Ping Identity

Increasing Healthcare Security Behind and Beyond the Firewall

How to Prevent Breaches With Unified Identity and Access Management

WHITE PAPER

Increasing Healthcare Cybersecurity Behind and Beyond the Firewall

The healthcare industry continues to be the prime target for cyberattacks. According to the 2023 Ping Identity Breach Report (formerly ForgeRock), healthcare has been the most targeted industry by cybercriminals for over five years.[1] This trend persists in 2024, with high profile attacks that have caused widespread disruption[2]. One breach, orchestrated by the Blackcat ransomware group, affected up to one-third of Americans and led to significant financial and operational impacts, with disruptions costing healthcare providers as much as $1 billion a day. Another attack disrupted services across 140 hospitals, cutting off access to electronic health records and delaying patient care.

37% of healthcare organizations remain unprepared for cyberattacks[3]

Healthcare's Lack of Preparedness

According to KLAS, "[healthcare] organizations are generally more reactive than proactive in their approach to cybersecurity." Despite the increasing threat landscape, more than a third of healthcare organizations remain unprepared for cyberattacks. This lack of readiness is concerning, especially given that 34% of organizations that experienced ransomware attacks failed to recover patient data.[4] The consequences of these attacks are severe. According to the Journal of mHealth, "of the 88% of healthcare organizations that experienced cyberattacks in 2023, roughly 20%-30% reported more fatalities as a result."[5]

Unauthorized Access As Enemy Number One

Unauthorized access remains the primary attack vector contributing to data breaches in the healthcare industry. The 2024 Verizon Data Breach Investigations Report reports that the "use of stolen credentials continues to dominate the System Intrusion pattern."[6] The most significant healthcare breach in 2024 is a notable example, where a lack of Multi-Factor Authentication (MFA) facilitated unauthorized access, leading to a nationwide outage and exposure of sensitive patient data. At the time of this paper, that single breach is estimated to cost the organization over $2.45 billion[7].

A healthcare ransomware attack by ALPHV/BlackCat in 2024 is estimated to cost over **$2.45 billion**[8]

[1] https://www.pingidentity.com/en/resources/content-library/analyst-reports/3763-2023-forgerock-identity-breach-report.html

[2] https://www.pingidentity.com/en/resources/blog/post/healthcare-cyberattacks-security.html

[3] https://www.healthcaredive.com/news/healthcare-ransomware-cyberattack-impacts-patient-care-software-advice/716971/#:~:text=from%20your%20inbox.,More%20than%20a%20third%20of%20healthcare%20organizations%20aren't%20prepared,new%20survey%20from%20Software%20Advice.

[4] https://www.morningstar.com/news/business-wire/20240521811121/more-than-one-in-four-ransomware-attacks-on-healthcare-providers-impact-patient-care

[5] https://thejournalofmhealth.com/the-link-between-health-care-cyberattacks-and-patient-mortality/

[6] https://www.verizon.com/business/resources/reports/dbir/

[7] https://www.beckershospitalreview.com/cybersecurity/change-healthcare-cyberattack-costs-soar-may-hit-2-45b.html#:~:text=UnitedHealth%20Group%20expects%20costs%20associated,at%20%241.6%20billion%20this%20year.

[8] https://www.beckershospitalreview.com/cybersecurity/change-healthcare-cyberattack-costs-soar-may-hit-2-45b.html#:~:text=UnitedHealth%20Group%20expects%20costs%20associated,at%20%241.6%20billion%20this%20year.

Internal and Third-Party Threats

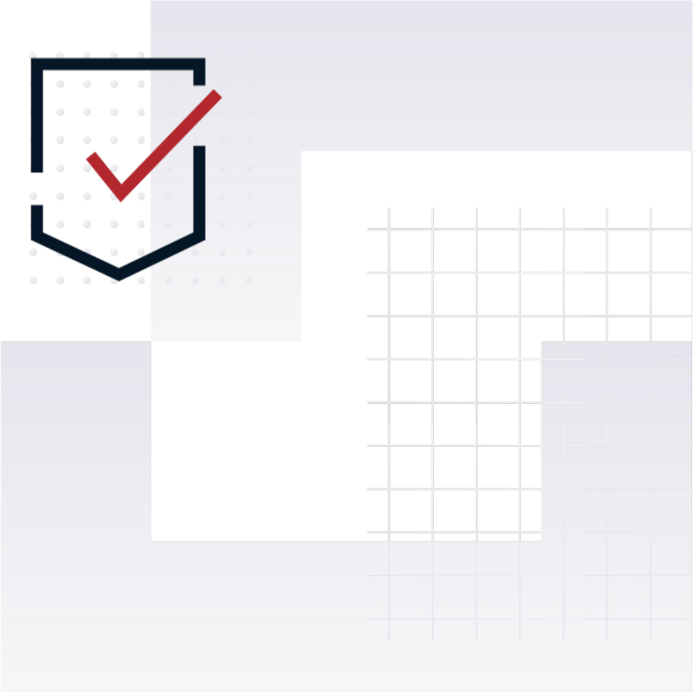
According to Morningstar, 55% of healthcare organizations allow employees to access more data than necessary for their job roles.[9] This is likely the reason why insiders are the second cause of breaches[10], highlighting the need for more stringent identity and data governance measures[11].

55% of healthcare organizations allow employees to access more data than necessary for their job roles[12]

Furthermore, 90% of the largest healthcare data breaches in 2022 were linked to third-party vendors according to Ping's 2023 Breach Report[13]. The interconnected nature of digital health ecosystems and services necessitates robust risk management to prevent breaches that can propagate through third-party endpoints.

EHR Security Capability Gaps

Electronic Health Records (EHR) systems are indispensable tools for managing patient information and streamlining healthcare processes. However, relying solely on EHRs for access and authorization exposes healthcare organizations to significant risks. EHRs native security features lack advanced identity and access management (IAM) capabilities essential for breach and fraud protection. For example, they lack comprehensive identity verification and advanced threat detection capabilities such as bot detection and suspicious device detection. They also don't provide the granularity and flexibility needed to handle the dynamic access needs of modern healthcare environments. As such, healthcare organizations must integrate EHRs with purpose-built IAM solutions to ensure comprehensive security. See the Integration section for details.



