Healthcare IT Solutions

BENEFITS OF CLOUD-BASED SECURITY IN HEALTHCARE IT

Cloud-based managed services reduce and mitigate risks for hospital IT

BENEFITS OF CLOUD-BASED SECURITY IN HEALTHCARE IT

Cloud-based managed services reduce and mitigate risks for hospital IT

INTRODUCTION

Healthcare organizations are facing a difficult challenge: They must collect, store and share electronic health records, but they must do so in ways that protect that data from falling into the wrong hands. In the modern landscape, healthcare data is more valuable than ever before. For clinicians, instant access to patient data can improve the quality of care. For the hospital, better patient care equals happier and more loyal consumers. Aggregated healthcare data, or big data, is foundational in evolving preventative and prescriptive medicine. Unfortunately, the data that is so valuable to hospitals is equally valuable to criminals.

In recent years, the black market, organized crime and technology-based crimes originating in nation states have grown to a multibillion-dollar industry. On-site IT infrastructure and tape-based storage is no longer adequate to protect hospitals from cybercrime.

Since 2003, the Health Insurance Portability and Accountability Act (HIPAA) has brought security and privacy enforcement to Covered Entities. Stringent regulations mean massive fines for data breaches, and the consumerization of healthcare services means patients/consumers are taking an active role in choosing where they are treated. Combined with a booming black market for healthcare data, these factors and others have hospital IT departments in volatile and unfamiliar territory.

EVOLVING THREATS TO HEALTHCARE IT

In the past few years, cybercrime has evolved from hackers showing off their technical skills to botnet attacks, exfiltration or stealing medical information or credit card data, and malware such as ransomware. Hospitals are particularly vulnerable to cyberattacks because, by design, most hospitals are one large network of systems where devices can communicate freely and computer systems can talk to each other. But the very same network architecture that allows for enhanced efficiency and productivity also allows the propagation of malware. Once malware finds its way into a system that is possibly full of security holes, it can access all of the systems holding information in the entire organization.

Ransomware is an insidious incarnation of cybercrime, and incidents are increasing rapidly. Ransomware is a form of malware that infiltrates an organization and encrypts much of the hospital's data once it's in the network. Perpetrators then demand that hospitals pay for the encryption key. If hospitals don't pay, or don't pay fast enough, they stand to lose all of their data—volumes now measured in terabytes. Ransomware

is becoming so sophisticated that some versions are "file-less," allowing them to evade many antivirus applications. File-less ransomware is often difficult to nearly impossible to detect until the damage has been done. Malware and ransomware are so lucrative that attacks escalated by over 300% in 2016.[1]

This trend means that for hospitals, malicious attacks are no longer a question of if but when. Cyberattacks can shut down entire hospitals, including expensive diagnostic equipment that earns its keep by operating 24 hours a day. Cyberattacks can also affect patient care and the hospital's brand and reputation, and lead to regulatory penalties.

MITIGATING RISKS AND IMPROVING HEALTHCARE IT SECURITY WITH MANAGED CLOUD SERVICES

Given these and other risks, hospitals are increasing their consumption of cloud infrastructure and services. The cost benefits of cloud help cash-strapped IT departments combat the growing volumes of data, reduce energy costs, shift capital expenditures to operational expenditures, and provide on-demand scalability for departments with ever-increasing storage demands. However, if hospitals are to embrace cloud technology, they must do so in a way that mitigates risks effectively. Not all cloud services are architected and maintained equally, and a thorough evaluation is always necessary. With the appropriate structure and protections in place, hospitals can safely put even their most sensitive data in the cloud. Often, data in a cloud data center is better protected than in a hospital's existing environment.

As threats to healthcare IT and patient data increase, remediation or "after-event"

services are not enough. The ideal strategy to mitigate security risk is to have a team of specialized security experts. But this is not always practical, as hospitals can't afford an army of specially trained staff, even if they were able to attract them. Adopting cloud services for IT infrastructure allows hospitals to partake in the security posture of cloud providers that operate at a scale that affords and demands the best talent and technology.

