KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

EBOOK

Your Playbook for Driving Digital Security in Healthcare

Author: Mark Thompson | VP, Product Management | Keyfactor

Table of Contents

An Evolving Landscape

Both the definition and delivery of healthcare is evolving at an exponential rate. A swift convergence of medical advances, emerging technologies, consumer choices and expectations is accelerating change. No longer confined by the walls and location of a hospital or doctor's office, traditional borders and guardrails are dissolving – and doctors, nurses, medical technicians and others are caring for patients face-to-face and from afar. This expanding & virtual healthcare drives better outcomes – from fewer office visits, to device monitoring, to 24/7 access to patient data in real-time.

Achieving secure digital interoperability within this multifaceted environment is challenging. But spending time focusing on the right things and incorporating best practices is a good place to start.

Healthcare as a Prime Target

As breaches continue to occur with greater frequency, consumer patience for an organization's inaction will take a toll. According to a recent study published in the Journal of the American Medical Association, healthcare data breaches jumped 70% between 2010 and 2017.

The healthcare industry is a prime target for hackers for a variety of reasons; there's a treasure trove of information captured and stored, and the prize money from insurance fraud and black market pharmaceutical sales can be extremely lucrative.

According to a recent study published in the Journal of the American Medical Association, healthcare data breaches jumped 70% between 2010 and 2017.

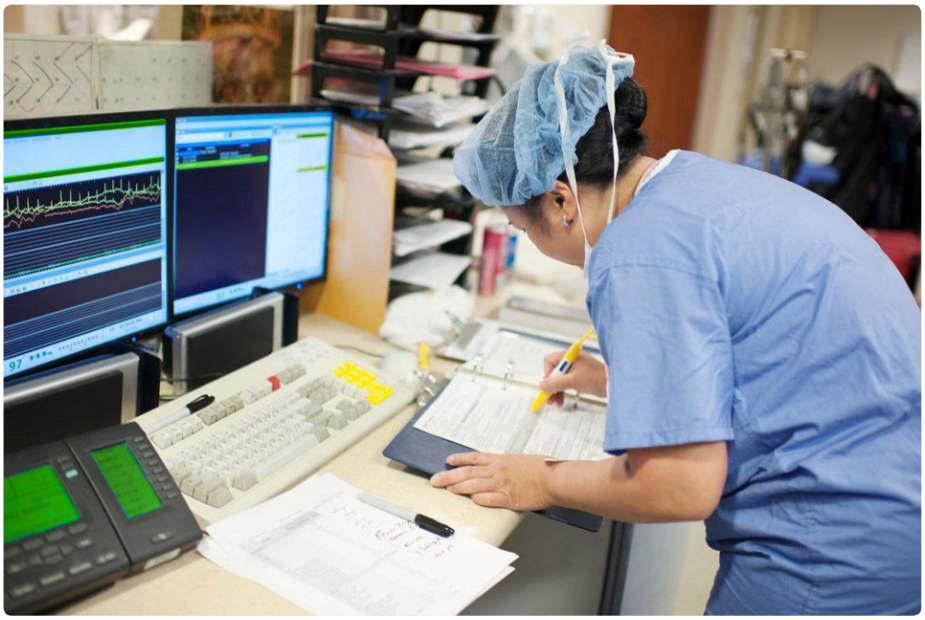


Photo Credit: REZA ESTAKHRIAN.

The Promise of Secure Healthcare

The industry as a whole is starting to take heed. At the heart of healthcare is every patient – trusting in authorities like surgeons and specialists – and the facilities they come to for care. You've undoubtedly made investments in digital security, aimed to build that trust. But is it enough? In order to cover every patient touchpoint you must secure all digital identities across your organization. This is the only way to ensure that any data, any device, every person, is completely secure.

This isn't an easy undertaking. Healthcare delivery organizations (HDOs) are dependent upon a variety of technologies & suppliers to optimize patient care. Electronic health record (EHR) technology is a great example – as patients willingly share personally identifiable information (PII) with staff, you must provide assurance that reliable controls are in place throughout the life of the software, protecting the data for as long as you have it.

An equally important player in the healthcare ecosystem is IoT. Medical devices are at the forefront of the healthcare evolution – from accelerating the discharging of patients, to providing remote monitoring and medicine delivery, and even self-serve care for extended periods of time. To work effectively & securely with equipment, HDOs must put an identity on every device that aligns with the original identity from the manufacturer.

Whether guarding personal information, constant data exchanges, or active medical devices, securing every digital identity across your organization is where patient trust transpires. Patients are presuming you're taking precautions. They're counting on you to provide safety and security throughout their healthcare experience.

SECURING PATIENT TRUST

At the heart of healthcare is every patient – trusting in authorities like surgeons and specialists – and the facilities they come to for care. In order to cover every patient touchpoint you must secure all digital identities across your organization. This is the only way to ensure that any data, any device, every person, is completely secure.

–

MARK THOMPSON
VP, PRODUCT MANAGEMENT, KEYFACTOR

KEYFACTOR

Protecting Every Patient at Every Touchpoint

Getting Started

No matter where you are in your digital security practice, it's always a good idea to evaluate what's working and what's not. Auditing your current asset inventory and number of certificates is a good place to start. Once you're aware of what you've got, you can spend time developing a long-term strategy to drive optimization.

YOUR GOALS SHOULD INCLUDE:

- Deploying high assurance security that's automated and future-proof.
- Strengthening the ability to effectively authenticate providers, patients and applications at scale.
- Covering everything within your organization without breaking your budget.