[9] https://www.morningstar.com/news/business-wire/20240521811121/more-than-one-in-four-ransomware-attacks-on-healthcare-providers-impact-patient-care
[10] https://www.verizon.com/business/resources/reports/dbir/
[11] https://www.verizon.com/business/resources/reports/dbir/
[12] https://www.morningstar.com/news/business-wire/20240521811121/more-than-one-in-four-ransomware-attacks-on-healthcare-providers-impact-patient-care
[13] https://www.pingidentity.com/en/resources/content-library/analyst-reports/3763-2023-forgerock-identity-breach-report.html

A Unified Identity Security Strategy Is Imperative For Healthcare Cyber Defense

The significant breaches in 2024 highlight the vulnerabilities within the healthcare sector and underscore the critical need for robust, unified identity and access management (IAM) and identity governance and administration (IGA) security strategies.

In today's healthcare environment, traditional security models are insufficient to defend against sophisticated cyber threats. The ever-evolving landscape of cyberattacks necessitates a modern approach where implicit trust is never granted, but continuously evaluated through advanced identity solutions. It is crucial for healthcare leaders to adopt a comprehensive IAM platform that includes IGA in order to secure their operations, protect sensitive data, and adhere to regulations and guidelines such as:

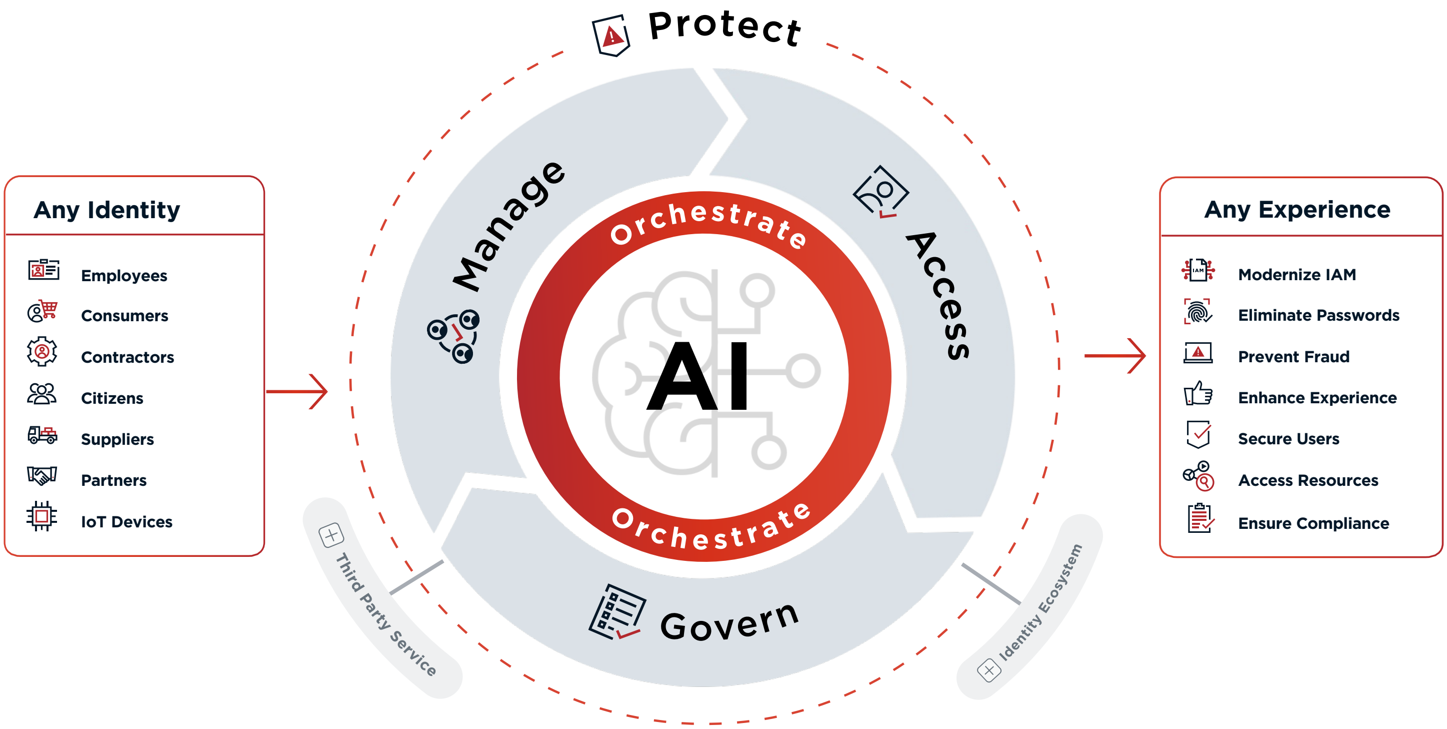
- The Health Insurance Portability and Accountability Act (HIPAA)
- The 21st Century Cures Act
- The CMS Interoperability Mandate
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Trusted Exchange Framework and Common Agreement (TEFCA)
- NIST CSF and NIST SP 800-83
- Center for Internet Security (CIS) Controls
- Health Industry Cybersecurity Practices (HICP)

96% of healthcare executives say their organization's long-term success will depend on next-generation computing, with encryption and cybersecurity at number one[14]

[14] https://newsroom.accenture.com/news/more-than-80-percent-of-healthcare-executives-expect-the-metaverse-will-have-a-positive-impact-on-their-organizations-according-to-a-new-accenture-report.htm

Ping Identity's unified approach to IAM and IGA is the optimal choice for healthcare organizations aiming to prevent cyberattacks without sacrificing user experience due to its comprehensive, adaptive, and policy-based solutions.

The Ping Identity Platform provides end-to-end, scalable, real-time protection against evolving cyber threats, making it indispensable for maintaining the integrity and confidentiality of healthcare information in an increasingly digital landscape.



