Revolutionizing Remote Secure Access: SecureAuth IdP

State of Security: Remote Access in Healthcare

We live an era of sophisticated threats and relentless cyber attacks. Criminal rings are well-funded, well-organized and technically advanced, while emerging trends such as the Internet of Things, Big Data, BYOD and cloud mobility have left IT teams struggling to create security strategies equal to their technical capabilities. For healthcare organizations, the quest for protection is especially critical. From keeping data safe and accessible to empowering patient care, healthcare IT security can be literally a matter of life or death.

It's a challenge that grows ever more intense, given the rise in the black market value of electronic protected health information (ePHI) as credit card data drops in worth. In under two years, the industry has seen the Community Health Systems breach, with 4.5 million individuals impacted; the attack on Premera Blue Cross, impacting 11 million; and finally the attack on Anthem, which affected an estimated 80 million individuals.[1]

As breaches become more frequent, their cost is rising – with an average $3.5 million USD cost per breach.[2] From HIPAA fines to a damaged brand reputation to the loss of customers and patients, just one breach can be a disaster for a hospital, clinic or private practice.

The Credential Conundrum

The primacy of healthcare cybersecurity is accompanied by challenges unique to the industry. On-the-go doctors demand frictionless secure remote access from any device. Password resets must be available remotely and preferably as a self-service function. The business arm drives technology decisions, leaving IT to create security programs that match those implementations. While they manage these dynamics, teams must also meet compliance standards from HIPAA and other regulatory organizations.

Many healthcare organizations rely on solutions like Citrix, a standard common in hospitals and other facilities. By enabling remote access, this technology improves patient care by delivering critical information at the point of contact in real time. Yet as it's evolved to offer increasing security, attackers have shifted their tactics to the next logical vulnerability: credentials.

To combat this growing risk, teams must reconsider their perimeter protections. With physicians, practitioners and employees relying on remote access to patient records, credentials have become

[1] The Biggest Health Breaches, Healthcare IT News, March 2015

[2] Fourth Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute, March 2014

the new keys to the data kingdom. Names, birthdates, insurance information, Social Security numbers, street addresses, e-mail addresses, employment information and income data are all available in healthcare systems - one reason the healthcare industry accounted for 42 percent of major data breaches reported in 2014.[3]

While managing remote and cloud user access via passwords has always been complex, elements such as password sprawl and shifting architectures have intensified the demand for fresh security strategies. Consider the following challenges:

- Remote access to EHR/EMR applications through VPNs must be secured beyond the vulnerable password.
- Doctors and other users often resist additional security measures in the fast-paced world of medicine and healthcare administration.
- Routine items such as password resets are burdensome if the user must be onsite to complete the task – a requirement that won't work for doctors rotating between facilities.
- Physicians' opinions tend to carry extra weight when it comes to evaluating IT initiatives and programs, making their needs a prime consideration in implementing security solutions.
- When confronted with an inconvenient step, many staff will find another way to get their jobs done, even if it means flouting security and compliance policies.
- Business initiatives drive much of the investment in new healthcare technology – leaving IT to ensure secure access to the applications chosen.
- IT teams want to partner with the business in embracing innovation – yet that innovation must fall within stringent security guidelines to ensure the safeguarding of patient data.

These dynamics leave healthcare leaders searching for a solution that can deliver both secure access and a frictionless user experience. Yet most platform-based or narrowly focused point solutions on the market today simply cannot enable strong authentication alongside ease of use.

The good news: emerging technologies can provide the protected and convenient access that pleases healthcare providers while helping organizations achieve their security and compliance goals.

[3] Data Breach Industry Forecast, Experian, 2015

CALL-OUT:
"Several factors suggest the healthcare industry will continue to be plagued with data breach headlines in 2015." – Data Breach Industry Forecast, Experian[4]

Advanced Security, World-Class Care

To operate effectively in today's healthcare IT climate, access control solutions must achieve a complex combination of flexibility, security, compliance and - above all – an inviting user experience.

