Cloud Security for Healthcare and Life Sciences Organizations
The healthcare and life sciences (HCLS) industry is in the midst of an evolution as organizations have embraced cloud technology. This cloud adoption has been driven by modernization, the rise of personalized medicine, economic pressures, and security and compliance regulations. According to industry research*, 56% of healthcare organizations named cloud the technology that will have the most transformational impact on their operations by 2020.

HCLS organizations are applying cloud technologies to processes for gathering, storing, and analyzing medical data. As an organization’s usage matures, they are often scaling this adoption to include advanced technologies such as container management, machine learning (ML), artificial intelligence (AI), and data and analytics. Finally, there is a growing trend of moving existing on-premises applications to the cloud. This adoption will have significant impact on the HCLS industry and how it impacts the delivery of patient care.

Security and compliance requirements are inherently one of the strongest drivers for HCLS organizations. Security governance, risk, and compliance are key concerns when evaluating cloud technologies. The HCLS industry faces stringent security regulations and are always under pressure to protect sensitive patient data from threats. This is due to the sensitive information they gather and maintain, and the delayed adoption of security best practices. In fact, according to industry research*, healthcare organizations identified information security (41%) and regulation/compliance (29%) as top IT pain points more frequently than organizations in other categories.

"Healthcare organizations identified information security (41%) and regulation/compliance (29%) as top IT pain points more frequently than organizations in other categories."

In this whitepaper, SANS Director of Emerging Technologies, John Pescatore, provides practical scenarios and guidance to help you quickly identify the right use cases to optimize cloud security operations, as well as determine which specific technologies are needed to execute your security mission in the cloud. John introduces this guidance through the NIST Framework, a comprehensive set of security controls that Amazon Web Services (AWS) has aligned its services to.

Building on John’s perspective, AWS Marketplace also shares how this framework can be applied to your AWS Cloud environment with an introduction to relevant AWS security services and AWS Marketplace software sellers. AWS Marketplace will also provide case studies that share how HCLS organizations are approaching security in their AWS environments, and steps you can take to get started strengthening your security posture.
Introduction

The use of cloud services by businesses and government agencies has grown rapidly, with the movement of production workloads to infrastructure as a service (IaaS) growing at more than 35 percent per year. This move to cloud-based services has required security programs to extend operations beyond the data center and to re-evaluate security architectures, processes and controls to maintain effectiveness and efficiency in their efforts to secure their sensitive business applications, be they local or cloud-based.

Some common success factors have emerged from enterprise cloud use cases where security has been maintained and even improved while moving critical services to IaaS:

- **Integrate security services available from cloud service providers with third-party security products/services to secure business-critical cloud workloads.** The virtualized infrastructure of IaaS offers native security services and capabilities that greatly reduce the attack aperture, and that can be augmented by additional third-party security controls when risk assessments require higher levels of protection.

- **Extend security architecture, processes and controls across local data center applications and cloud IaaS implementations.** Most enterprises use a mix of applications that run in local data centers, on external IaaS services and in hybrid configurations of both environments. Using common security controls and

---

products across environments reduces the skills gap, eliminates data islands and silos, and makes it simpler to maintain a single security dashboard with a meaningful set of security metrics.

- **Use an established framework to plan, implement and justify the changes needed to enable secure business use of IaaS.** While securing cloud services relies on the same basic security ingredients used in traditional data center systems, the overall security architecture, processes and security controls must change to ensure that the necessary levels of reliability and safety are maintained. Basing the process on an established framework, such as the NIST Cyber Security Framework, ensures a thorough risk evaluation and implementation and provides a solid basis for justifying plans, strategies and resource requests to management.

Many businesses and government agencies have followed these guidelines to maintain their on-premises levels of security for production applications as those applications were moved to IaaS services. Even better, though, as new cloud security approaches emerged, they were able to raise the security level overall.

**Keeping Business Safe—or Even Safer—in the Cloud**

Cloud services security has evolved pretty much as security has evolved for all new technologies and innovations. Initially, security teams, with a healthy fear of the unknown, rated external cloud services as high risks because of reduced visibility and control, and so attempted to prevent their use. As the benefits of cloud services became apparent to business units and IT organizations, they adopted them, even if it meant bypassing the security organization. Security teams considered those cloud deployments to be rogue efforts, and therefore did not even evaluate the security arrangements.

In the face of security’s resistance, CEOs began to tell CISOs, “We are moving to use cloud services, so tell us how to secure them or just get out of the way.” Only then did most security teams begin to try to reactively add security controls on top of cloud services and replicate on-premises data-centric security processes at virtualized cloud-based services. Their efforts did usually reduce risk, but at a high cost of business disruption. What’s more, the tacked-on security processes were redundant and inefficient.

