are multiple systems that access other systems. For example, a connected medical device like an infusion pump may access a patient's health vitals stored in a particular database to administer the right dosage of a drug. IT teams must therefore ensure that each system only gets access to the data it needs.

How healthcare organizations can establish a least privilege environment

There are many ways healthcare organizations can establish an environment of least privilege. However, in this e-book, we'll go over a data-centric approach, assuming sensitive data is the most important asset to protect in a healthcare organization.

Here are the steps to implement least privilege in a healthcare organization:

1. **Perform a data risk assessment:** A data risk assessment enables the organization to identify and take inventory of all business-critical data, including health data that it holds. According to the McGraw-Hill Concise Dictionary of Modern Medicine, health data is any information related to health conditions, reproductive outcomes, causes of death, and quality of life.5 Apart from identifying all data assets, the organization must also assess the negative business impact in case of a compromise.

   Table 1 illustrates how this can be done. For each identified data asset, we need to estimate the risk and cost of a compromise. The estimate is more qualitative than quantitative, and will need an assigned value of High (H), Medium (M), or Low (L). The estimated business impact will simply be a product of the estimated risk and cost. Organizations have to take time and effort to identify all their data assets at this stage. The first line has been filled as an example. There are solutions that can scan an entire network, including different file servers, to identify specific types of data.

Data asset	Description	Level of risk (High, Medium, Low)	Estimated cost (High, Medium, Low)	Business impact (High, Medium, Low)
X-ray reports	X-ray reports of patients	M	M	H
Lab test results				
Genetic information				
Prescription history				
Financial information				

Table 1: Performing a data risk assessment.

2 **Associate groups and systems with data assets:** Next, organizations need to prioritize the data assets for which they need to establish least privilege. For each data asset, they need to clearly define the privileged groups and systems that have access and privileges. There are solutions that can help with this.

Table 2 illustrates how this can be done. This framework may need to be tweaked based on an organization's specific needs. For example, a multi-specialty hospital may have several radiologists working in several departments. A radiologist from the oncology department would never need access to reports that a radiologist from pediatrics has prepared. So, the organization must account for similar types of data existing across departments, and decide which access privileges need to be different. The first line has been filled as an example.

Priority	Data asset	Associated groups	Associated systems	Department	How is this data accessed (cloud, on-premises)?
1	X-ray reports	Lab technicians, radiologists		Oncology, Pediatrics, Cardiology, Orthopedics	Cloud, on-premises
2	Lab test results				
3	Genetic information				
4	Prescription history				
5	Financial information				

Table 2: Associating groups and systems with specific data assets.

3 **Continuous monitoring and verification:** The organization must then clearly define the extent of privileges that each group gets. This is where privileged access is distinguished from least privilege. While privileged access is concerned with whether a user has view or access privileges, least privilege is concerned with more granular privileges such as write, modify, delete, move, and copy-and-paste.

Table 3 shows how a healthcare organization can do this. Again, please note that we are simplifying the model here to illustrate how it works; it may need to be modified to suit the requirements of an organization. The first line has been filled as an example.

Priority	Data asset	Associated group 1	Associated group 2	Associated group 3
1	X-ray reports	Read only	Read, write	All privileges
2	Lab test results			
3	Genetic information			
4	Prescription history			
5	Financial information			

Table 3: Setting privileges for user groups.

All privileged actions must be continuously monitored so the IT administrator can be notified in case of any privilege escalation. If privilege escalation does occur, there must be measures in place to distrust the associated user account immediately. This distrust should continue until the user verifies the account once again and authenticates themselves.

Apart from rule-based monitoring, in which IT administrators have to constantly look for security thresholds that are breached, healthcare organizations can also implement advanced security analytics systems powered by machine learning algorithms. This is called user and entity behavior analytics (UEBA), and has become a necessary tool in the security arsenal of any company. UEBA monitors the regular activities of each user and entity, and creates a baseline. Any activity that deviates from this baseline gets flagged as an anomaly. The IT administrator can then investigate the issue and take the necessary steps to mitigate the risk. UEBA solutions grow more effective the more experience they gain.

Use case

UEBA in action in healthcare: Blocking the sale of illicit information

Mark Carter is a med student at Chicago Hope Hospital. In dire need of money, he steals patient information by sneakily copying it to a USB device after his shift ends at 5pm. He plans to sell the illicit information on the black market for a good price.

But wait! Chicago Hope Hospital utilizes a UEBA solution, which monitors the behavior of every entity and user that belongs to the hospital network. Carter tries to copy critical information to his device at 7pm, but UEBA detects pattern and time anomalies, and increases his risk score substantially.