Cloud services go a long way toward mitigating risk, but not all of a hospital's infrastructure can run out of the cloud today. There is still technology that remains local. Security is much more than technology; it requires physical safeguards and administrative procedure—not to mention the value of an educated end-user base. To address these concerns, hospitals have begun sourcing specific security services from third parties.

Security-as-a-service allows hospital IT staff to focus on day-to-day operations and value-add projects instead of attempting to be security experts. With the threat landscape changing rapidly, security-as-a-service provides infrastructure, expertise and constant monitoring—a combination that is the most sophisticated defense against cybercrime.

1 "How to Protect Your Networks from Ransomware," U.S. Department of Justice, Computer Crime and Intellectual Property Section

CLOUDWAVE SECURITY-AS-A-SERVICE

CloudWave's OpSus Cloud Services offer security of scale and experience. OpSus is operated out of tier-four data centers that have triple redundancies, physical security, geographic stability, biometric entry screening and fire suppression. This model makes state-of-the-art technology such as periodic vulnerability scans and daily log reviews economical, so small hospitals can enjoy the benefits of cloud technology without a large capital expenditure. OpSus Cloud Services are designed with a defense-in-depth approach to security, measuring, monitoring and protecting at every layer: perimeter, server and port.

In addition to managed infrastructure, embedded with state-of-the-art security technology and process, OpSus Cloud Services include OpSus Defend, a suite of security services that allow hospitals to protect and secure their own on-premises private cloud. This managed service provides cloud-based security-as-a-service powered by Fortified Health Security. The service includes a team of dedicated healthcare security experts who know how to best protect a hospital's data, networks and services, as well as how to identify risks that could lead to a data breach.

OpSus Defend adds layers of managed protection and monitoring, either on premises or in a hosted environment, and is available as individual or bundled services.

OpSus Defend includes HIPAA risk analysis, vulnerability threat management, security information and event monitoring, penetration testing, vulnerability threat management and data loss prevention—all as modular, managed services. Delivered via the OpSus Cloud, OpSus Defend makes secure cloud affordable for hospitals, improves clinician workflows and helps hospitals meet compliance goals.

CONCLUSION

Healthcare organizations are under increasing pressure to protect healthcare data. Not only is this data valuable to clinicians as they provide patient care, but it has also become incredibly valuable on the black market. For hospitals, the costs and consequences of data breaches include loss of patient trust, brand damage, regulatory fines and even whole-hospital shutdowns. Hospital IT must find a way to mitigate the risks of new security threats, but the solution has to fit into traditionally tight budgets.

Sourcing security from a third party is an effective solution to the staffing and budgetary challenges in the face of constant

and evolving threats. Managed services take the strain off IT staff and help mitigate risk by not placing the burden for highly specialized skills on the organization's resources. Security-as-a-service provides the right combination of infrastructure and expertise for a sophisticated defense against cybercrime.

CloudWave's OpSus Cloud Services, including security, hosting, disaster recovery, backup and archive services, offer the risk-based information security procedures required to meet your regulatory and security goals. OpSus is the Healthcare Cloud, built and operated by healthcare people for healthcare people.

ABOUT CLOUDWAVE

CloudWave creates cloud solutions for healthcare that embrace the full continuum from on-premises customer private cloud to professionally managed cloud services in our OpSus Healthcare Cloud, to seamless federation with public cloud services like Office 365 and Microsoft Azure. CloudWave's focused portfolio of OpSus Healthcare Cloud services built for healthcare (B4H) include hosting of over 100 healthcare applications, disaster recovery with disciplined, auditable restoral testing, systems management, security, backup and archiving services. CloudWave architects healthcare IT solutions with the goal of operational sustainability. Our engineers and consultants have long-standing, successful track records designing and implementing solutions for hospitals. For more information, visit www.gocloudwave.com or call (877) 991-1991.

Cloud solutions are helping hospitals by providing a positive business impact on resource availability, economics, and compliance. CloudWave helps healthcare organizations meet challenges and transform IT with OpSus Cloud Services and on-premises solutions designed for the hybrid cloud. Visit **www.gocloudwave.com** to learn more.

CloudWave is helping hospitals transform IT with the OpSus Healthcare Cloud, built on a proven platform that includes HPE technology to minimize risk and deliver excellent performance.