



## Delivering Frictionless Security to the Clinical Workflow: Virtues of Single-solution Approach versus Point Solutions

A Frost & Sullivan White Paper

---

[www.frost.com](http://www.frost.com)

---

Mike Jude, Ph.D.

**Abstract..... 3**

**Introduction ..... 3**

**Virtues of Single-solution Approach vs. Point Solutions ..... 4**

**Last Word ..... 6**

## ABSTRACT

The clinical workflow defines the delivery of healthcare services to patients. As such, managing it efficiently is critical to achieving the Quadruple Aim of healthcare, as espoused by HIMSS: enhancing patient experience, improving population health, reducing costs, and improving the work life of healthcare providers, including clinicians and staff. Yet these objectives are hard to achieve when workflow automation is characterized by an expanding, complex ecosystem of devices, applications, and evolving delivery options. Complicating this is the increasing need for data security to ensure that only those clinicians who have the appropriate privileges will have access to sensitive patient data and IT systems. What is needed is frictionless security—security that is unobtrusive and comprehensive, and that doesn't hinder clinical workflows or the delivery of care to patients. Unfortunately, current security solutions, designed to address the needs of multiple industry verticals, fail to meet the specific needs of healthcare. An IT and security strategy driven by a holistic, integrated identity, governance, authorization, and access management solution purpose-built for healthcare is essential.

## INTRODUCTION

Single sign-on (SSO) is a key requirement for improving workflow efficiency, yet many healthcare delivery organizations still depend on multiple security solutions to prevent unauthorized access to proprietary and patient data. Although a multiple-solution approach can provide good security, it can also have deleterious effects on the delivery of healthcare. Making the physician the front line for security enforcement by requiring multiple sign-ons for each shift or treatment venue distracts the physician from providing the best treatment and can add to overheads that lead to burnout.

The solution is to approach security from a holistic perspective; rather than securing each point of vulnerability, secure the clinical workflow as a continuum. This approach, however, is only possible when the entire security fabric is provided by a single security vendor. Multiple solutions lead to the sort of overheads that can impact workflow efficiency.



A single source for clinical workflow security can improve consistency across security interfaces, enable adoption of more forward-looking technologies, and reduce the possibility and financial impacts of security breaches. However, not just any solution provider will do; what is needed is a purpose-built solution that takes into account the unique requirements of healthcare delivery.

## VIRTUES OF SINGLE-SOLUTION APPROACH VS. POINT SOLUTIONS

Repeated authentication to healthcare systems can introduce inefficiencies into clinical workflows. Yet the cost of such interruptions can pale in comparison to the impact that multiple points of system integration can impose on healthcare system adoption and support. Changing integration ecosystems, increasingly complex regulatory demands, and the eventuality of healthcare systems moving to the cloud dictate that solutions be purpose-built for healthcare. Only by consolidating access under a single solution can many of the complexities of technology adoption be avoided.

Healthcare IT has evolved over time to include myriad point solutions. Rather than introducing new functionality to existing systems, the only way to adopt new capabilities was often to implement a new point solution that addressed the need. Over time, this has led to an ecosystem of applications, rather than one overarching system with multiple functions. Given the complexity of delivering care, this is an understandable outcome. Yet when every point solution requires separate administrative controls and discrete update cadences, point solutions rapidly saturate an organization's ability to absorb new technologies.

The dilemma for IT decision makers is that many point solutions are good. They have been developed to address common needs across industry verticals, often with excellent results. Nevertheless, there are verticals, such as healthcare, where multiple solutions can lead to inefficiencies that degrade the organization's overall security strategy. In particular, in healthcare IT, where multiple solutions carry a concurrent need to secure access to each unique application, a single access system can be the difference between staying current with technology or falling behind the technology curve.