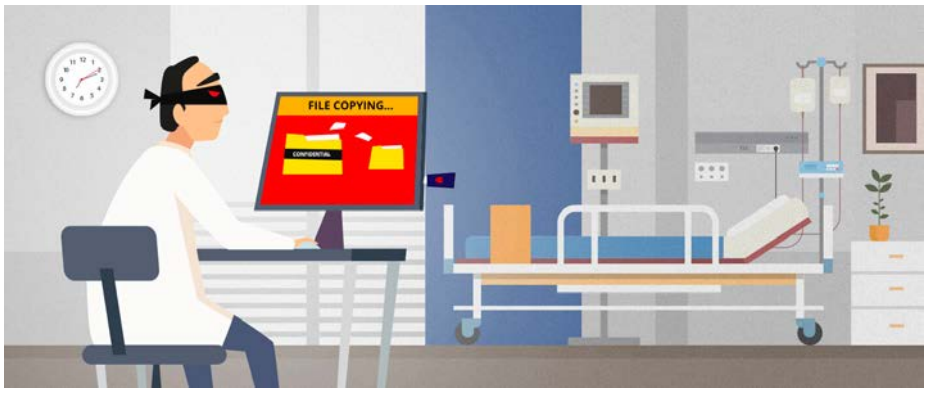


Figure 4: Dr. Carter tries to exfiltrate critical data.

Despite having the necessary access permissions, his risk score is increased because his actions deviate from his usual behavior, which typically includes viewing, creating, and editing patient records only between 9am and 5pm. The IT security officer notices the abnormal risk score spike in the UEBA portal, and Carter's user account permissions are immediately revoked. His hard disk is confiscated, and the hospital initiates legal actions against him.

Read more interesting use cases about UEBA at:
https://www.manageengine.com/log-management/ueba/resources.html

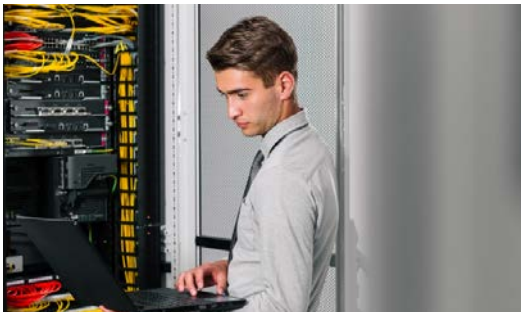
Best practices for implementing least privilege in your organization

Here are a few more best practices that healthcare organizations can adopt as they establish a least privilege environment:

Have clear processes and procedures in place for creating and deleting user accounts: The processes for user account creations and deletions must be clearly defined. Organizations must plan for role changes, department changes, promotions, new recruits, and people who leave.

Standardize a limited number of user account types: To ensure privacy and safety, it's important for healthcare organizations to standardize a limited number of user account types. This will ensure that user accounts with various permission levels and attributes are not unscrupulously created. Organizations need a way to audit all modifications to user attributes.

For example, all medical interns in a hospital should have a common user creation template to give them all the same permission levels and security attributes. Organizations should deviate from these standard templates only if they really need to.

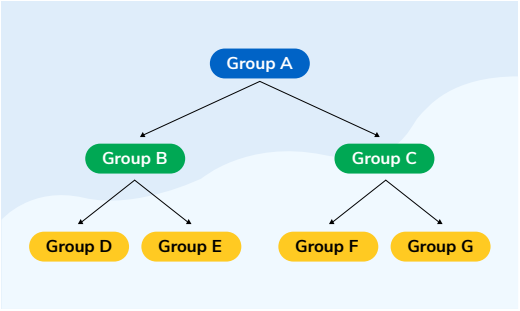


Limit the number of users with administrator accounts: Administrator accounts are the most privileged accounts in any organization. It's imperative that organizations limit the number of administrator accounts and the number of people with full administrator privileges. Moreover, these accounts must only be used for truly privileged actions and not for day-to-day tasks.

Organizations must also have a mechanism to audit all the administrative user actions that take place in their environment.

Make optimum use of groups: Organizations must never set privileges for a single user account. Privileges must always be given to a security group, even if it's a group of one. If this is not done, it may become difficult to track who has access to what resource. Moreover, IT administrators would then need to go into each user account and set permission levels individually. It's simpler to manage the permissions for a group and add users to the group. In case a user transfers into a different department, the IT administrator would simply need to move the user into a new group without doing anything else.

Discover privileged accounts continuously: This will enable organizations to find out if a particular user still requires privileges over a specific data asset. For example, there are cases in which a general physician may collaborate with a cardiologist for an expert opinion about the health of a patient. And for a period of time, the cardiologist may need access to some of the patient's medical records. However, the access must end once the collaboration is over.



Don't forget about inherited privileges: Child processes usually inherit the permissions of parent processes. It's critical for healthcare organizations to identify all child processes and ensure that their permissions are set properly. For example, there could be a parent group called "Medical interns," and a child group called "Radiology interns." Not all the privileges of the former need to be inherited by the latter. Organizations need a mechanism to assess the privileges of nested groups and monitor user actions.

Securing your organization with ManageEngine Log360

Log360 is a comprehensive security information and event management (SIEM) solution that helps enterprises detect data breaches, ensure the security of stored patient data, and track each and every access to personal data. It also tracks critical changes to the files and folders where personal data is stored.