Specifically the ideal healthcare IT solution will:

- Deliver frictionless secure user access to any resource from any device, anywhere.
- Provide the user with self-service tools that support a diverse and dispersed user base.
- Enable teams to control the access and authentication for any technology initiative.
- Deliver secure access control that meets and even exceeds HIPAA requirements and other regulations.
- Provide strong and innovative methods to protect access to ePHI.

In short, healthcare organizations must offer the smooth and secure remote access that enables physicians to provide excellent patient care whenever they need to, from wherever they are.

CALL-OUT:

According to the Ponemon Institute, 90 percent of healthcare organizations have had at least one data breach in the past two years. 38 percent report that they have had more than five incidents.[5]

Adapting to a New Era in Security

Traditional two-factor authentication functionality has long been regarded as too cumbersome to offer the necessary balance between security and user experience. Yet by layering two-factor and adaptive authentication as additional layers of security on top of technologies like Citrix, healthcare teams can enjoy both advanced security and a swift and convenient user experience.

Adaptive authentication's benefit is that it takes security to a higher level without adding friction. As part of its risk analysis, it considers contextual factors such as IP address, device fingerprint, geo-location and IP reputation data while leveraging global threat intelligence to block attacks.

---

[4] Data Breach Industry Forecast, Experian, 2015

[5] Fourth Annual Benchmark Study on Patient Privacy and Data Security, Ponemon Institute, March 2014

Teams can customize workflows to enjoy greater visibility into authentication attempts, as well as greater control over authentication. The result: stronger security partnered with a frictionless user experience.

Device fingerprinting is another tool that helps healthcare organizations embrace mobility while protecting their assets. By discerning between devices that match a stored footprint and devices that don't, this tool provides secure access to data from any desktop, laptop, tablet or smartphone. Once a user is successfully authenticated, the solution captures and stores that device's unique characteristics, such as HTTP headers, IP addresses, browser fonts, browser plug-ins, user data storage, and time zone – essentially registering that device. Those characteristics are used to validate the user and device in the future, delivering a low-friction user experience without sacrificing security.

By layering these technologies, healthcare organizations can empower their physicians and providers to deliver the world-class care that is their mission, while protecting their data, patients and staff.

CALL-OUT:

The FBI has warned the healthcare industry that their cyber security systems are lax compared to other sectors in a memo that stated, "The healthcare industry is not as resilient to cyber intrusions compared to financial and retail sectors, therefore the possibilities of increased cyber intrusions are likely."[6]

SecureAuth IdP: The New Face of Secure Remote Access

Now your healthcare IT team can take advantage of an innovative new solution that delivers security, control and a seamless user experience – SecureAuth IdP.

As most healthcare IT professionals know, Citrix offers strong remote access with NetScaler, including the benefit of built-in network security features. SecureAuth adds another layer of protection by delivering strong authentication in advance of those layers. The result? Secure, flexible, adaptive two-factor authentication in addition to single sign-on. Attackers attempting to exploit VPN connections are stopped in their tracks - even those equipped with valid passwords.

SecureAuth IdP's SecurePath enables your team to enjoy control over authentication for all on-premise, cloud, mobile, web and VPN resources in a single solution. Your team can leverage your current legacy infrastructure while using IdP, thanks to an innovative architecture unique in the industry. With authentication challenges matched to risk factors, IdP helps your healthcare providers obtain the data they need to provide excellent patient care, whenever and wherever they are.

---

[6] "The FBI warns healthcare sector vulnerable to cyber attacks," Reuters, April 2014

CALL-OUT:

From Struggle to Security

A nonprofit organization based in Houston, Texas, Houston Methodist Hospital faced a classic healthcare security conundrum: doctors needed remote secure access so they could deliver the best patient care possible – but single-factor authentication wasn't secure enough. When multi-factor solutions were rejected by either staff or other technologies, the hospital turned to SecureAuth. They found it worked with the Citrix-based application, VPN, web reverse proxy, cloud-based SaaS apps and other technologies. Most importantly, physicians loved the frictionless user experience.

