HealthManagement
Promoting Management and Leadership

Managing access to a Windows network for healthcare organisations

François Amigorena
******@***isdecisions.com

CEO - IS Decisions

The importance of getting access management right cannot be overstated. You need to make sure that anybody accessing your systems – and the data within – is exactly who they say they are.

This is especially important when dealing with **healthcare professionals** who have access to vast amounts of sensitive medical data. Most compliance standards require that individuals handling patient data have access to the degree that is necessary for them to perform their role – no more, no less. But according to our study, 37% of healthcare workers don't even have unique logins. Quite aside from the issue of user identification to determine what data an individual requires access to, to perform their role, this obviously leaves access wide open to attackers

Many organizations fall down in the same areas where access management is concerned. So to help healthcare organizations better protect their Windows network, here is a list of **four of the most common mistakes** when it comes to managing access.

1. Time consuming and disruptive

When we first think about it, we wouldn't consider this a big mistake. But then, we've done some research. In fact, one of the biggest barriers to adopting a technology is the amount of time it takes IT to actually manage the software. We surveyed 250 American companies , 18% of them believe that 'time to manage and oversee' is the biggest barrier to adoption.

Spending too much time managing the software means that it will have some serious repercussions on productivity. This leads to the fact that the total cost of ownership for the tool is often much higher than you would initially think. The best advice would be to try the product first, if you can, to make sure that it's the right choice for you.

Security solutions with 'stickiness' tend to be simple to implement and intuitive to manage.

2. Overwhelming productivity

If the productivity is overwhelmed and restrained by the security, users aren't able do their job properly and the solution is already dead on arrival. However, organizations are aware of the problem — 47% believe that complex IT security measures in place within their organization negatively impacts employee productivity.

Security should work behind the scenes, protecting the users and the environment until the moment the user is truly conflicting with security protocol.

3. Monitoring everything on your network

As said before, you need to make sure that anybody accessing your system is exactly who they say they are. It's not effective to try and monitor

every last bit of your network looking for anything that looks unusual, especially when your time is limited.

This approach would end up being pretty costly and requiring significant IT time and resources to put proper detection mechanisms in place. This mode of operation will likely raise an initial set of false positives that need to be fine-tuned, and necessitates reports and meetings to ensure the detection is actually working.

A better approach would be to run and monitor solutions that offer automated controls in addition to threat identification and real time response.

In short, should something fall outside a set of established restrictions, your solution should automatically take action before the damage is done – not only when IT intervenes.

4. Blaming your employees

While users are often the weakest link in any network security, they can also be the solution if you stop blaming them and start empowering them in the right way. Healthcare professionals are (usually) human. They are careless, flawed and often exploited. That's what makes them so attractive to attackers, they're naïve so it's easy.

One successful phishing email is enough to persuade one user to hand over his organizations login details. The use of compromised internal credentials by an external attacker is the most common threat action in data breaches (Verizon, Data Breach Investigations Report 2018).

Education is key. In fact, only 48% of healthcare organizations provide ongoing security training.

Once an education program has been put in place, you need to then make sure that your access management software has the ability to warn users themselves of unusual connection events involving their credentials.

Who better than the user to judge whether the activity is suspicious or not.

Protecting sensitive patient data

Many healthcare organizations in today's cybersecurity world are making these four mistakes. To solve this problem, we suggest to look for access management solutions that include context-aware security.

To explain briefly, when someone attempts to connect, this approach uses and benefits from supplemental information to decide whether this access is genuine or not (compromised). After that, the system can automatically grant or deny access using admin-set rules that are based on this supplemental information.

Restricting access like this monitors the right aspects of security, doesn't take much time to manage, doesn't impede users' productivity, empowers those employees to make the right security choices and doesn't force you to choose between security and productivity. It's a win-win scenario for you and your healthcare employees.

Learn more about how contextual access security with UserLock helps healthcare organizations secure user sessions and stop unauthorized access that could lead to fraud, data breaches and non-compliance issues.

About the Author

François Amigorena is the founder and CEO of IS Decisions, and an expert commentator on cybersecurity issues.

IS Decisions is a provider of infrastructure and security management software solutions for Microsoft Windows and Active Directory. The company offers solutions for user-access control, file auditing, server and desktop reporting, and remote installations.

It's customers include the FBI, the US Air Force, the United Nations and Barclays — each of which rely on IS Decisions to prevent security breaches; ensure compliance with major regulations; such as SOX and FISMA; quickly respond to IT emergencies; and save time and money for the IT department.

Published on : Fri, 8 Mar 2019