Any Identity

- Employees
- Consumers
- Contractors
- Citizens
- Suppliers
- Partners
- IoT Devices

Any Experience

- Modernize IAM
- Eliminate Passwords
- Prevent Fraud
- Enhance Experience
- Secure Users
- Access Resources
- Ensure Compliance

Achieve Tangible Results With Ping Identity

$19.2M
annual saving

A $35B organization is saving $19.2M in fraud costs annually with PingOne Verify

120%
improvement in fraud detection

A software platform vendor improved overall fraud detection rates by 120% with PingOne Protect, reducing new account fraud losses

↑ **user registration**

↓ **user frustration**

A senior living center with ~30,000 residents using Ping's Protect and Passwordless Authentication solutions,:

- Increased resident registration and usage of the mobile app
- Reduced user frustration and abandonment
- Reduced technical assistance and password reset costs

Five Pillars Of Identity Security For Healthcare

For healthcare leaders to fully defend against breaches, fraud, and ransomware from both behind and beyond the firewall, the following five pillars of identity-enabled cybersecurity are a requirement.

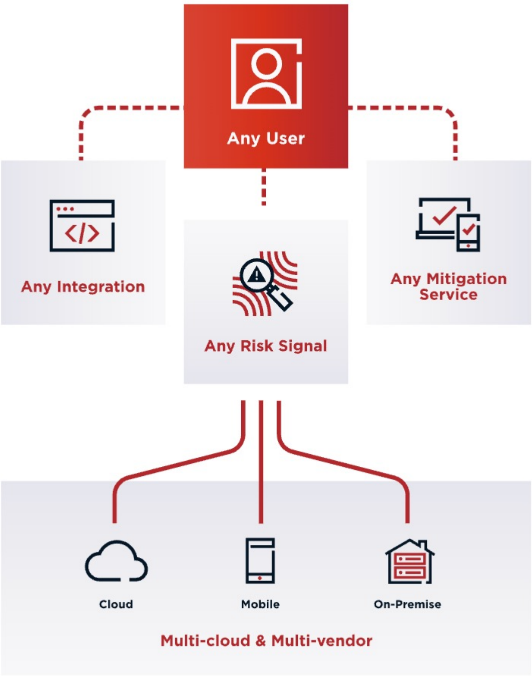
1. Integrate and Augment Disparate Systems and EHRs

The Problem

Healthcare IT consisting of fragmented systems, point solutions, and multiple EHRs is rife with vulnerabilities, such as multiple entry points for cybercriminals. Data silos make it difficult to implement consistent security policies and track user access across the entire organization. This lack of visibility and control over access can lead to over-provisioning, unauthorized access, and internal threats.

The Solution

Ping Identity’s unified, enterprise-grade IAM platform integrates disparate hybrid IT environments and point solutions. The platform includes dynamic authorization and fine-grained access control to ensure secure and compliant access to EHR systems, supporting HITECH privacy and security provisions. And policy-based access control (PBAC) and integration capabilities enable secure and seamless data exchange, aligning with TEFCA interoperability goals. Further, Ping Identity's API security and access management solutions ensure secure data exchange and fine-grained access control to electronic health information (EHI), supporting the CMS and Cures Act's interoperability and data protection requirements.



With Ping Identity, you can:

- Speed security implementation and ensure every endpoint is protected.
- Participate in a Community Connect digital ecosystem.
- Reduce developer overheads and costs by significantly reducing the time to build, test, and deploy integrations.
- Ensure flexibility to implement technologies and adapt user journeys to meet future needs.
- Streamline all identity services and reduce duplicative processes and the costs of maintaining multiple product platforms and their integrations.
- Consolidate identity and access management costs into one platform across all deployment settings and multiple business lines to increase ROI and decrease TCO.

Important Integration Capabilities to Consider

1. Identity Gateway

An identity gateway acts as a centralized access point, managing authentication and authorization, thereby unifying multiple systems under a single identity framework. This ensures that healthcare providers can securely access patient records, clinical applications, and other essential services without compromising security or user experience. By using standardized protocols and APIs, such as OAuth, OpenID Connect, and SAML, the identity gateway facilitates interoperability and data sharing across diverse systems, enhancing operational efficiency and patient care.

2. Centralized Directory

A centralized user directory helps integrate disparate IT systems by providing a unified repository for managing user identities and access permissions. By consolidating user information in a single location, it ensures consistent and up-to-date user data across all integrated systems, simplifying user management and reducing administrative overhead. This centralization allows for seamless authentication and authorization processes, as applications and services can reference the same user directory for identity verification. Consequently, it enhances security and efficiency by enabling single sign-on (SSO), enforcing consistent access policies, and facilitating easier provisioning and de-provisioning of user accounts across various systems, thus creating a cohesive and interconnected IT environment.

3. Lifecycle Management

Lifecycle management in healthcare refers to the comprehensive process of managing the entire lifecycle of identities, from creation and provisioning to modification and eventual de-provisioning. This capability is crucial for efficiently provisioning employees, providers, and patients, ensuring that each individual has appropriate access to necessary resources at all times. Effective lifecycle management supports multiple interfaces for electronic health records (EHRs) and Fast Healthcare Interoperability Resources (FHIR), enabling seamless data exchange and interoperability across systems. This not only enhances operational efficiency but also strengthens security, compliance, and the overall quality of patient care.

4. Standards Compliance

Open standards are publicly available specifications that ensure interoperability and compatibility between different systems and technologies. For healthcare organizations, working with an IAM provider that supports open standards is crucial for seamless integration and secure data exchange. Full support for legacy SAML and the flexibility to support custom SAML integrations ensures that existing systems can communicate effectively with new applications. Additionally, full support for OpenID Connect (OIDC) and OAuth facilitates secure and scalable access management. Comprehensive support for FHIR and SMART on FHIR standards enables the efficient and interoperable exchange of healthcare data, enhancing care delivery and operational efficiency.

5. Policy-Based Access Control (PBAC)

Policy-Based Access Control (PBAC) is a method of regulating access to resources based on policies defined by the organization. This approach is more flexible and context-aware compared to traditional access control methods like Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). PBAC uses policies to determine access rights, which can consider various factors such as user roles, attributes, environmental conditions, and actions.

6. Single Sign-On

Single Sign-On (SSO) is an authentication process that allows users to access multiple IT systems and applications with a single set of login credentials. By enabling users to log in once and gain seamless access to all integrated systems, SSO simplifies the user experience and enhances productivity, as users do not need to remember and manage multiple passwords. This unified access mechanism not only improves security by reducing the risk of password-related breaches but also allows IT administrators to centrally manage and enforce security policies across diverse systems. By leveraging identity federation protocols such as SAML, OAuth, and OpenID Connect, SSO facilitates the integration of disparate IT systems, creating a cohesive and efficient authentication environment.

