SOLUTION BRIEF
Intel Hardware-enabled Security
Healthcare Cloud Computing

Protecting Healthcare Data in the Cloud: GNAX Health and Intel

GNAX Health cloud solutions use Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI) to improve the security of sensitive data while increasing cryptographic performance by more than 60 percent over other encryption methods.

As changes sweep through the healthcare industry to reduce costs and improve clinical outcomes, healthcare organizations are turning to electronic health records (EHRs) to streamline and manage patient and other medical data. With the proliferation of EHR and other health IT systems, organizations must digitize and store increasing volumes of sensitive data. This presents two key challenges: providing the performance and availability needed for processing vast amounts of data, and protecting confidential health information to meet the requirements of regulations such as the U.S. Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Global Net Access Health (GNAX Health) cloud solutions for healthcare organizations use Intel® Xeon® processors equipped with hardware-enabled security features such as Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI)[1] to provide high availability and protection of sensitive data while preserving the server performance that users expect.

Data Proliferation: The New Health IT Challenge

Many EHR systems now include medical images, further increasing the volume of data that is processed and stored as the industry adopts higher image resolution, 3-D imaging, and video. Data retention requirements of HIPAA[2] and other regulations contribute to the proliferation of medical data—and the complexity of managing the health information life cycle is causing some organizations to retain this information in perpetuity.

Not only must organizations process and store healthcare information, they also must protect it. As the volume of digitized health information increases and electronic copies proliferate, so does the "attack surface" that may be exploited by a malicious threat agent. According to the Ponemon *2010 Annual Study, U.S. Cost of a Data Breach*,[3] the average cost of a data breach for U.S. companies rose for the fifth straight year to USD 7.2 million, or USD 214 per compromised record. The frequency of breaches is also on the rise; 26 percent of respondents to the 2011 Healthcare Information and Management Systems Society (HIMSS) Leadership Survey[4] indicated that they had experienced a security breach within the previous 12 months, up from 23 percent the previous year.

In dealing with the rising cost and frequency of data breaches and complying with HITECH Act regulations, healthcare organizations are highly motivated to protect their sensitive information. Many are looking at cloud computing as the answer.

ABOUT GNAX HEALTH

Global Net Access Health (GNAX Health) is a leading healthcare technology infrastructure provider. The company offers hospitals, pharmacies, labs, and other healthcare organizations mission-critical data center, co-location, managed hosting, storage and backup, and health information exchange (HIE) solutions, as well as enterprise-level VMware-based cloud computing services.

GNAX Health's cloud solutions deliver secure, scalable, and self-service public and private clouds that reduce expenses, improve application performance, and increase organization agility. GNAX Health's 70,000-square-foot mission-critical data center in Atlanta, Georgia, is SSAE 16 Type II compliant, with Tier-4 power, and serves as its home base with an additional strategic facility located in Dallas, Texas.

Learn more at www.gnaxhealth.net.

Cloud Computing and Health IT

The benefits of cloud computing are evident: highly available resources, improved efficiency and agility, simplified management, and lower costs. Healthcare CIOs who want to focus on improving patient care and generating revenue while optimizing limited IT resources can use the cloud to provide cost-effective capacity and application support.

However, when considering cloud computing, security and availability are top concerns to health IT administrators, who must protect the security and always-on availability of medical data to meet rigorous standards. Cloud computing holds the promises of reduced costs, pay-as-you-go services, and improved agility, allowing organizations to leverage external IT capabilities that they may not have in-house. When properly architected, cloud computing can also address the stringent security requirements and demands of the healthcare domain.

Protecting the Healthcare Cloud

With cloud solutions, it is easier to secure centralized data and applications (for example, using role-based access control) and also to protect them against viruses and intrusion. However, one aspect of security that is frequently overlooked is the physical security of the data center facility. Hosted cloud solutions with on-site security systems, such as key cards, biometric scanners, and armed security guards, limit direct access to data, so that even internal healthcare employees do not have physical access to the stored data. This addresses concerns expressed in the HIMSS Leadership Survey, which cites internal breaches from potentially disgruntled employees as their number one security concern. According to the 2011 CyberSecurity Watch Survey,[5] 21 percent of electronic security attacks were known or suspected to be from insiders, and 57 percent of the reported insider attacks resulted in unintentional exposure of private or sensitive data.

In addition to physical security controls, healthcare cloud facilities should also provide a reliable physical infrastructure with multiple layers of redundancy for power, cooling, and connectivity to help ensure cloud availability.