"It was really a home run in every category," reported Matt Johnson, Manager of Server Engineering who said that SecureAuth enables the hospital to fulfill its mission of "leading medicine" while maintaining security. "They aren't even prompted for their credentials, let alone questions and answers — in fact, they often don't even realize authentication is happening. .. SecureAuth allows us to be the good guys who provide solutions instead of closing the door on them."

How SecureAuth IdP Works

With some of the industry's most advanced adaptive authentication capabilities, IdP performs dynamic risk analysis using multiple factors. The user's identity is mapped to existing data stores by examining device fingerprints, geo-location and geo-velocity, and later confirmed using any of more than twenty methods. Before authentication begins, IdP analyzes the IP address by comparing it to lists of malicious and compromised websites, as well as live threat intelligence from the industry-leading Norse DarkMatter™ platform.

During IdP's authorization process, the identity presented is inspected and compared to defined group memberships and authorization restrictions in the data store. The solution also analyzes heuristics and geo-velocity, comparing digital fingerprints from browsers or devices to stored profiles; it also compares the last log in time and location to the current login attempt to detect improbable travel events.

IT teams further control this process through features such as time-limited registration, device revocation, waived or required subsequent authentications and other factors. Self-management features allow healthcare providers to register themselves or reset their passwords without assistance from IT, increasing user satisfaction and reducing your help desk costs.

During authentication, IdP takes one of several actions: it permits the authentication to proceed, steps up the authentication and forces the user to fulfill a Two-Factor authentication workflow, redirects the user or denies access all together. The result: single sign-on that streamlines access to all applications with one set of credentials across VPN, LAN, mobile, cloud and web connections.

Discover the SecureAuth IdP Difference

All-in-one security.

SecureAuth IdP provides secure and convenient remote access in a single solution. With adaptive and two-factor authentication alongside single sign-on, IdP helps you meet both your security and compliance goals.

PHI protection.

Thanks to the latest innovations in adaptive authentication, IdP can drop a net around suspicious actors to keep them from moving laterally in your network. Teams can inspect IP addresses, analyze group memberships or check the plausibility of geo location and velocity to easily build risk analysis into authentication workflows.

Speed and Convenience.

With life or death decisions on the line, doctors and other users need fast and convenient access to data like diagnoses, medical histories and test results. IdP offers swift remote access, with authentication workflows that meet users where they are, from their iPads to the cloud to their laptops. Low-friction, transparent features like device fingerprinting keep the focus on patient care, while self-service features like password resets helps users solve their own challenges without calling your help desk.

Friendly Integration.

IdP easily supports over 20 two-factor authentication methods, including SMS, telephony and e-mail OTPs, push notification, OATH tokens, social network IDs, device fingerprints, and of course traditional smartcards and tokens. Instead of overhauling your current security infrastructure, IdP allows you to leverage your tools of today while acquiring what you'll need tomorrow.

Easier Innovation.

Because line of business owners drive more and more technology decisions, it's IT’s job to ensure new solutions can be secured and integrated into existing infrastructure. IdP’s broad range of support for applications in the cloud, on the web, via mobile, on premise and via VPN helps you feel confident about securing any new technology thrown your way. IdP puts control of the authentication process back in your hands, helping you stay agile without sacrificing security.

Rapid deployment.

IdP's GUI-based configurator lets you point and click your way through building workflows, rather than coding. Because IdP is delivered on hardened appliances that are plug and play, as well as isolated from hacks, your risk is reduced and your time to value accelerated.

Compliance made simple.

IdP helps you prove you're delivering strong and secure authentication that satisfies HIPPA standards. Instead of maintaining separate logs for each application, you can unify all access activity through IdP, with your logs shipped to your SIEM tool of choice.

Stopping Tomorrow's Attacks with Secure Remote Access Today

The rising tide of cybercrime has taught healthcare organizations they must all proactively minimize their risk before an attack. By opening a doorway to smooth and secure remote access, SecureAuth IdP offers stronger data protection and a user experience that helps physicians offer exceptional patient care – and helps organizations succeed at their missions today and tomorrow.

CTA:

Stop breaches before they stop you. Request a SecureAuth IdP demo today and find out how SecureAuth can help you solve your access control challenges.