Automation Drives Assurance

AUTOMATION

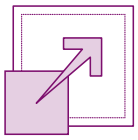
In an ideal scenario, you'd have the luxury of employing a sizable IT department whose only charge would be to monitor and manage this entire process. Even then, manual efforts are prone to blind spots. Whether you've got a team of 1 or 100, automating digital security management helps expedite deployment, standardize processes, and alleviate missteps.

The burdens of manual and decentralized certificate administration are many. Starting with successful management of what could be hundreds of thousands – even millions of digital identities across your organization. Your team is stressed and stretched – and likely unaware of what certs are where and pending expiration dates.

Automation supports visibility of activity to all levels of the organization. Teams on the ground will be able to see and respond proactively to threats and upcoming certificate expirations. High-level reporting provides insights your senior management is looking for to understand what challenges are being faced, and where investments need to be made.

Automation provides the certainty you and your team need to know that you've got complete control over your digital certificate management. It's the kind of innovation that drives efficiencies and allows for growth in the near and long-term.

Scalability for Today and Tomorrow



SCALABILITY

Any organization looking to grow will continue to evolve. As more devices come onto your network and more apps are rolled out, the need for you to enforce encryption, authenticate and manage overall security is going to continue to expand.

Customized applications can be costly and slow down progress. Consider open platforms with vetted workflow scenarios that align to yours, and can easily adapt as your certificate numbers flex.

Many HDOs are bound by budget and believe they have to make hard decisions on which devices to cover. Investing in coverage that doesn't use a per-cert fee model can help squash cost concerns, and eliminate the practice of having to choose which identities are covered.

Time and Money Well Spent

TIME & MONEY

No doubt you're being asked to save time, increase productivity, and reduce costs while driving innovation. Through automation your team will have the ability to quickly identify threats across devices, applications and people. Faster recognition means faster response.

The cost of a security compromise doesn't reside in your IT budget alone. By taking preventative measures today you'll mitigate real business risks and costs down the road that come with a breach – patients who may go elsewhere, lost revenue, staff turnover, and overall crisis management.

You'll also be able to redeploy already stretched resources to focus on other important business initiatives that are in need of IT attention.

Managing the Entire Certificate Lifecycle

CERTIFICATE LIFECYCLE MANAGEMENT

Getting digital security right means investing in the time and technology needed for complete and comprehensive coverage – from issuance to revocation and ongoing management of every certificate – at scale, at every moment.

End-to-end visibility and control will give you the freedom to know you've got everything covered, allowing you to focus on other important areas the business is expecting you to drive.

Getting started is easier than you think.

With Keyfactor, managing the entire certificate lifecycle is easier than you think. End-to-end visibility and control will give you the freedom to know you've got everything covered.

Elevating Your Digital Security Management

OVERVIEW

Finding Freedom with Keyfactor

For over fifteen years, Keyfactor has been empowering healthcare organizations with the tools, technology and support they need to master every digital identity. **Keyfactor™ Command** simplifies the identification, cataloging, monitoring, issuance and revocation of digital certificates across multiple platforms. Our platform is used by hospitals, pharmaceutical companies, device manufacturers and government agencies. Keyfactor technology and workflows are uniquely designed and implemented to address the specific certificate environment and requirements of your organization.

Keyfactor Case Study

SYNOPSIS

A growing Fortune 1000 healthcare company had several challenges in managing their large, disparate environment with hundreds of thousands of certificates. They chose Keyfactor to help elevate their digital security through discovery and ongoing management of every certificate across their organization.

Keyfactor has been empowering healthcare orgnizations with the tools, technology and support they need to master every digital identity.

CUSTOMER CHALLENGES	HOW KEYFACTOR HELPED
Scheduling and executing SSL scanning of multiple environments at-scale	Simplified and accelerated SSL scanning across the organization with enhanced discovery and inventory management plus immediate monitoring of certificates at discovery
Reporting certificate locations, key strength and expiration dates	Provided easily accessible, customized reports for every stakeholder across the organization
Integration with workflows for issuance around DevOps processes	API integration allowed individual application owners to easily integrate with the Keyfactor platform for certificate issuance

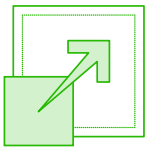
Finding Freedom with Keyfactor

CONCLUSION

Our proven technology is used by hospitals, pharmaceutical companies, device manufacturers and government agencies, but is uniquely designed and implemented to address the specific certificate environment and requirements of your organization.

Visibility

A complete view of your certificate inventory including location and expiration status.



Scalability

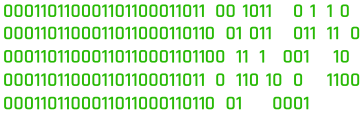
Expand and easily manage identities anywhere in the world – from one device to 500M.

Automation

Management of every certificate across the globe including publicly-trusted and other issuing authorities.

Optimize Costs

- No per-certificate fees
- No installation charges
- Increase resource productivity



Accelerate Transformation

- Aligns to Cloud-First initiatives
- Extensible by API to other business systems

KEYFACTOR

ABOUT KEYFACTOR

Keyfactor™, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its lifecycle, Keyfactor empowers global enterprises with the freedom to master every digital identity. Our clients are the most innovative brands in the industries where trust and reliability matter most.

CONTACT US

- Visit: www.keyfactor.com
- Client Assistance: success@keyfactor.com
- 216.785.2990