Finally, a secure cloud is built on a solid hardware, virtualization, and software stack. Healthcare cloud providers should use best-of-breed technologies in constructing the solution, not just for the computing power but also for technologies designed to secure the cloud. Proven products from trusted providers such as Intel, Cisco, VMware, and HP should make up the components of the system.

Understanding the security characteristics of a particular cloud offering is paramount, as a poorly architected cloud could significantly compromise data security and availability.

Healthcare Cloud Solutions from GNAX Health

GNAX Health provides healthcare technology solutions that create a healthcare information technology (HIT) ecosystem using a secure cloud infrastructure built on Intel® processors and virtualization software from VMware. The HIT ecosystem consists of private, public, and hybrid clouds; managed healthcare application delivery; secure offsite backup and disaster recovery; medical image vendor neutral archive (VNA); and healthcare software solutions such as health information exchange (HIE) and EHRs.

Healthcare providers operate a myriad of secondary, or second-tier, applications that are outside of their core clinical applications. With its Second Tier Healthcare Application Delivery system, GNAX Health has worked with suppliers to virtualize these applications so they can be run and managed in a private or public cloud, freeing costly resources at the client location.

GNAX Health VNA combines the cost benefits of cloud storage with the security of a robust, permanent picture archiving and communication system (PACS). GNAX Health normalizes the medical images and stores them in a neutral archive that is accessible to any PACS or EHR. This reduces costs in storage, application integrations, and future PACS migrations for hospitals while providing robust disaster recovery.

To complete its service offerings, GNAX Health also offers a hosted HIE and EHR platform for select end-user software solutions. The GNAX Health HIE is built on the National Health Information Network (NHIN) Direct and Connect standards established by the Office of National Coordinator (ONC) for Health Information Technology. It facilitates the exchange of healthcare records and medical images between healthcare providers. This secure Web-based solution is easy to use, interoperable with any EHR, and HIPAA compliant.

GNAX Health plans to release an ambulatory-level EHR in early 2012 that will integrate directly with the GNAX Health HIE. This software will be delivered over the Web with a simple and intuitive interface. It will provide a robust clinical health record system which includes e-prescribing, lab results delivery, and secure records exchange through the HIE module.

GNAX Health has created a highly efficient, stable, and secure cloud storage environment that is redundant across two geographically dispersed data centers. Its fully managed backup and disaster recovery solutions give users real-time replication capabilities with near zero loss in recovery time and point objectives.

The GNAX Health Cloud Infrastructure

In order to meet the demanding needs of healthcare organizations, the infrastructure that supports applications, such as the GNAX Health EHR and HIE, must be secure, reliable, and highly performant. This starts with the basic building blocks of the data center and extends to the hardware, virtualization, and software stack. GNAX Health carefully constructed each layer of its solution to adhere not only to the highest availability and security standards, but also to enable HIPAA and HITECH compliance.

The multiple layers of security and redundancy that GNAX Health has built into its healthcare cloud solutions is shown in Figure 1. GNAX Health has the necessary controls in place to protect its cloud, including biometric-controlled access to the data center, isolated customer silos in the healthcare cloud, and a two-factor, out-of-band authentication requirement for access to its HIE and EHR applications. This robust architecture relies on Intel Xeon processor-based servers, chosen specifically for their performance and security features.

The GNAX Health cloud infrastructure extends from its Atlanta, Georgia, facility to a secondary data center nearly 1,000

GNAX Health has created a highly efficient, stable, and secure cloud storage environment that is redundant across two geographically dispersed data centers.