But things have improved. Today, organizations can build in security as an integrated part of the migration to IaaS services, optimizing security processes so they can be extended to work seamlessly across both local and external services. Similarly, security operations teams can focus on selecting products to implement security controls that are integrated across both environments, often minimizing vendor count, employee staffing and training requirements while enabling a single view of situational awareness and risk.

*Today, organizations can build in security as an integrated part of the migration to IaaS services, optimizing security processes so they can be extended to work seamlessly across both local and external services.*
Differences in Securing Cloud Workloads

Just as any recipe for a meal can be broken down into the five basic tastes (sweet, sour, salty, bitter and umami), securing information always comes down to providing three basic security functions, the “CIA triad” of confidentiality, integrity and availability. Security processes based on one or more of those basic functions deliver protect/detect/respond services using common security practices and products such as vulnerability assessment, configuration management, firewalls, anti-malware, SIEM and data protection.

All these security controls are necessary because of three key ongoing vulnerabilities:

- Applications and operating systems continue to have vulnerabilities that are not known until researchers find them and/or attackers exploit them.
- System administrators often make mistakes in configuring and maintaining servers and PCs.
- Users will always fall victim to scams such as phishing and malvertising.

The adoption of cloud services does not eliminate any of those areas of vulnerability—and can in fact magnify them, because the power of the cloud can greatly expand the vulnerabilities that result from weak practices in IT or security operations and administration.

On the other hand, IaaS brings the opportunity to significantly reduce the frequency of dangerous errors in operations and administration. The virtualized infrastructure of cloud services supports internal security mechanisms that evolving security processes can use in a number of ways:

- **Containers**—A container is a packaged unit of software that includes the application, the runtime operating systems, tools, libraries and so on. Well-prepared security teams can bake in configuration baselines and security agents that ensure that security controls will run anytime an application is launched.

- **Isolation**—Network segmentation has long been a proven way to limit exposure from attackers to an isolated segment and limit the spread of malware or other payloads. IaaS offerings can provide virtual private clouds that support segmentation at a granular level, with automated placement and enforcement when new servers are enabled. Containers also provide process isolation that enables CPU and memory utilization to be defined and limited on a granular basis.

- **Orchestration and automation**—Many security processes are relatively static IF–THEN sequences that are often documented in playbooks. Orchestration defines the conditions and sequences, but implementation can be a highly manual process. Integration of security processes into cloud service management capabilities can automate many steps in security operations playbooks.

In this section we outlined the differences in securing cloud workloads. Next, we discuss using a security framework to address the needs security teams face.

---


Securing information always comes down to providing three basic security functions, the “CIA triad” of confidentiality, integrity and availability.
The NIST Cyber Security Framework (CSF) came out of the Cybersecurity Enhancement Act of 2014, with the charter to be “a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure.” While there is nothing revolutionary about the NIST CSF, the “consensus-based, industry-led” approach resulted in widespread acceptance and adoption of the CSF by U.S. enterprises and the governments of several other countries.

The top level of the framework lists the five major functions (identify, protect, detect, respond and recover) of cybersecurity. These functions, which are intended to include all basic cybersecurity activities, are broken into 22 categories representing program-level outcomes required to maintain cybersecurity, as illustrated in Figure 1. These categories are further decomposed to list 98 subcategories that list specific results required to successfully implement the appropriate level of security.

The identify/protect/detect/respond/recover construct has proved to be a powerful tool in explaining to upper-level management the necessary core functions for protecting business systems, but in operational environments, very few processes or products perform just one of the top-level functions. For example, while firewalls are most closely identified with protective technology, they also play key roles in identify, protect, detect and respond. The construct also does not differentiate functional areas, processes and products that are important to use for proactive (before the attack) or reactive (during and after the attack) reduction of risk.
Moving from Frameworks to Features, Talk to Walk

Business units have been demanding the use of cloud-based services because of advantages they provide to efficiently deliver business services and adapt to changing needs. In order for security controls to be successful across both data center and cloud environments, security architectures, processes, controls and operations need to meet those same demands and provide the same seamless integration achievable in hybrid cloud services.

Delivering Seamless Security Services

There are three key focus areas for delivering seamless security services across the data center and IaaS-based applications.