Frost & Sullivan has conducted surveys of IT decision makers and discovered that there is a correlation between the pace of technology adoption and the impact on support organizations. Multiple point solutions, because they may come with different features and different upgrade schedules, tax both support and users by forcing them to learn how to use new features and adapt to new capabilities. The more applications and the more endpoints they impact—thick versus thin (zero application), device type, etc.—the more this impacts an organization.

Once an organization falls behind the technology adoption curve, it is hard to catch up. In the case of access and identity control, falling behind can lead to exploitable vulnerabilities. Yet ignoring the impact of point solution saturation is not an option. Consequently, many healthcare organizations simply shift the burden of point solutions to the personnel least likely to be able to accommodate it: physicians.

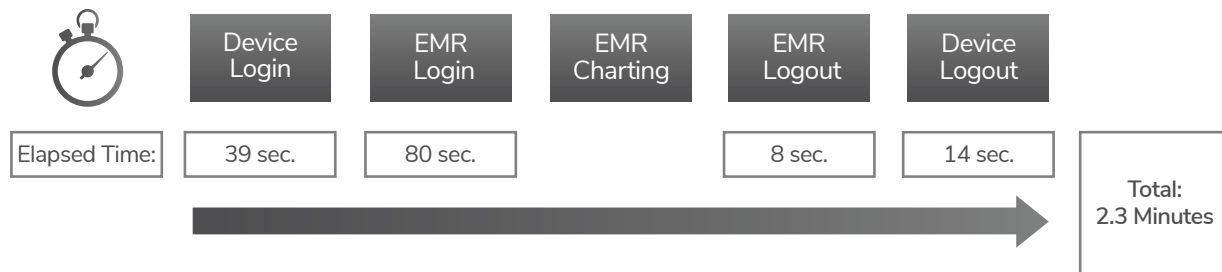
Physician burnout is one of the biggest concerns of healthcare provider organizations. The *Annals of Family Medicine* estimates that almost half of a physician's workday can be consumed by clinical documentation, including the time spent to access the variety of health IT applications needed. Burnout can be accelerated by administration overheads, which distract from primary work functions—not least of which is patient care. Any approach that reduces the overhead on physicians, then, would seem to be a good idea. In the area of

security, one way to reduce overhead is to minimize the number of security solutions, standardizing on a single identity, governance, authorization, and access management platform, rather than using multiple, and disjointed, point solutions.

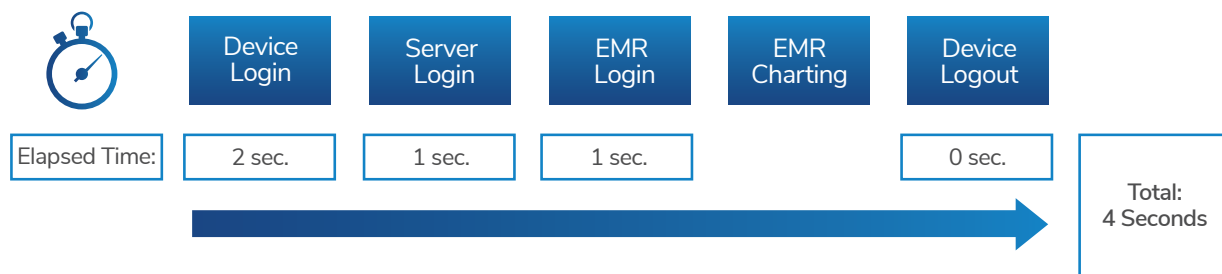
**Figure 2: Impact of Single Sign On Technology**

**Nursing Staff - Faster, Easier Desktop & Application Access with Virtualization and Single Sign-on**

RN's EMR access with HIPAA-compliant workflow:



With Virtualization and Single Sign-on:



Source: Frost & Sullivan, Imprivata

A single-solution approach to identity, access, and authentication management is superior for a number of reasons. A single platform provides:

- **One consistent interface:** A single solution for SSO, authentication and authorization leads to less physician overhead and makes it easier for a physician to maintain technical currency. While clinical systems may change over time, the method for accessing them remains constant.
- **An easier way to port to a cloud environment and integrate with big data:** It goes without saying that many computing functions are beginning to rely on big data lakes, which typically live in a cloud environment. Cloud-compatible access management makes such a migration more efficient since it is not necessary for the user to learn new protocols that are cloud-dependent.
- **An easier audit process:** As privacy becomes more important in healthcare delivery, knowing who had access to patient records and for what purpose becomes critical. Although security systems are not typically the primary means of satisfying patient data access audits, access management systems can make conducting such audits much easier. Further, comparing the access being granted with what is actually being accessed on endpoints allows proactive management of risk areas and data breaches.

- **A lower potential risk of security breach:** This may be the single most important aspect of adopting a single-solution approach. When IT/security teams have to manage multiple integration points, they have less time to focus on higher-priority tasks to protect their network.
- **Reduced costs associated with security breaches:** The cost of a breach can be considerable. Health IT Security News estimated that the average cost of a healthcare data breach in 2017 exceeded \$3.62 million per instance. Even one breach, caused by multiple points of vulnerability, can dramatically impact the organization's financials.

A single solution optimizes IT resources, reduces overhead, and enables a more efficient customer care workflow. Although healthcare organizations are generally deeply invested in multiple applications, one way to begin to turn this around is to start with the user interface. By incrementally masking the underlying complexity from the attention of clinicians, utilizing health IT applications can, ultimately, be simplified and made more efficient.

## LAST WORD

Single sourcing has been an approach used effectively in manufacturing since the days of Total Quality Management (TQM). The concept of optimizing supply lines by partnering with a vendor rather than using multiple vendors has led to innovations such as just-in-time manufacturing and has delivered radical reductions in manufacturing cost and substantial improvements in the quality of goods and services. Yet this approach is rarely considered in healthcare. Why is that?

Healthcare is fundamentally more complex than manufacturing, and the impact of failure can be catastrophic. This has led to a focus on function rather than efficiency for most technology applied to the clinical workflow. Yet there is a place where a single source makes sense and is, in fact, the best option for both positive outcomes and workflow efficiency: security.

A single source for access management ensures that the benefits of a holistic approach to security can be achieved. However, not just any solution will suffice. While there are many security solutions available, most have been developed to address the general security needs of every market vertical, rather than focusing on the special needs of the healthcare market. A vendor that can deliver a purpose-built healthcare security solution is critical to achieving the benefits of frictionless security for the clinical workflow.

---

**A vendor that can deliver a purpose-built healthcare security solution is critical to achieving the benefits of frictionless security for the clinical workflow.**

Healthcare professionals, faced with securing an increasingly complex workflow automation environment, can't wait. The security landscape will only become more diverse and complex over time. It is important to select a vendor that can deliver a single identity and access governance solution that is capable of scaling as organizational needs change. Decision makers should consider Imprivata, a healthcare technology provider that is building such governance solutions today.



Silicon Valley  
3211 Scott Blvd  
Santa Clara, CA 95054  
Tel +1 650.475.4500  
Fax +1 650.475.1571

San Antonio  
7550 West Interstate 10, Suite 400,  
San Antonio, Texas 78229-5616  
Tel +1 210.348.1000  
Fax +1 210.348.1003

London  
Floor 3 - Building 5,  
Chiswick Business Park  
566 Chiswick High Road,  
London W4 5YF  
Tel +44 (0)20 8996 8500  
Fax +44 (0)20 8994 1389

877.GoFrost • [myfrost@frost.com](mailto:myfrost@frost.com)  
<http://www.frost.com>

## NEXT STEPS

-  [Schedule a meeting with our global team](#) to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
-  Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
-  Visit our [Transformational Health](#) web page.
-  Attend one of our [Growth Innovation & Leadership \(GIL\)](#) events to unearth hidden growth opportunities.

---

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:  
Frost & Sullivan  
3211 Scott Blvd  
Santa Clara CA, 95054