7. API Security

API security is essential for protecting applications and data, involving strategies like robust authentication, authorization, and encryption. Utilizing standards such as OAuth, API Keys, and JWTs ensures secure access and data transmission. Implementing rate limiting, input validation, and comprehensive logging helps mitigate threats and monitor API usage. Tools like API gateways centralize security management, while secure coding practices and regular audits prevent vulnerabilities.

8. IoMT / Edge Security

Edge security refers to the protection of data and applications at the edge of the network, closer to where data is generated and used, such as Internet of Medical Things (IoMT) devices. For healthcare organizations, working with an IAM provider that offers edge security is vital to safeguard sensitive information and ensure the integrity of connected medical devices. By securing data and operations at the edge, organizations can ensure that sensitive information is protected as it moves between different systems and devices, facilitating the integration of disparate IT systems. Edge security helps maintain data integrity and privacy across a distributed network, enabling seamless and secure communication between various applications and services.

2. Support A Zero Trust Security Framework

The Problem

Remote work, IoMT such as remote patient monitoring (RPM), and increased endpoints make traditional healthcare security models obsolete. Perimeter-based approaches to security don't sufficiently thwart bad actors. Healthcare organizations need a modern approach to security where implicit trust is no longer granted, but instead continuously evaluated with modern identity.

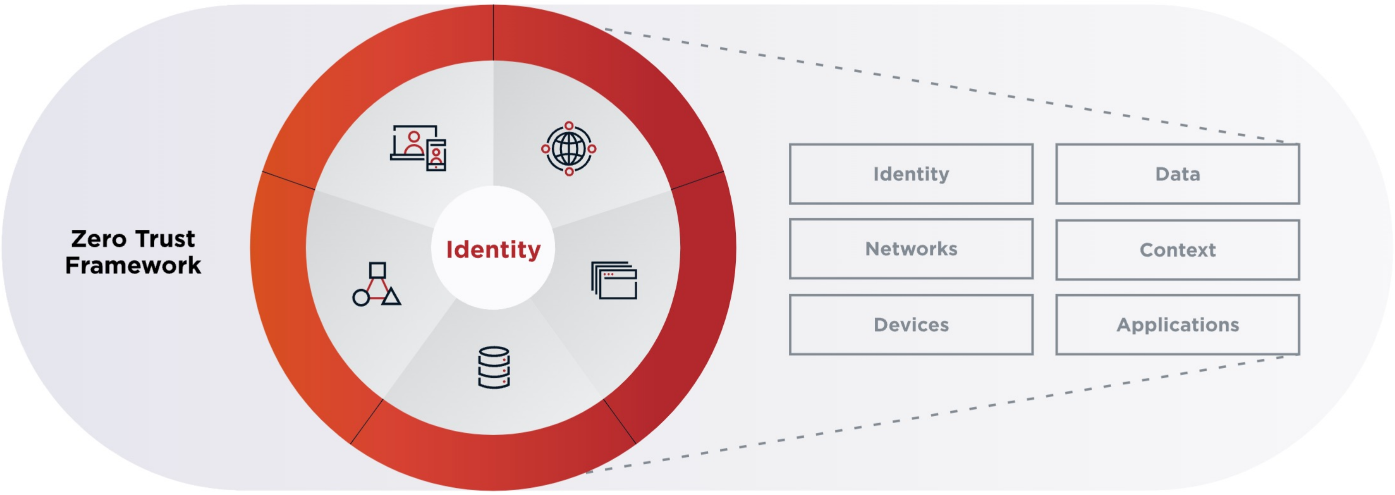
Complicating matters, a lack of visibility into identity management also creates significant organizational blind spots in understanding and controlling user access across the entire IT landscape. This absence of oversight can lead to undetected access anomalies, unauthorized privileges, and increased vulnerability to attack vectors like insider threats.

The Solution

Take the burden out of achieving Zero Trust with the Ping Identity Platform by integrating new vendor solutions with ease, increasing access oversight organization-wide, and incorporating best-of-breed access management methodologies. For example, Ping Identity's multi-factor authentication (MFA), passwordless authentication, and single sign-on (SSO) solutions ensure secure access to PHI, helping organizations meet HIPAA's access control and data protection standards. Dynamic authorization and fine-grained access control also ensure secure and compliant access hybrid IT systems, supporting HITECH's privacy and security provisions. And advanced monitoring tools and integration capabilities help healthcare organizations detect and respond to suspicious activities, supporting the continuous monitoring and improvement requirements outlined in NIST SP 800-83.

With Ping Identity, you can:

- Establish Identity as the new perimeter
- Simplify vendor integration along the journey to Zero Trust
- Facilitate the addition of new Zero Trust technologies with hundreds of third-party pre-built services and out-of-the-box workflows
- Gain comprehensive oversight into identity management for centralized visibility and security control



Important Zero Trust Capabilities to Consider

1. Multi-Factor Authentication (for all user types)

Multi-Factor Authentication (MFA) enhances security by requiring consumers, employees, and partners to provide additional forms of identification, such as a password and a fingerprint or a security token. This layered approach ensures that even if one credential is compromised, unauthorized access is still prevented without the other required factors.

Implementing MFA can significantly bolster security within a zero trust framework, which is crucial for protecting sensitive data. By demanding multiple user-specific credentials, MFA greatly complicates the efforts of hackers. They would need to bypass several layers of security, such as a password, a biometric scan, and a physical security token, making unauthorized entry exponentially more difficult. This heightened level of security is essential for safeguarding healthcare information and maintaining compliance with stringent regulatory standards.

2. Passwordless Authentication (for all user types)

Password-based authentication is high risk and doesn't deliver a great user experience. Passwordless authentication is a way for healthcare consumers, employees, and partners to sign in to digital accounts without using a password, enhancing both security and user experience. Traditional passwords, known as "knowledge factors," are vulnerable to sharing, insecure storage, phishing, and malware. Passwordless authentication eliminates these risks by relying on "possession factors" (something a user has, like a mobile device) or "inherence factors" (something a user is, like a fingerprint). This approach not only improves security by removing the risks associated with passwords but also enhances user experience by eliminating the need to remember and enter passwords. Additionally, it reduces the IT burden and costs associated with password management and help desk calls for password resets, providing a more efficient and secure authentication method for healthcare organizations.