Integration of Infrastructure and External Security Controls at Each Boundary

Most organizations already have standard architectures for delivering identify/protect/detect/respond/restore services to data-center-based systems. When working with physical servers, organizations rely on a mix of security capabilities built into the Linux and Windows operating systems, as well as third-party host-based and network-based security controls. As local data centers moved to virtualization, another element was added to the mix: security primitives available in VMware or other underlying virtualization platforms. Similar, and often enhanced, security primitives are available from all major IaaS providers.

For companies other than startups, extending existing architectures to secure cloud-based services is the key first step. Those organizations should focus on integrating services at each boundary layer. See Figure 2.

In the early days of using the internet, many enterprises felt that there was a security gain by using products from different vendors at different layers in the architecture. However, real-world results proved this thinking to be false.7 For most security organizations, keeping the security architecture consistent across cloud services and the data center will support running the same security products across both environments. This will reduce training costs and administrative errors and also support more timely and accurate situational awareness and continuous monitoring.

7 www.gartner.com/document/500890?ref=solrResearch&refval=214539204&qid=d3f5b689a39463b6c77406155a9672a1 [Registration required for access.]
Common Practice/Due Diligence Controls

Many security controls, such as firewalls, log monitoring and even intrusion detection systems, are mandated by compliance regimes (e.g., PCI DSS, HIPAA, FISMA, etc.) and represent due diligence controls. Any system containing sensitive or mission-critical data connected to the internet without a firewall and without log collection/monitoring/analysis would be considered noncompliant. While compliant does not always mean secure, noncompliant *almost always* represents unacceptable business risk.

Best Practice/“Lean Forward Risk Reduction” Controls

As the continuing news of breaches makes clear, for many organizations “common practice” is insufficient to mitigate their actual risk exposure. Best practice approaches that increase identify and protect levels and decrease time to detect, respond and restore are key, but require additional resources and skill levels. “Lean forward” organizations that have the staff skills and product/service budgets to deploy, tune and monitor advanced and proactive risk reduction controls generally are not the ones showing up in the breach headlines.

Using the NIST CSF Framework as a Starting Point for Putting Controls in Action

As mentioned earlier, the major security functions listed in the NIST CSF do not represent distinct product areas. However, Table 1 assigns a primary mapping for each major product area. This mapping can be used as a starting point in conjunction with a scenario-based approach to ensure that 1) you have no due diligence/compliance gaps, and 2) you have a solid baseline to which advanced capabilities can be added.

The decision on when to move beyond due diligence should be based on your own risk analysis. The NIST CSF points to the NIST Risk Management Framework, but many organizations have their own risk assessment and tracking processes that are outside the scope of this paper.

The selection of architectures and products to implement security controls to protect

<table>
<thead>
<tr>
<th>NIST CSF Functions</th>
<th>Primary Product Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Due Diligence</td>
</tr>
<tr>
<td>Identify</td>
<td>Configuration management</td>
</tr>
<tr>
<td></td>
<td>System management</td>
</tr>
<tr>
<td></td>
<td>Vulnerability assessment</td>
</tr>
<tr>
<td></td>
<td>Awareness training</td>
</tr>
<tr>
<td>Proactive</td>
<td>Access management</td>
</tr>
<tr>
<td></td>
<td>Data masking</td>
</tr>
<tr>
<td></td>
<td>DDOS filtering</td>
</tr>
<tr>
<td></td>
<td>Endpoint protection</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>Ops skills training</td>
</tr>
<tr>
<td>Reactive</td>
<td>Intrusion detection systems</td>
</tr>
<tr>
<td></td>
<td>Network monitoring</td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
</tr>
<tr>
<td>Respond</td>
<td>Incident response services</td>
</tr>
<tr>
<td></td>
<td>Trouble ticket systems</td>
</tr>
<tr>
<td></td>
<td>System/endpoint backup</td>
</tr>
</tbody>
</table>

---

cloud-based applications should be based on that assessment and the particular
cloud deployment scenarios you face. The NIST CSF details the use of profiles and
implementation tiers for this purpose. We will focus on a simplified approach
based on the three most common cloud adoption scenarios facing businesses and
government agencies:

- Dev/test environment
- Business app launched on or moved to IaaS
- Hybrid architecture

These scenarios represent the most frequent scenarios for securely moving business
applications to cloud services in the typical order of adoption. While they do not
represent every possible situation, these three scenarios generally provide a proven
starting point you can tailor to your unique situation.

At the due diligence level, the basic security controls required are largely the same
across the scenarios when business-critical or sensitive data is involved. The sections
that follow describe the different drivers for each scenario with the assumption that
such sensitive data is involved.

