

Three Reasons Your IT Infrastructure is More Secure in the Cloud



“From a security standpoint, the cloud offers many advantages over an on-premise IT infrastructure.”

Matt Ferrari
Chief Technology Officer
ClearDATA

Ask any healthcare CIO and you will find data security is a top-of-mind concern. Healthcare organizations that suffer data breaches risk a loss of reputation and costly fines and penalties related to stolen protected health information (PHI).

Because of this sensitivity to security risks, many healthcare organizations have been reluctant to move their information technology (IT) infrastructure to the cloud. “There is a myth that physical access implies security,” said Matt Ferrari, chief technology officer (CTO), ClearDATA. “The truth is that from a security standpoint, the cloud offers many advantages over an on-premise IT infrastructure.”

ClearDATA provides security solutions for healthcare providers, payers, pharmaceutical organizations and independent software vendors (ISVs). ClearDATA’s security solutions are built on top of the AWS Cloud. AWS provides the “undifferentiated heavy lifting” that secures an organization’s IT infrastructure. This allows healthcare organizations to focus on application security, often in partnership with companies such as ClearDATA.

“AWS is truly committed to driving cloud security. That is the why ClearDATA works with them,” said Ferrari. He outlined three reasons why leveraging the AWS Cloud offers security advantages over an on-premise approach.



1. Economies of scale

AWS’s investment in security includes exceptional physical security, secure infrastructure design and the highest level of professional expertise. Few, if any, healthcare providers can match AWS’s investment in security in these areas, said Ferrari.

By moving their IT infrastructure to the AWS Cloud, organizations can benefit from enterprise-level security at a lower cost required to provide the same level of security in an on-premise environment. “The neat thing about the cloud’s economy of scale is now small, rural-access hospitals can afford to access the same enterprise-level security services as larger organizations,” he said. “That has been an enormous improvement.”

In addition, the breadth and depth of AWS’s operations ensure AWS finds out about security concerns before individual providers do. “Many providers have only a few individuals internally who manage security for the entire organization. That is a tough road to climb,” Ferrari noted.

AWS manages more than 1 million active accounts each month, running every conceivable type of workload, which gives AWS insight into security issues that occur as infrequently as once in a billion operations. When issues are identified, AWS deploys remedies across the entire platform. For AWS

“The goal is to free up the healthcare organization’s internal IT team so they can concentrate on taking care of their doctors and nurses and other patient care provider.”

Matt Ferrari

customers, this means security issues are identified and remediated before they can impact the individual customer’s organization.



2. HIPAA Compliance Support

AWS offers more than 50 global compliance certifications and accreditations, which ensure healthcare organizations can operate on AWS in accordance with relevant laws and regulations, including HIPAA. “AWS has the ability to build HIPAA-compliant applications,” he said. “They will also sign Business Associate Agreements (BAAs) that document the AWS architecture is HIPAA-compliant at the time of deployment.”

By design, the AWS Cloud offers higher levels of transparency, monitoring and traceability than on-premise environments. The AWS Cloud allows organizations to set up rules-based, automated compliance – essentially “codifying” their compliance posture. Deviations from organizational policy – for example, an occurrence of unencrypted data storage – are detected and communicated automatically. “These capabilities are absolutely crucial when maintaining compliance and data security,” said Ferrari.



3. Robust, integrated security toolsets

“AWS has a deep security toolset, including network security, encryption and identity management,” said Ferrari. For example, AWS Trusted Advisor analyzes each customer’s AWS environment with a focus on optimizing performance, reducing costs and improving security. “Once you have a healthcare app in production, Trusted Advisor can identify where your security gaps may be inside of the AWS environment. Rather than just deploying tools and saying, ‘I’m secure,’ it helps you make sure those tools are working as intended,” Ferrari said.

One of the risks of using an on-premise security infrastructure is the tendency to “set it and forget it,” said Ferrari. Healthcare organizations often deploy new IT infrastructure and move on to other priorities. Even if they have processes for updating, upgrading and monitoring infrastructure components that impact security, most have no staff or expertise to provide 24/7 security support.

“Security and compliance are living, breathing things,” said Ferrari. “There are new threats coming at you every single day and your environment and applications are constantly changing.” Ultimately, moving IT infrastructure to the cloud helps CIOs focus less on security and more on their organization’s core competencies. “The goal is to free up the healthcare organization’s internal IT team so they can concentrate on taking care of their doctors and nurses and other patient care providers, rather than worrying about security,” Ferrari concluded.



About Amazon Web Services :

For 10 years, Amazon Web Services has been the world’s most comprehensive and broadly adopted cloud platform. AWS offers over 90 fully featured services for compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid and enterprise applications, from 42 Availability Zones (AZs) across 16 geographic regions in the U.S., Australia, Brazil, Canada, China, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of active customers around the world monthly – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit aws.amazon.com/health.