3. Single Sign-On

Single Sign-On (SSO) is an authentication process that allows users to access multiple IT systems and applications with a single set of login credentials. By enabling users to log in once and gain seamless access to all integrated systems, SSO simplifies the user experience and enhances productivity, as users do not need to remember and manage multiple passwords. This unified access mechanism not only improves security by reducing the risk of password-related breaches but also allows IT administrators to centrally manage and enforce security policies across diverse systems. By leveraging identity federation protocols such as SAML, OAuth, and OpenID Connect, SSO facilitates the integration of disparate IT systems, creating a cohesive and efficient authentication environment.

4. Endpoint Verification

Endpoint verification is a critical security practice in a zero trust strategy for the healthcare industry, ensuring that each endpoint is controlled by the appropriate person. This involves both the user and the endpoint presenting credentials to the network, adding an extra layer of authentication. Users must authenticate themselves before accessing any endpoint, and each endpoint must also authenticate itself before gaining network access. The network sends a verification request to the device, prompting the user to respond. The data received is used to determine the endpoint's validity, and successful verification grants the device "trustworthy" status.

Unified Endpoint Management (UEM) centralizes IT infrastructure management by providing a single set of tools to manage various endpoints. Additionally, Endpoint Detection and Response (EDR) enhances security by continuously scanning endpoints, identifying threats, and taking necessary actions to protect the device and the network, functioning similarly to advanced antivirus software. This comprehensive approach is essential for maintaining robust security and protecting sensitive patient data in healthcare environments.

5. Least-Privileged Access

In the healthcare industry, adopting a zero trust model with least-privilege access is crucial for safeguarding sensitive patient data and critical infrastructure. This approach ensures that users and devices are granted access only to the resources necessary for their specific tasks, significantly reducing the potential entry points for hackers. By limiting access in this way, healthcare organizations can make it more challenging for unauthorized users to infiltrate their systems. Additionally, implementing least-privilege access can lead to time and resource savings by minimizing the need for extensive multi-factor authentication measures, thereby reducing the volume of identification credentials that need to be issued and managed. This not only enhances security but also streamlines operational efficiency, allowing healthcare providers to focus more on patient care.

6. Fine-Grained Access Control

Fine-grained access control is a security approach that allows precise, detailed management of user permissions, ensuring that access to resources is granted based on specific attributes and contextual factors. Unlike coarse-grained access control, which typically grants broad access based on roles or groups, fine-grained control evaluates a range of criteria such as user roles, the resource being accessed, the action being performed, and the context of the request (e.g., time, location, device). This method enhances security by enforcing strict policies and reducing the risk of unauthorized access, thereby ensuring that users have the minimum necessary permissions to perform their tasks.

7. IoMT / Edge Security

Edge security is critical for the effective management of the Internet of Medical Things (IoMT), such as Remote Patient Monitoring (RPM) devices. These devices, which operate at the network's edge, collect and transmit sensitive data and must be managed securely to prevent breaches. Implementing edge security ensures that each device is authenticated and authorized before gaining network access, thus safeguarding patient information. Features such as automatic device registration and zero-touch authentication streamline this process, ensuring that only verified devices can connect to the healthcare network. Additionally, configuration management and certificate management capabilities allow healthcare providers to maintain up-to-date security protocols across all devices, even those in remote locations with intermittent connectivity. By treating IoMT devices as first-class identities within a comprehensive identity platform, healthcare organizations can ensure robust security, enhance care, and maintain compliance with stringent regulatory standards.

3. Prevent Fraud Without Impacting Experience

The Problem

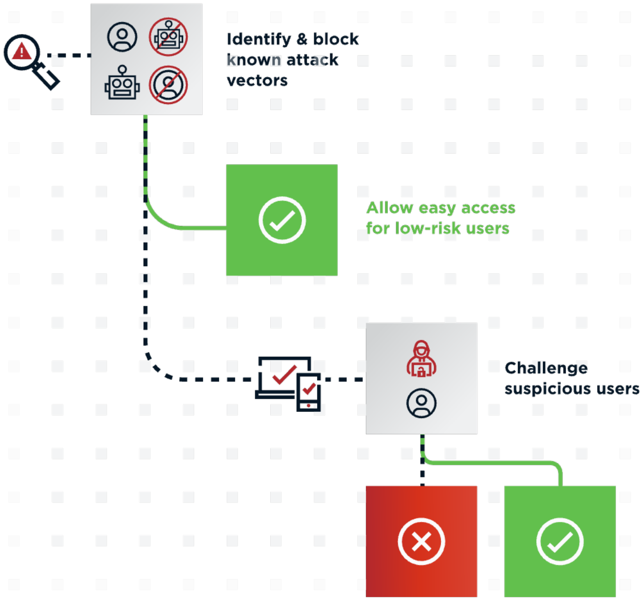
The healthcare sector is under constant threat from fraudsters who use stolen or synthetic identity data to create new accounts or take over existing ones (called Account Takeover or ATO). ATO is when fraudsters use compromised credentials to log into an online app or service posing as a legitimate customer. Once in, they can steal PII, PHI, payment card information, and/or loyalty points in the case of Healthcare Retailers. They can also initiate transactions, use stored payment information, transfer balances to their own accounts, and more.

84% of organizations could reduce fraud risk if they were certain about customers' identity[15]

The result of fraud includes reputational and financial damage, along with a terrible experience for the legitimate user whose credentials were compromised.

Unfortunately, counter-fraud measures often involve adding friction to user sessions, and stringent fraud prevention efforts may be blocked by digital experience teams that worry about the negative impacts of a bad experience.

The Solution


Identify & block known attack vectors
Allow easy access for low-risk users
Challenge suspicious users

Ping Identity helps you combat account takeover, unauthorized access, and new account fraud by integrating fraud prevention directly into the user journey. Incorporate friction when and where it is needed by building adaptive user journeys that evaluate and act on risk signals without frustrating legitimate users with excessive security steps.