**Dev/Test Environment**

Moving a development and test environment to the cloud is often the first toe in
the water for enterprise use of IaaS. The “pay as you go, not when you don’t need
it” nature of IaaS is well-suited for this application. Rather than waste dedicated
resources for development and test efforts that might only be used a small
percentage of the time, an IaaS-based dev/test environment can be spun up and paid
for only when actually needed.

All too often, the security organization is not involved in the migration, a circumstance
with three downsides:

- Test data used in the IaaS instantiation often puts sensitive customer and
  business data at risk.
- That same environment can be used to rapidly evaluate operating systems and
  application patches, reducing exposure.
- The initial movement to dev/test on IaaS is an ideal chance for the security
  operation team to “plus up” its skills and develop knowledge around cloud
capabilities and risks.

Data masking, obfuscation or encryption is a critical due-diligence requirement for
dev/test environments. While realistic test data is necessary, you should never expose
live customer data in dev/test usage. Similarly, standard boundary/perimeter network
segmentation and monitoring as implemented by firewalls and IDS are required
between this environment and the corporate network. If dev/test requires a live internet
connection, the same controls are required at the internet connection side.

---

**Analyst Program**

*How to Optimize Security Operations in the Cloud Through the Lens of the NIST Framework*
Because the entire purpose of a dev/test environment is to support an environment to deliver product-ready applications, the due diligence level includes application security (AppSec) testing tools/services that compliance regimes do not always require. Embedding AppSec testing into the development and test cycle is especially important in the rapid iteration cycles in agile/DevOps methodologies.

The traffic and user/endpoint behaviors on dev/test networks differ greatly from those on production systems, and advanced analytics and behavior-based detection/prevention usually generate large volumes of false positives. With data masking in use, there is less of a need for data loss prevention, and dev/test environments generally do not require full DDoS protection. See Table 2.

**Business App Launched on/Moved to IaaS**

When a production application is launched from or moved to IaaS, the full range of confidentiality/integrity/availability services is required across all five NIST CSF functions to reach the due diligence level. From a product perspective, only data masking is typically not included in the architecture, because real product data is required and must be safeguarded. A typical example is a new web-based commerce application that will be first launched from an IaaS platform, but the same security principles apply to an existing application being updated and moved to IaaS.

The due diligence level of this scenario has two key goals:

- **Extend security configuration standards and continuous monitoring to IaaS.**
  Every organization should have standards for the baseline configuration of all servers, applications, security controls and the like used in the production environment. These same standards, such as the Center for Internet Security Benchmarks, should be applied to applications running on IaaS. The processes for monitoring for misconfigurations and vulnerabilities should be identical for both data center applications and those running in IaaS. When it comes to product selection, it is key to have logging, monitoring and configuration/vulnerability analysis that integrates with a common SIEM platform and supports all applications.

---

Table 2. Security Control Set for Dev/Test Migration to IaaS

<table>
<thead>
<tr>
<th>NIST CSF Functions</th>
<th>Primary Product Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Due Diligence</td>
</tr>
<tr>
<td>Identify</td>
<td>AppSec testing</td>
</tr>
<tr>
<td></td>
<td>Configuration management</td>
</tr>
<tr>
<td></td>
<td>System management</td>
</tr>
<tr>
<td></td>
<td>Vulnerability assessment</td>
</tr>
<tr>
<td>Protect</td>
<td>Access management</td>
</tr>
<tr>
<td></td>
<td>Data masking</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>Ops skills training</td>
</tr>
<tr>
<td>Detect</td>
<td>Intrusion detection systems</td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
</tr>
<tr>
<td>Respond</td>
<td>Incident response services</td>
</tr>
<tr>
<td></td>
<td>Trouble ticket systems</td>
</tr>
<tr>
<td>Recover</td>
<td>System/endpoint backup</td>
</tr>
</tbody>
</table>

---

• Use common products for protect/detect infrastructure functions where possible. Most firewall, intrusion detection/protection, and endpoint protection products (and those like them) have both data center products and cloud-centric versions. Using the same vendor on IaaS as is used for data center security has all the advantages previously discussed.

When risk analysis requires higher levels of protection and resources (people, skills, budget) to support it, moving to the advanced security level generally means being proactive in avoiding or quickly mitigating vulnerabilities (AppSec testing, penetration testing); reducing unnecessary access privileges through secure access management, encryption and strong authentication (as a minimum for admin access); and reducing time to detect/respond/restore through the products and services listed.