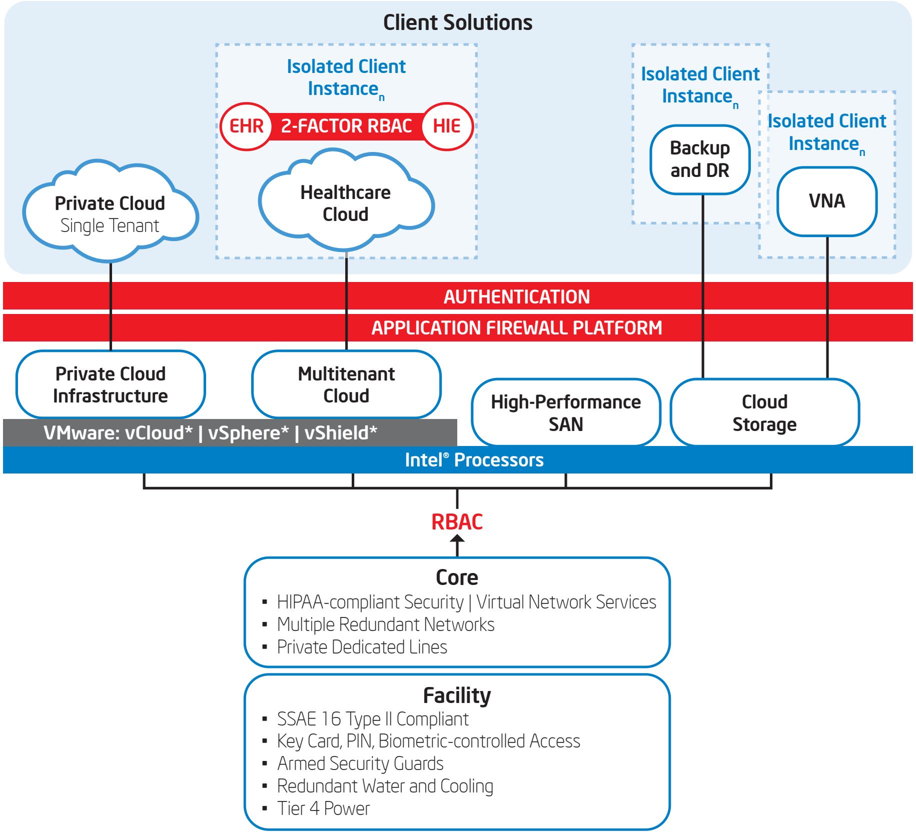
Each layer of the GNAX Health solution was built to adhere not only to the highest availability and security standards, but also to enable HIPAA and HITECH compliance.

miles away in Dallas, Texas, providing the geographic separation necessary for backup, disaster recovery, and business continuity solutions. Every level of the system is auditable and capable of generating appropriate reports required by HIPAA.

Intel® Xeon® Processors: Improving the User Experience and Compliance

User experience is impacted by the performance of the entire solution, from the client device and applications, to the network and server infrastructure. If technical security controls degrade performance, users tend to circumvent those controls or find other solutions, introducing major security risks to healthcare organizations.

GNAX Health relies on Intel® Xeon® processor 5600 series as the foundation of its cloud solution. Intel focuses on improving the robustness of technical controls through hardware-enabled security features, which improves performance not only on the backend server but also on client devices that access the system. Hardware-enabled security moves some tasks traditionally performed by software down to the


Client Solutions
Isolated Client Instance$_n$
EHR
2-FACTOR RBAC
HIE
Private Cloud Single Tenant
Healthcare Cloud
Isolated Client Instance$_n$
Backup and DR
Isolated Client Instance$_n$
VNA
AUTHENTICATION
APPLICATION FIREWALL PLATFORM
Private Cloud Infrastructure
Multitenant Cloud
High-Performance SAN
Cloud Storage
VMware: vCloud* | vSphere* | vShield*
Intel® Processors
RBAC
Core
▪ HIPAA-compliant Security | Virtual Network Services
▪ Multiple Redundant Networks
▪ Private Dedicated Lines
Facility
▪ SSAE 16 Type II Compliant
▪ Key Card, PIN, Biometric-controlled Access
▪ Armed Security Guards
▪ Redundant Water and Cooling
▪ Tier 4 Power

DR disaster recovery; **EHR** electronic health record; **HIE** health information exchange; **RBAC** role-based access control
SAN storage area network; **VNA** vendor neutral archive

Figure 1. The healthcare cloud architecture from GNAX Health has multiple layers of security and redundancy.

hardware layer, freeing computational cycles for improved performance for healthcare applications. These technologies also help defend against other threats such as increasingly sophisticated malware attacks. This is shown in Figure 2, where the core security logic is implemented in hardware.

Intel AES-NI is one example of hardware-enabled security. With Intel AES-NI, key components of the AES algorithm have been implemented in the hardware through the addition of several new processor instructions. The resulting solution moves the processing overhead of decryption and encryption to the CPU, providing encryption protection without impacting performance. It also hardens solutions against side channel leak vulnerabilities and associated exploits.

By employing Intel AES-NI in the EHR and HIE solutions hosted on its cloud platform, GNAX Health achieved a performance improvement greater than 60 percent (see sidebar) while also addressing the side channel attacks to which standard AES is vulnerable.[6]

Encryption is a key safeguard for protecting the confidentiality of sensitive healthcare information at rest and in transit, however ensuring the integrity of the actual computing platform is also important. The Intel Xeon processor 5600 series addresses this with Intel® Trusted Execution Technology (Intel® TXT), which mitigates the risk of malware attacks (such as rootkit). GNAX Health is testing this feature. When implemented, they will be able to verify the integrity of key platform components such as the BIOS and the hypervisor by comparing them with known good measurements of these components stored in the underlying hardware.