With Ping Identity, you can:

- Detect and prevent account takeovers and new account fraud
- Stop fraudsters early, before they can do damage
- Reduce unnecessary friction for legitimate customers
- Gain visibility into risk and fraud posture and trends
- Get the most out of your existing fraud tools

[15] https://www.experian.com/innovation/thought-leadership/experian-2023-identity-and-fraud-report.jsp

Important Fraud Prevention Capabilities to Consider

1. Identity Verification

Identity verification is the process of confirming that a person is who they say they are at the point of registration and/or during authentication. The goal is to prevent fraud and ensure that only the right people can register a new account and access certain services or information.

To eliminate user abandonment, this process should be quick and easy. Identity verification can be streamlined by using a combination of Mobile Match (MM) and Dynamic Knowledge Based Authentication (KBA) to achieve up to a 95% verification rate. Document verification, the process of validating the authenticity of a user's identity document, such as a passport or driver's license, and Voice biometrics can be added for additional assurance. Read our blog to learn more.

2. Behavioral Biometrics

As cyber threats in the healthcare industry become more sophisticated, traditional security measures like PINs are becoming less effective. Behavioral biometrics, which analyze interactive human gestures such as how we hold our devices, scroll patterns, and keystroke dynamics, are emerging as a powerful tool to differentiate between legitimate and fraudulent users. These micro-gestures are unique to each individual and difficult to replicate, making them an effective way to flag suspicious activity. When a healthcare professional's behavior deviates from their established pattern or resembles that of a bot, digital tools can detect this and prompt further verification, enhancing security and protecting sensitive patient data.

3. Bot Detection & Management

Many bots are designed to cause harm, but not all bots are bad. In the healthcare industry, for example, good bots are used to automate administrative tasks, manage patient engagement, and analyze medical data. Bot detection and management tools aim to distinguish between good and bad bots, determining which ones can access healthcare systems. This capability is critical: As important as it is to block malicious bots that engage in activities like data breaches or system disruptions, it is also important to allow beneficial bots that enhance operational efficiency and patient care. Bot detection and management tools use machine learning and threat intelligence to differentiate between human users, good bots, and bad bots, effectively preventing fraudulent activities such as data theft and unauthorized access to patient information.

4. Device ID

Device identification in the healthcare industry focuses on devices rather than users. Information such as a device's type, IP address, local time zone, and browser language forms a "fingerprint" that helps detect fraud. For example, if one specific device is linked to multiple accounts attempting to access patient records, device ID tools can flag this as potential fraudulent activity. Advantages of using device ID tools in healthcare include not requiring personal user data and the ability to block returning fraudsters based on the device they previously used. This enhances security by preventing unauthorized access to sensitive patient information and ensuring compliance with regulatory standards.

5. Authorization Tools

In the healthcare industry, after authenticating users, organizations grant different levels of access to their systems using authorization tools. These tools use settings and parameters set by security teams and access tokens to permit or deny user actions. While some tools focus solely on authorization, others integrate both authentication and authorization features. By implementing these tools, healthcare providers can manage access and permissions for both external users and internal staff. Advanced authorization tools, known as attribute-based access control (ABAC) or externalized authorization management (EAM), surpass traditional methods by enabling the evaluation of any data set and enforcing policy-based decisions on permitted actions, thus enhancing security and compliance in healthcare operations.

4. Uplevel Identity Governance and Administration (IGA)

The Problem

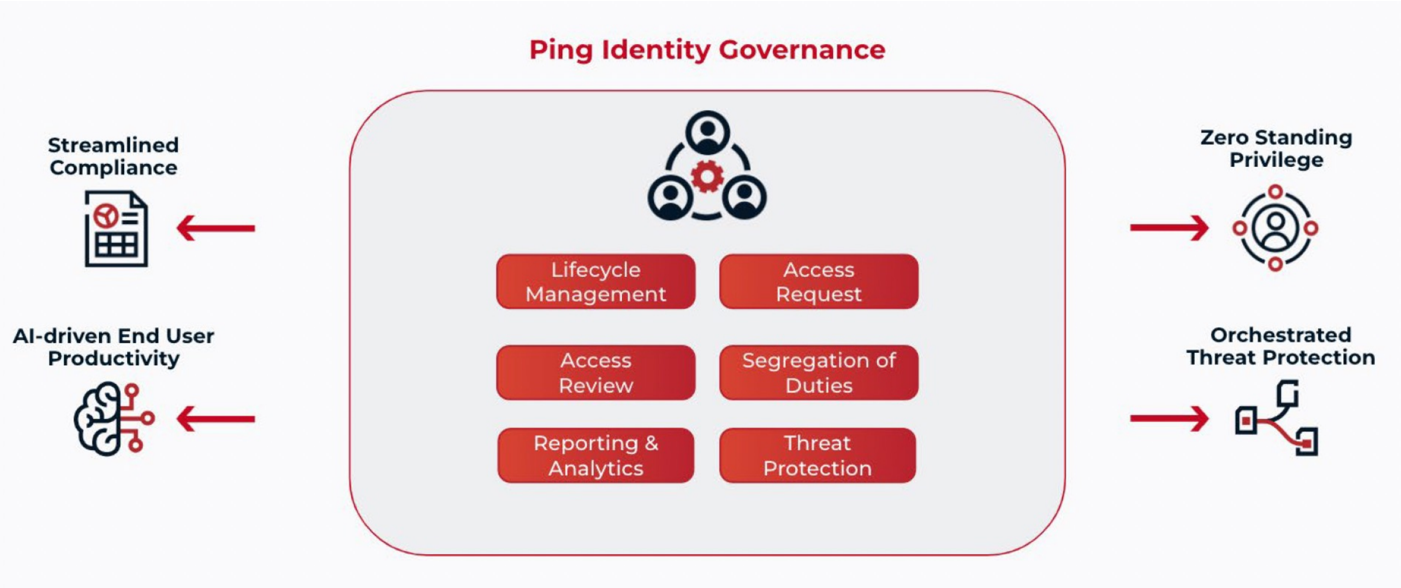
According to Morningstar, 55% of healthcare organizations allow employees to access more data than necessary for their job roles.[16] Furthermore, a significant number of attacks against large healthcare organizations come from social engineering and other internal threat vectors. Bad actors seek to exploit vulnerabilities in the workforce, contractor, and partner access policies.