In addition, you can raise the security bar for applications running on IaaS with such advanced cloud security capabilities as secure images and containers (discussed earlier). DDoS protection becomes more critical when an application is fully cloud-based. While cloud management platforms are not strictly security products, their use can increase the accuracy of asset management and vulnerability data, as well as support compliance reporting requirements. Governance, risk and compliance (GRC) platforms can greatly reduce the cost of demonstrating compliance (allowing more of the security budget to be focused on security), but they require large up-front investments in both procurement costs and administrative time and skills. See Table 3.

Hybrid Architecture

The final scenario is when organizations begin to run applications that span both local data centers and IaaS services in a near seamless manner. A common situation is expanding an application that has been running in a data center servicing one geographic region to global coverage using IaaS to expand capacity and proximity. The risk assessment used for the previous scenario (“Business App Launched on/Moved to IaaS”) does not change for this scenario, but hybrid cloud environments do raise a number of unique challenges and opportunities:

<table>
<thead>
<tr>
<th>NIST CSF Functions</th>
<th>Primary Product Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Due Diligence</strong></td>
<td><strong>Advanced/Lean Forward</strong></td>
</tr>
<tr>
<td>Identify</td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td></td>
</tr>
</tbody>
</table>

- **Due Diligence**
  - Awareness training
  - Configuration management
  - System management
  - Vulnerability assessment

- **Advanced/Lean Forward**
  - AppSec testing
  - GRC
  - Penetration testing
  - Cloud management platforms

- **Proactive**
  - Access management
  - DDOS filtering
  - Endpoint protection
  - Firewall
  - Ops skills training

- **Detect**
  - Intrusion detection systems
  - Network monitoring
  - SIEM

- **Respond**
  - Incident response services
  - Trouble ticket systems

- **Recover**
  - System/endpoint backup
  - Firewall policy management
  - Encryption
  - Intrusion prevention systems
  - Secure image/container
  - Strong authentication
  - Data analytics
  - Data loss prevention
  - Forensic analysis
  - High-avail/mirroring services
• Changes in policy standards for identify and protect products must be distributed, validated and audited in an integrated manner across the environments.

• Detect products have a more complex environment to monitor, and behaviors in the more rigid data center environment often differ from what is seen on the IaaS environment.

• Forensic analysis as a respond function has more complicated attack paths to collect and analyze.

• If the IaaS environment supports a failover or mirroring capability, backup and recovery may be simplified in hybrid cloud environments.

For organizations that have not first moved through the first two scenarios, the migration to hybrid cloud services should not proceed without establishing a baseline of due diligence cloud infrastructure protection, monitoring and respond/restore capabilities, along with a security operations staff that has already expanded its skills to include cloud environments. From this starting point, staff can integrate the same advanced capabilities as in the previous scenario to raise security levels.

The primary difference in product selection for the hybrid cloud scenario is selecting products that you can deploy, manage and monitor across both environments (see Table 4). The typical starting point is to look at the security products in use on the data center side and see whether those vendors are listed in the IaaS provider’s partners list or marketplace. Ideally you would use only products that are supported across the major IaaS providers, but there are simple workarounds for many product areas if you have to use different products:

• Network policy management tools support change control, auditing and analysis of firewall policies across multiple vendors.

• Any host-based product that supports syslog generation can report to a SIEM console.

• The output from disparate vulnerability assessment products that support the Security Content Automation Protocol (SCAP) can be consolidated by SIEM products.

<table>
<thead>
<tr>
<th>NIST CSF Functions</th>
<th>Primary Product Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Due Diligence</td>
</tr>
<tr>
<td>Identify</td>
<td>Configuration management</td>
</tr>
<tr>
<td></td>
<td>System management</td>
</tr>
<tr>
<td></td>
<td>Vulnerability assessment</td>
</tr>
<tr>
<td></td>
<td>Awareness training</td>
</tr>
<tr>
<td>Proactive Protect</td>
<td>Access management</td>
</tr>
<tr>
<td></td>
<td>Data masking</td>
</tr>
<tr>
<td></td>
<td>DDOS filtering</td>
</tr>
<tr>
<td></td>
<td>Endpoint protection</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>Ops skills training</td>
</tr>
<tr>
<td>Detect</td>
<td>Intrusion detection systems</td>
</tr>
<tr>
<td></td>
<td>Network monitoring</td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
</tr>
<tr>
<td>Respond</td>
<td>Incident response services</td>
</tr>
<tr>
<td></td>
<td>Trouble ticket systems</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td>System/endpoint backup</td>
</tr>
</tbody>
</table>

Table 4. Security Control Set for the Hybrid Cloud
Using Metrics to Assess and Communicate Effective Security Operations

From a security perspective, the movement to use IaaS does not change the need to collect meaningful security metrics. Metrics are needed not only to assess, evolve and optimize security operations, but also to provide accurate status, trend and risk data to management.