Here's a closer look at some of Log360's features that can help healthcare organizations tighten their security:

Real-time Active Directory (AD) auditing: Log360 aggregates security log data from different domain controllers to centralize AD audit information. Administrators can track important changes made to AD objects, including users, computers, groups, organizational units (OUs), and Group Policy Objects (GPOs), and get real-time alerts about critical changes. If access permissions are changed and privileges are escalated in AD, administrators will receive real-time notifications and can investigate if it's a threat.

Real-time network device auditing: Log360 can analyze syslogs generated by network perimeter devices, including routers, switches, firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs), in real time. Administrators can track configuration changes—such as rule modifications, links that are up or down, denied and accepted firewall connections, and IDS/IPS alerts—all from a single console. This helps in mitigating data breach risks that originate outside the business' network.

Discover data: With Log360, administrators can find, analyze, and track sensitive personal data—such as electronic health records—stored in files, folders, or shares. This will prove beneficial when dealing with requests from consumers on data deletion and data access.

Audit file servers: Companies can monitor, report on, and receive real-time alerts for changes made to files and folders in file servers. This is how Log360 maintains the integrity of data and ensures it's not being misused. In addition to this, Log360 can thoroughly audit activities on your files and folders in Windows and Linux devices.

Every access, creation, deletion, modification, and permission change made to files and folders can be tracked to ensure the security of confidential data. Figure 3 shows the file integrity monitoring report available in Log360. Using this report, administrators can quickly investigate if sensitive data has been leaked.

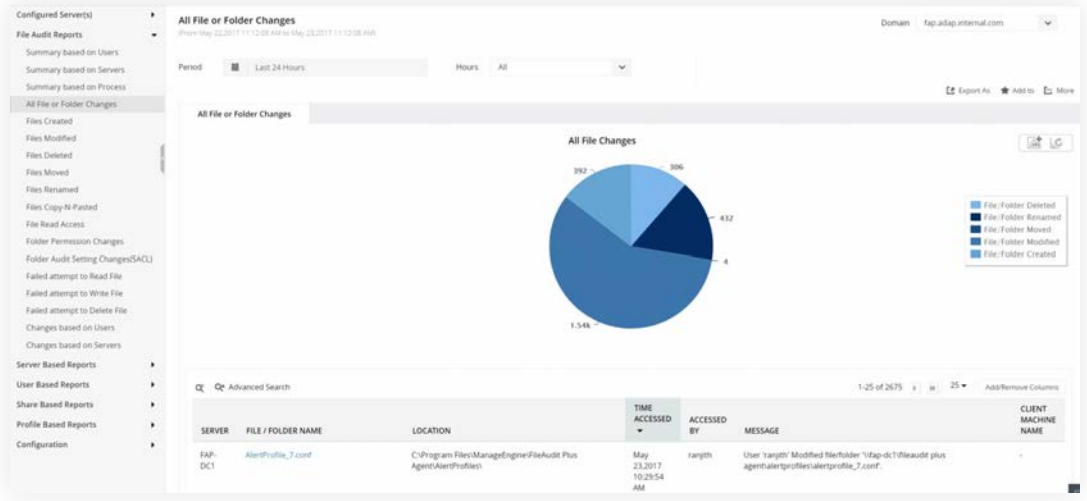


Figure 3: File integrity monitoring in Log360.

Conduct audit trails: Log360's log search capability makes forensic analysis easy (Figure 4 shows the ElasticSearch module of Log360). One of the requirements of HIPAA is quickly stopping a breach or breach attempt. This can be accomplished by finding the root cause of any security issue. Log360 can help find the root cause of a data breach by searching terabytes of log data within minutes. The solution also provides an option to export the search results as a forensic report.

Figure 4: ElasticSearch in Log360.

UEBA: Powered by machine learning, Log360's UEBA module grows more effective the more experience it gains. A risk score is calculated for each user and entity in the organization after comparing their actions to their baseline of regular activities. The risk score can range from 0 to 100, indicating no risk to maximum risk, respectively. If the IT administrator feels an entity or user's risk score is too high, they can investigate it further and quickly stop any potential catastrophes.

For example, the chief of medicine of a hospital may usually log on to the network between 9am and 6pm, and the system would learn that this is their “normal” behavior. If this user logs on to the network at 12:30am, it would then be treated as an anomaly and their risk score would be increased.

About ManageEngine

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our 90+ products and free tools cover everything your IT team needs at prices you can afford.

From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT.

$ Get Quote Download

References

1. Mariya Yao, "Your electronic medical records could be worth $1000 to hackers," *Forbes*, April 14, 2017, https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#3687c24f50cf.

2. HIPAA Journal, "Analysis of 2018 healthcare data breaches," *HIPAA Journal*, January 28, 2019, https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/.

3. Ponemon Institute LLC, "2018 Cost of a data breach study: Global overview," *IBM Security*, July 2019, https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

4. Ibid.

5. McGraw-Hill Concise Dictionary of Modern Medicine, "Health data," The McGraw-Hill Companies Inc., 2002, https://medical-dictionary.thefreedictionary.com/health+data.