The Solution

Ping Identity's IGA solution helps healthcare organizations mitigate common insider threats across the workforce, contractor, and partner identity lifecycle and enforce least-privilege access as part of an overall zero-trust security strategy. These capabilities also enable organizations to comply with HIPAA mandates to protect the confidentiality, integrity, and availability of protected health information (PHI) with identity governance that controls who has access to PHI and under what conditions.

With Ping Identity, you can:

- Reduce access vulnerabilities with strengthened security across all workforce, contractor, and partner access requests by eliminating error prone manual processes.
- Automate role engineering and governance along with self-service access requests to reduce workforce access costs.
- Achieve a complete understanding of all your identity provisioning, administration, compliance, and employee access management landscapes and needs organization-wide.
- Spot anomalous behavior before it represents a threat and enable solutions to proactively identify access risks and highlight excessive privileges.
- Leverage workforce identities to solidify enterprise-wide security at the perimeter.



[16] https://www.morningstar.com/news/business-wire/20240521811121/more-than-one-in-four-ransomware-attacks-on-healthcare-providers-impact-patient-care

Important IGA Capabilities to Consider

1. Legacy Application Support

In the healthcare industry, many organizations rely on legacy systems and applications that store critical user data and credentials. An Identity Governance and Administration (IGA) platform must manage the user lifecycle and ensure governance for these applications to maintain compliance and security. This is achieved through support for both legacy application connectors and standards-based connectors. Supporting legacy applications allows healthcare organizations to extend their existing investments, thereby increasing ROI and reducing costs without the need for extensive system overhauls. This ensures that critical data remains secure and compliant with regulatory standards.

2. Segregation of Duties

In the healthcare industry, segregation of duties, combined with the ability to schedule policy evaluations, allows organizations to proactively scan all identity data to detect rogue accounts or inappropriate user access. Automating policy enforcement reduces security access risks and ensures regulatory compliance across the entire organization. This proactive approach helps healthcare providers maintain the integrity and security of sensitive data while adhering to strict regulatory standards.

3. Role Mining

Role mining is a critical process within Identity Governance that automatically analyzes user permissions and activities to identify common patterns. By uncovering these patterns, role mining helps healthcare organizations create more efficient and secure access control structures. This proactive approach enhances compliance, streamlines user access, and mitigates security risks by aligning permissions with specific job roles and responsibilities, ensuring that healthcare professionals have the appropriate access to sensitive data and resources while maintaining robust security and regulatory compliance.

4. Security-Minded Architecture

To effectively address the security requirements of large healthcare organizations, an identity governance solution must offer more than just encryption and industry certifications. It should provide architectural and platform-level differentiating features, such as tenant isolation and data sovereignty, to mitigate common cloud platform issues like nosy and noisy neighbors. These features ensure that sensitive data remains secure and compliant with healthcare regulations, while maintaining robust privacy and operational integrity across the organization.

5. Identity Analytics with AI/ML

Identity analytics capabilities provide valuable insights into user behavior and access patterns, crucial for managing the vast amount of identity and access data generated by large healthcare organizations. Traditional analysis methods are inadequate for handling this volume of data, making specialized AI and machine learning (ML) engines essential. These advanced systems are fine-tuned for rapid pattern recognition and can assign confidence scores while providing detailed explanations for flagging certain access or users as outliers, ensuring precise and informed decision-making.

AI and ML elevate Identity Governance by swiftly identifying outliers within extensive data sets. These technologies generate confidence scores to assist managers and approvers in conducting access reviews and approvals efficiently. Modern IAM platforms that integrate AI and ML for identity and IGA significantly enhance efficiency, allowing IT staff and access approvers to focus on access rights identified as risky or anomalous. This leads to improved security and a reduced administrative burden, ultimately fostering a safer and more compliant healthcare environment.

5. Be An Early Adopter Of Decentralized Identity

The Problem

Identity fraud in healthcare is widespread, causing substantial financial losses and escalating the costs of identity verification. Current efforts to mitigate risk, coupled with regulatory requirements, hinder business agility. Healthcare consumers, employees, and partners are burdened with lengthy ID checks, repetitive data entry, and challenges related to securely sharing verified identity information, which often involves manual processes and complex integrations. In addition, fragmented data spread across numerous systems poses challenges to secure data sharing and consumer control over personal information. And centralized data repositories are vulnerable to breaches, putting sensitive health information at risk.

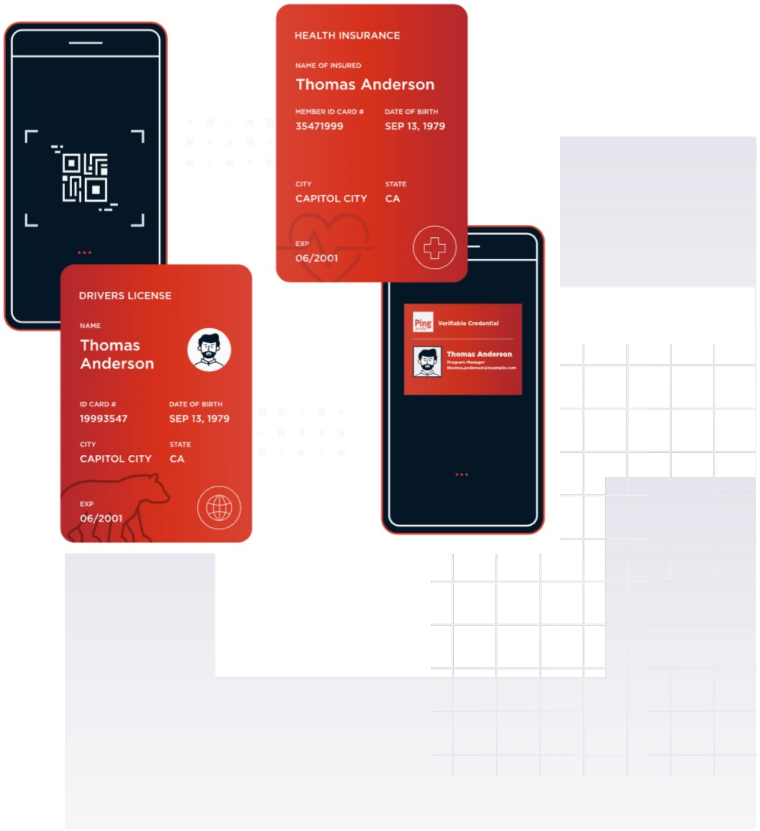
The Solution

The fundamental building blocks of decentralized identity (DCI) include identity verification, reusable digital credentials, and digital wallet technology. Healthcare organizations can leverage decentralized identity and verifiable credentials to address a wide array of consumer, workforce, and partner use cases.