The minimal set of operations metrics that organizations should establish for their systems running on cloud services include:

• **Asset management accuracy**—What percentage of assets are identified and profiled correctly?

• **Time to detect**—How quickly is an attack detected?

• **Time to respond**—How quickly are incident response actions initiated?

• **Time to restore**—How quickly is incident response completed and full business services restored?

• **Real-time risk assessment**—What percentage of business-critical operations is currently at risk from known threats?

For most organizations, the metrics that security personnel show to CEOs and boards of directors will be different from operational metrics—the focus needs to be more strategic and show more connection to business services and less to attacks and threats. Figure 3 translates the key performance metrics into points that will resonate with CXOs and boards.

---

**Figure 3. Connecting Metrics to Business Services**

<table>
<thead>
<tr>
<th>EFFICIENCY</th>
<th>EFFECTIVENESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrease the cost of dealing with known threats.</td>
<td>Increase the speed of dealing with a new threat or technology.</td>
</tr>
<tr>
<td>Decrease the realized impact of residual risks.</td>
<td>Decrease the time required to secure a new business application, partner, or supplier.</td>
</tr>
</tbody>
</table>
| Decrease the cost of demonstrating compliance. | Reduce incident cost:  
  - Less downtime  
  - Few customer defections |
| Increase incident count with constant staff. | Security as a competitive business factor |
| Maintain level of protection with less EBITDA impact. | |
Summary

Thousands of businesses are successfully and safely using cloud services to meet business goals for increasing the agility and decreasing the cost of IT services. SANS has seen several common patterns across the security operations organizations that have been able to deliver the needed security architectures, processes and controls to enable safe business use of cloud services:

• Organizations use the NIST CSF Framework as a baseline and a tool to communicate and justify strategy, plans and resource needs to management.

• They involve the security team when IT first tries out IaaS, typically when dev/test is moved to the cloud. A robust selection of third-party security products in the cloud environment should be a key input into the evaluation of the IaaS provider.

• Teams extend the security architecture and processes to include applications running in the cloud, focusing on the most common business use cases.

• They maximize both effectiveness and efficiency by using the same third-party security products in the cloud that they use to secure on-premises applications (where possible).

• Once a secure baseline has been established for security operations in the cloud, security teams investigate cloud-specific security processes and controls that can result in advances over existing security practices.

Security teams will need to use mixes of people, processes and technologies to make sure business use of cloud services is secure. These patterns apply across all three of those areas. An honest assessment of your security operations team skills and processes completeness against the NIST CSF will enable you to evolve and extend security operations to enable business services while justifying needed changes and resources allocations.
**About the Author**

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems “and the occasional ballistic armor installation.” John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

**Sponsor**

SANS would like to thank this paper’s sponsor:

![aws marketplace](#)
Healthcare and life sciences (HCLS) organizations are increasingly faced with strict regulation and growing security needs. This is because the HCLS industry has been slower in adopting security best practices, while also hosting a wealth of information that is valuable to those seeking to exploit it. This information, in the form of electronic medical records (EMRs) for example, are core to a HCLS organization’s operations. It is also core to regulation compliance, such as HIPAA and PII. This creates the challenge around information security that drives technology decision-making.

Forward-thinking HCLS organizations are embracing security advances. Many are doing so as they migrate workloads and data to the cloud, and are trying to maintain compliance and protection while doing so. The first step to prioritizing your HCLS organization’s security controls is to understand which Amazon Web Services (AWS) services you can leverage to best protect your assets and maintain compliance. As you can see below, AWS services follow the NIST framework to make it a seamless process.
Secondly, HCLS organization's moving their workloads and data to the cloud will need to prioritize the controls that extend past the available AWS native services. In these cases, AWS Marketplace offers thousands of software seller solutions for healthcare security needs. AWS Marketplace is a digital software catalog where security practitioners can find, try, buy, deploy, and manage software that runs on AWS. This enables organizations to deploy a comprehensive security architecture across their AWS environments.

Case studies in AWS Marketplace for HCLS organizations

Here are just a couple of examples of how HCLS organizations are utilizing AWS Marketplace security software solutions to facilitate innovation and establish secure IT operations.
Health Quest cuts disaster recovery costs in half with CloudEndure

Located in New York, Health Quest is an integrated delivery healthcare system that services 250 doctors in four hospitals across the Hudson Valley area. With more than 6,000 employees, Health Quest supports award-winning hospitals and highly-ranked specialty care. The organization’s services are focused on providing an accessible continuum of care.