While security and performance are critically important, so is accessibility. This is especially the case in urgent patient care, where a delay in accessing patient data can be life threatening. Intel is committed to mission-critical

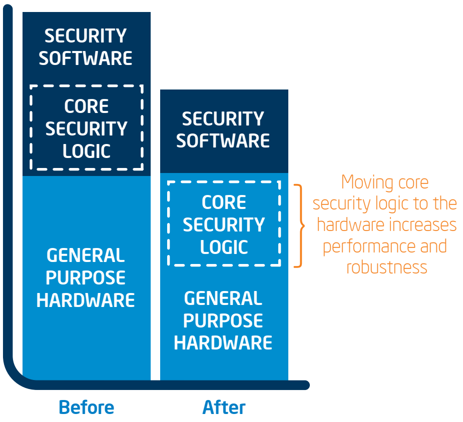


Figure 2. Hardware-enabled security provides increased performance and robustness.

CASE STUDY: INTEL® ADVANCED ENCRYPTION STANDARD-NEW INSTRUCTIONS

GNAX Health recently conducted benchmarking tests on their healthcare application servers to measure performance as well as average times to encrypt and decrypt a test file, both with and without Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI).

The results of these tests clearly show significant performance acceleration provided by Intel AES-NI—a nearly 50 percent increase in performance during encryption and more than 60 percent during decryption. This enables GNAX Health servers to protect sensitive healthcare data stored on servers with strong encryption, while also delivering improved healthcare application server performance and a better user experience to their customers.

The following tables show the details of the tests. The averages were computed from measurements taken over 10 test iterations.

Environment Used for Benchmark Testing	
Test Virtual Server	CentOS 5.5* with 1 GHz CPU and 8 GB RAM
Hardware	HP ProLiant BL460c G6* blade server with Intel® Xeon® processor E5620
Software	VMware vCloud Director 1.0.1*, VMware vSphere 4.1 U1*, Java* Development Kit v 1.6
Encryption Library	Network Security Services (NSS) v 3.12.6*
Test File Size	181 MB
Encryption	AES CBC 256-bit encryption

	Average without Intel® AES-NI	Average with Intel® AES-NI	Acceleration
Encryption	6.70 seconds	3.40 seconds	49.25% (1.97x)
Decryption	7.40 seconds	2.80 seconds	62.16% (2.64x)

computing, and the latest Intel® Xeon® processors offer an extensive set of features for reliability and availability of mission-critical deployments.

Conclusion

Healthcare organizations looking to benefit from cloud computing must carefully choose a cloud solution supplier who can maintain required security and availability standards. GNAX Health's healthcare technology solutions and the cloud infrastructure that supports them are based on Intel Xeon processor 5600 series-based servers, which include hardware-enabled security technologies such as Intel AES-NI. These technologies are a critical component of the administrative, physical, and technical controls that make up GNAX Health's multi-layered approach to security. The result is a robust, secure, and highly available cloud infrastructure that runs important healthcare systems, reliably protects sensitive healthcare data, and complies with organizational security protocols and regulations such as HIPAA and HITECH.

Learn more about GNAX Health and Intel.

- GNAX Health: www.gnaxhealth.net
- Malware Reduction: Intel® Trusted Execution Technology (Intel® TXT): www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html
- Intel® Advanced Encryption Standard-New Instructions: www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html
- Intel Mission-critical Computing: www.intel.com/missioncritical

[1] AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling AES-NI requires a computer system with an AES-NI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. For availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer.

[2] HIPAAdvisory, "Record Retention Periods" by Sue Dill Calloway, www.glrm-online.com/pdfs/HIPAA%20Record%20Retention%20Periods%202006.pdf

[3] Ponemon, "2010 Annual Study: U.S. Cost of a Data Breach," www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

[4] Healthcare Information and Management Systems Society (HIMSS), "2011 HIMSS Leadership Survey," www.himss.org/2011Survey/healthcareCIO_final07.asp

[5] Carnegie Mellon University, "2011 CyberSecurity Watch Survey," www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf

[6] Intel Corporation, "Intel® Advanced Encryption Standard (AES) Instructions," www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, reference www.intel.com/performance/resources/benchmark_limitations.htm or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Printed in USA 0811/CG/KC/PDF ♻ Please Recycle 325593-001US