DCI provides individuals with control over their own digital identities without relying on a central authority. This approach uses decentralized identifiers (DIDs) and verifiable credentials, allowing users to create, manage, and share their identity information directly with a service provider. Through cryptographic keys, individuals can verify their credentials and prove their identity to others without needing a third party to authenticate the information. This enhances privacy, security, and user autonomy, reducing the risk of data breaches and unauthorized access to personal information.

With Ping Identity, you can:

- Reduce the possibility of transaction fraud and identity fraud by instantly verifying identity, authenticity, and accuracy of issuance and data integrity at the time of presentation.
- Allow users to share only necessary identity attributes for a specific transaction, such as confirmation of age instead of date of birth.
- Gather, store, and protect only the user data you need, eliminating sensitive information that malicious actors are after.
- Facilitate interoperability with third parties by providing a common standard for identity management using verifiable credentials.
- Use DCI to adhere to regulations like, HIPAA, TEFCA, and the 21st Century Cures Act



[15] https://www.experian.com/innovation/thought-leadership/experian-2023-identity-and-fraud-report.jsp

Important DCI Capabilities to Consider

1. Identity Verification

Identity verification confirms that a user's online identity matches their actual identity, using documents like a driver's license or passport. This process assures healthcare organizations that the individuals interacting with their business are who they say they are, not imposters or automated bots.

Identity verification is commonly used in initial interactions with new users, like during account creation or application submission, or before providing the user with secure, reusable digital credentials.

2. Verifiable Credentials

A verifiable credential (VC) is a digital version of a physical credential, like a driver's license or diploma, that can be securely stored and presented electronically. It's tamper-proof and can be verified instantly due to its cryptographic signatures. VCs allow individuals to prove their identity, qualifications, or other attributes without revealing unnecessary personal information, enhancing privacy and control over their data. For healthcare organizations, partnering with an IAM provider that offers verifiable credentials is essential for maintaining the integrity and trustworthiness of digital identities. This ensures that employees, providers, partners, and consumers can present and authenticate their credentials efficiently and securely. Utilizing verifiable credentials reduces the risk of fraud, streamlines administrative processes, and enhances compliance with regulatory requirements.

3. Capture Consent

Capture Consent is the process of obtaining and documenting a user's explicit agreement or permission for a specific action or purpose. In this framework, explicit consent by the credential owner is required to share a verifiable credential, ensuring that the individual maintains control over their personal information. Additionally, verifiable credentials provide selective consent, allowing the owner to share only specific identity attributes they permit. This process enhances privacy and security, giving users greater autonomy over their identity data while ensuring compliance with regulatory requirements and fostering trust in digital interactions.

4. Centralized Lifecycle Management

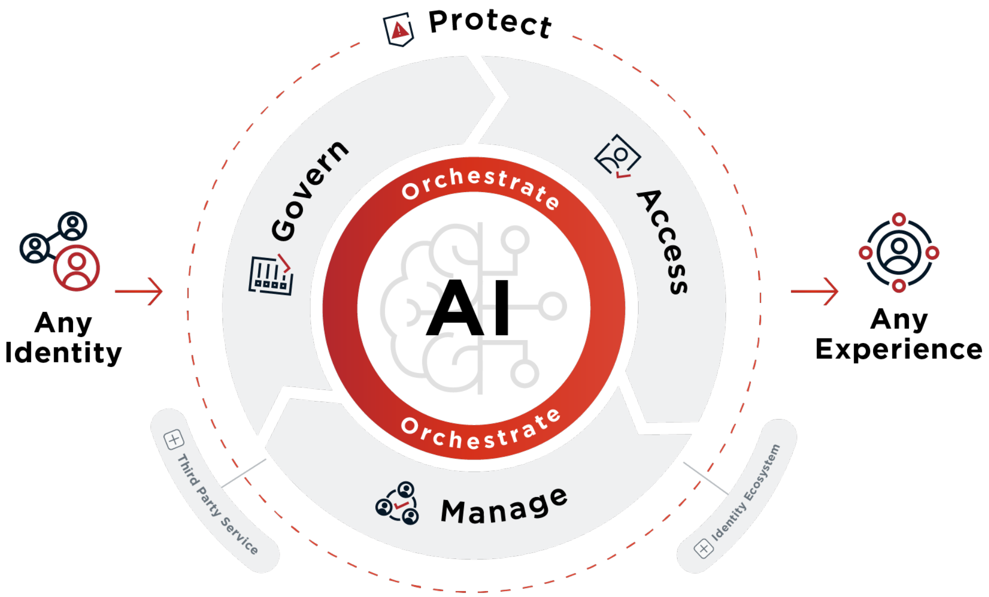
Manage the entire life cycle of credentials, from definition to revocation, from a single management console.

Just like a physical credential, verifiable digital credentials may also have an expiration date or be revoked. Decentralized identity revocation occurs in real-time. That way, Verifiers always know whether the issuer has decided the data has expired, or whether the user has removed consent to use the data.

5. Automated ID Inspection

Automated ID Inspection refers to the process of automatically verifying the authenticity of identification documents using advanced technologies. Ping Identity's solution excels in this area by being able to authenticate over 3,000 types of IDs from around 200 countries. This solution links verified identities to a device, an application, and a physical presence, ensuring a robust and secure identity verification process. Automated ID Inspection enhances trust and security by reducing the risk of fraud and streamlining the verification process, making it particularly valuable for healthcare organizations that need to securely manage patient, provider, and employee identities.

Start Revolutionizing Your Healthcare Cybersecurity With Ping Identity



It's time to secure your healthcare business both behind and beyond the firewall. Contact us for more information on how to get started on a more secure future with Ping Identity.

# 4062 August 2024 Version 1