“The majority of our disaster recovery is sitting in the cloud with CloudEndure. This downsizing has already resulted in about 50% cost savings.”
- Rob Gilliland, CTO, Health Quest

The Challenge

In the healthcare industry, many different systems operate interdependently, which makes it difficult to achieve IT resiliency. And with government regulations requiring all services to be covered by a robust disaster recovery plan, healthcare organizations face significant challenges for supporting new technology.

While Health Quest was able to protect hundreds of servers with its secondary disaster recovery site, the strategy wasn’t sufficient for a greater number of servers. Based on their previous strategy, the solution would have been to purchase additional servers. However, because the old strategy and infrastructure were never able to achieve the four-hour Recovery Point Objective (RPO), the team decided to find a new, cloud-based disaster recovery solution that could support its mix of physical and virtual servers.

The Solution

The pressure of compliance led Health Quest to evaluate a few different cloud solutions that could enhance its disaster recovery capabilities and included managed services to ensure their systems were replicated properly and that the environment was healthy. Their stringent parameters led them to evaluate CloudEndure.

The proof of concept process included Health Quest choosing a few of its critical applications and deploying them in AWS. The IT team was able to spin up systems and infrastructure without any data loss or application access issues. Health Quest then moved forward implementing CloudEndure Disaster Recovery on hundreds of servers, including multiple checkpoints for point-in-time recovery.
The Results

Since implementation, Health Quest has reduced the size of its secondary data center so that it is only responsible for a small subset of disaster recovery. “The majority of our disaster recovery is sitting in the cloud with CloudEndure,” said Rob Gilliland, CTO at Health Quest. And the financial impact? According to Gilliland, “This downsizing has already resulted in about 50% cost savings.”

Moreover, now that CloudEndure has become part of normal operations, Health Quest’s real-world Recovery Point Objective (RPO) has dropped to two minutes in most cases. Another key benefit that Health Quest has enjoyed is the single pane of glass interface. In the past, coordinating disaster recovery testing was time-consuming — sometimes taking several weeks as the IT team managed recovery issues. “With CloudEndure, all we have to do is log into the CloudEndure website and we can see everything in real time,” explained Gilliland. “This helps us create a fluid testing process and stay on top of the whole DR environment. In a fast-paced IT department that is undermanned, having CloudEndure’s simple management and expert support staff is very helpful.”

About CloudEndure

CloudEndure provides Disaster Recovery and Live Migration for all applications, allowing enterprises to mobilize entire workloads to and across clouds with near-zero downtime and no data loss. CloudEndure solutions, including CloudEndure Disaster Recovery, can be found in AWS Marketplace.

Case Study 2: SANSOROHEALTH

Sansoro Health improved customer service and speed-to-market with ClearDATA

Sansoro Health makes it easy to design and deploy applications that exchange data with electronic health records (EHRs) in real-time. The company’s flagship product, Emissary®, is a reusable, rapidly scalable, and secure API solution for robust EHR data integration. Its plug-and-play simplicity takes the burden of integration off busy health IT professionals, so they can focus their efforts on key initiatives. Emissary also provides a custom integration solution that is readily scalable and easily adjusts to software updates.
There have been no connectivity challenges and almost 100% uptime (99.9999%). We’re seeing healthcare evolve and be more open to the benefits of the cloud, and ClearDATA is the answer. There is no doubt: we would not have closed a key account without the healthcare compliance solution ClearDATA brings to the table."

- Mike Pietig, Customer Success Officer and Co-founder, Sansoro Health

The Challenge

Health IT applications are usually deployed in one of two ways: on local application servers that are kept on-premises or in remotely hosted servers in the public cloud. Increasingly, just as in other industries, the cloud is becoming the preferred option. However, hosting these applications in the cloud requires specialized healthcare expertise and keen knowledge of security and privacy regulations designed to safeguard Protected Health Information (PHI).

“We are getting more requests from our partners who don’t want to be in the hosting business and are looking to Sansoro Health to provide an all-in-one solution that covers both healthcare managed services and integration of their application to EHRs,” says Rich Walker, IT Director for Sansoro Health. “To meet those needs, we wanted to partner with an expert in healthcare managed services and compliance.”

The Solution

After considering several alternatives, Sansoro Health chose ClearDATA running on AWS.

