Authomize HITRUST

Protecting Healthcare Providers from Identity-Based Attacks with ITDR

Protecting Health Information with HITRUST

The healthcare industry is under a constant barrage of data security attacks with near daily reports of breaches across the world. Electronic Medical Records (EMR) containing personal healthcare details, as well as additional personally identifiable information (PII) and payment information, have made healthcare a prime target for malicious insiders and external hackers alike.

In light of the rise in risks to their data security, 80% of U.S. hospitals and 85% of U.S. healthcare industry organizations have turned to the Health Information Trust Alliance Certification Standard Framework (HITRUST CSF) to meet their HIPAA compliance requirements and secure their patients' data. HITRUST CSF is a widely accepted framework for addressing information security in the healthcare industry. It combines requirements from multiple standards and regulations, including HIPAA, ISO 27001, NIST 800-53, PCI DSS, and SOC 2.

Identity Threat Detection and Response (ITDR) Can Help

ITDR is a new cybersecurity discipline aimed at protecting organizations from Identity-based threats like insider threats, account takeovers, and privilege escalations. Securing identities and access privileges is essential for mitigating cyberattacks and protecting Healthcare information. ITDR platforms bridge the gap between identity and security to ensure that risks and threats are discovered, investigated, and mitigated in-line with your security operations.

> **The team used Authomize** to gain deep visibility into our access policies in AWS, GitHub, and Okta, as well as automate and centralize access reviews, saving valuable time and manual efforts."

Paul Ellis Head of Information Security Curebase

Read More

Authomize is the first agentless ITDR platform that empowers customers to achieve Least Privilege across cloud services and applications and secure their IAM solutions from threats of user impersonation and accounts takeover.

Achieve Least Privilege and Establish a Secure Access Baseline

(HITRUST 01.b User Registration, 01.c Privilege Management, 01.e Review of User Access Rights)

To ensure that the allocation and use of privileges is restricted to Just Enough Access, Authomize detects and eliminates risks of stale access, over-privileges, and privilege escalation paths across cloud services (IaaS) and cloud applications (SaaS). Authomize also detects and mitigates misconfigurations and trust manipulations in critical identity and access management (IAM) infrastructure to block active account takeover and admin impersonation threats. Authomize collects and visualizes granular identity, access privilege, asset, and usage data to continuously monitor for risks and threats, and to automate the attestation of user access rights based on proprietary ML-based recommendations (SmartGroups).

Harden Security Posture by Monitoring Lifecycle Changes

(HITRUST 02.g Termination or Change Responsibilities)

Authomize eliminates privilege sprawl and partial offboarding by continuously monitoring granular identity, access, and usage data from HR systems, IAM solutions, and cloud services and applications. Authomize detects lifecycle changes (JML = Joiner-Mover-Leaver) and stale access to ensure that employees and external contractors do not hold access privileges that they no longer require. Authomize collects and unifies identity and access data from a wide range of systems, including "Bring Your Own Identity" applications like GitHub, and is easily extendable to any application (including homegrown) with an open API.

Automate Remediation and Incident Response

(HITRUST 11.0 Information Security Incident Management)

Authomize detects identity risks and threats and provides automated remediation and response workflows to ensure that risks are eliminated and threats are mitigated. In addition to inherent reporting and remediation, Authomize integrates easily with SIEM, SOAR, and XDR solutions to ensure a standard procedure for handling identity and access incidents.

Benefits

- Uncover and eliminate Identity-based risks to Health Information
- Cut on audit preparation efforts with automated User Access Reviews
- Achieve Least Privilege across cloud services and applications
- Detect and mitigate active threats to your identity infrastructure
- Automate remediation and incident response to protect against cyberattacks
- Incorporate identity context into security operations to prioritize based on blast radius

Run a Health Check for Your Health Information

Sign up for the Free Assessment ›