“We found ClearDATA through a reference and we immediately saw there was strong alignment,” says Mike Pietig, Customer Success Officer and co-founder at Sansoro Health. “The cost was right, and we knew that ClearDATA on AWS could keep up with our aggressive growth goals. We also knew that ClearDATA would stand behind its technology, offer HIPAA and HITRUST protection, and protect PHI by limiting our exposure and risk.”

The Results

Working with ClearDATA, Sansoro Health can provide the turn-key, all-in-one solution customers want and need when it comes to cloud hosting. With its exclusive healthcare focus and in-depth security expertise, ClearDATA puts Sansoro Health’s customers at ease about healthcare managed services and compliance safeguards.
Sansoro Health’s customers receive several benefits in terms of cost savings and reduced time to market. A provider of scheduling software for hospitals and clinics could, for example, leverage Emissary to immediately make direct updates from the clinics’ scheduling information to the EHR, updating and creating new patients and new registration events. Emissary passes data from the scheduling application to the hospital EHR and back, all in a secure, HITRUST-certified environment provided by ClearDATA.

Sansoro Health and ClearDATA make life easier for health systems’ IT departments. It is not uncommon for many of these departments to have a nine to 18-month backlog of integration projects they have to complete. Sansoro Health can deliver a superior integration solution faster – often in a matter of weeks. The entire process is streamlined and efficient because the IT staff no longer has to set up and maintain another on-site server, freeing up their time to focus on other high-priority needs.

Since signing on with ClearDATA on AWS, Sansoro Health has had a seamless experience and superb support. “There have been no connectivity challenges and almost 100% uptime (99.9999%),” says Mike Pietig, Customer Success Officer and co-founder at Sansoro Health. “We’re seeing healthcare evolve and be more open to the benefits of the cloud, and ClearDATA is the answer. There is no doubt: we would not have closed a key account without the healthcare compliance solution ClearDATA brings to the table.”

**About CloudEndure**

ClearDATA is a healthcare exclusive, HITRUST certified AWS managed service provider. They also provide a compliance dashboard that is available through AWS Marketplace. This dashboard is mapped directly to HIPAA, GDPR, GxP, NIST, and ISO controls and guidelines.

### Summary

Sansoro Health and Health Quest showcase just a few of the many security use cases that AWS Marketplace software sellers can help solve for. Whether it be the ability to securely innovate, improve clinical outcomes, or maintain compliance, AWS Marketplace sellers are equipped to help you achieve your security goals.
Security teams are using AWS native services and solutions from independent software vendors and APN consulting partners that complement AWS solutions. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of independent software vendors, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more. These solutions can be integrated with AWS services and other existing technologies, facilitating HCLS organizations to defend against pervasive threats and strengthen their security posture in the cloud. These solutions can enable HCLS organizations to cost-effectively drive innovation, efficiency, and security in the cloud.

Below are a selection of software sellers in AWS Marketplace that offer security solutions for the HCLS industry:

Why buy in AWS Marketplace

AWS Marketplace is a digital catalog of software products offered by independent software vendors and APN consulting partners that complement AWS solutions. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of independent software vendors, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more. These solutions can be integrated with AWS services and other existing technologies, facilitating HCLS organizations to defend against pervasive threats and strengthen their security posture in the cloud. These solutions can enable HCLS organizations to cost-effectively drive innovation, efficiency, and security in the cloud.

Below are a selection of software sellers in AWS Marketplace that offer security solutions for the HCLS industry:

### Seller solutions further support your CSF activities

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ClearDATA Compliance Dashboard (C2) allows you to quickly validate your compliance posture and identify security risks and gaps so you can validate your compliance to an auditor.</td>
<td>Sophos Unified Threat Management (UTM), makes security easier to deploy and manage, providing essential next-gen firewall protection for network, web, email, applications, and users.</td>
<td>The VM-Series Next-Generation Firewall allows developers and cloud security architects to embed inline threat and data theft prevention into their application development workflows.</td>
<td>Trend Micro Deep Security provides a comprehensive suite of cloud security capabilities from a single agent, so healthcare organizations can secure patient data in less time and at lower cost.</td>
<td>NetApp Cloud Volumes ONTAP can be easily integrated with your AWS infrastructure to backup data from your on-premises and/or cloud environments to AWS storage targets.</td>
</tr>
</tbody>
</table>

To learn more about these and other seller solutions in AWS Marketplace that can enhance your security posture, click here.

### How to get started with security solutions in AWS Marketplace

Security teams are using AWS native services and solutions from independent software vendors in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security posture. The following steps can help you get started:

- **Speak with an AWS Solutions Architect for guidance on solutions aligned to your security priorities**
- **Explore more use cases and solutions for healthcare**

---