A SANS Whitepaper

How to Optimize Security Operations in the Cloud Through the Lens of the NIST Framework

Written by **John Pescatore**

February 2019

Sponsored by:

AWS Marketplace

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.[1] 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

[1] "IaaS Emerges as Fastest-growing Sector of the Global Public Cloud Market," ComputerWeekly, April 12, 2018, www.computerweekly.com/news/252438790/IaaS-emerges-as-fastest-growing-sector-of-the-global-public-cloud-market

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.

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.

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.

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.[2] 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.

Securing information always comes down to providing three basic security functions, the "CIA triad" of confidentiality, integrity and availability.

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.[3] 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.

---

[2] "Security Best Practices for IT Managers," June 2013, www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257

[3] "Security Assurance of Docker Containers," October 2016, www.sans.org/reading-room/whitepapers/assurance/security-assurance-docker-containers-37432

The NIST Cyber Security Framework

The NIST Cyber Security Framework (CSF) came out of the Cybersecurity Enhancement Act of 2014,[4] 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."[5] 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.

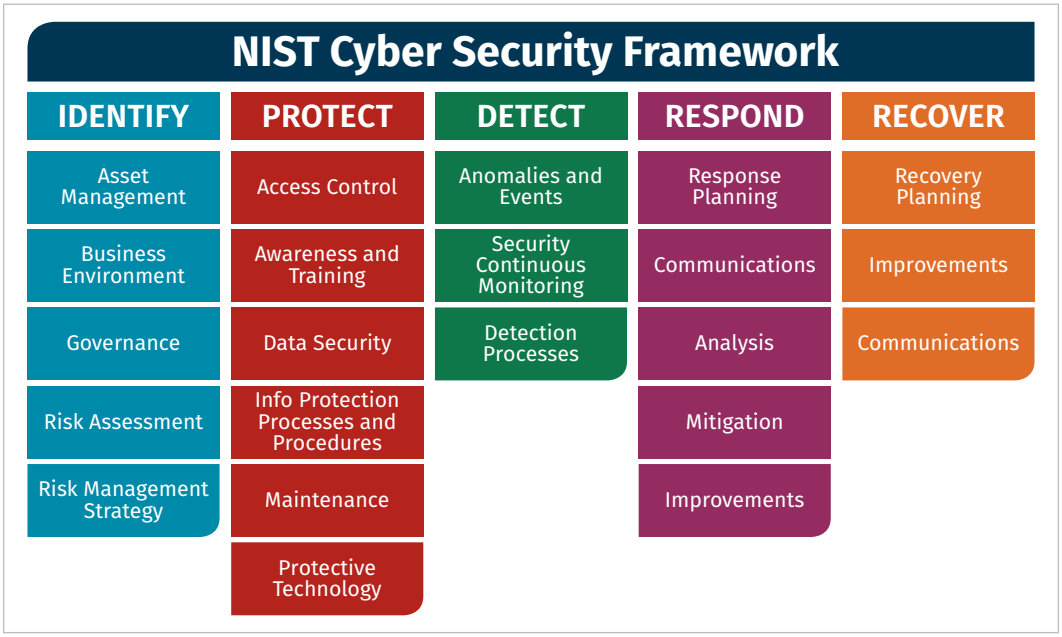


Figure 1. The NIST CSF[6]

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.

Why a Framework?

Regardless of the existing level of operations maturity, security teams face common needs:

- Adapting to changing business demands and evolving threats
- Obtaining management support for necessary resources and changes in IT or other areas
- Demonstrating improvement and providing risk assessment and forecasting
- Reducing the burden of satisfying auditors that security operations are compliant

A security framework, with its recommended set of security processes and controls, along with a risk assessment and management approach to match the appropriate set of controls to the business and threat environment, is an efficient way to meet these needs. Using an established framework can take the guesswork out of the process for smaller organizations, while allowing larger and more mature security operations to justify their decisions and resource requests to management and auditors.

[4] "National Institute of Standards and Technology, www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[5] Cybersecurity Enhancement Act of 2014, www.congress.gov/bill/113th-congress/senate-bill/1353/text

[6] "Introduction to the NIST CyberSecurity Framework for a Landscape of Cyber Menaces," Security Affairs, April 20, 2017, https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html

A more effective and efficient approach to selecting the most appropriate and effective security products and services to secure both data center and cloud-based systems is a scenario-based approach, which is covered in the next section.

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.

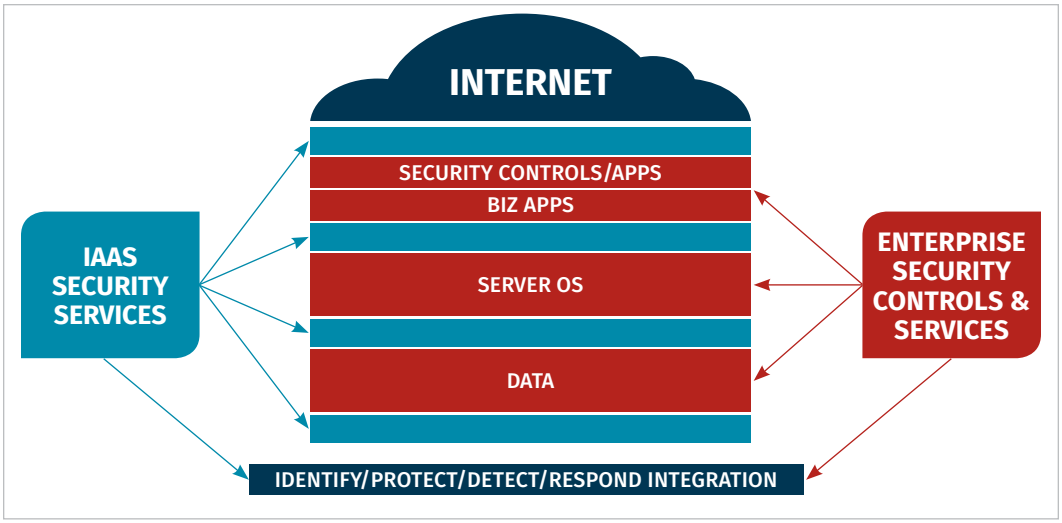


Figure 2. Integrated Services at Each Boundary Layer

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,[8] 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 1. Mapping Cloud Controls to the NIST CSF Framework

NIST CSF Functions		Primary Product Categories	
		Due Diligence	Advanced/Lean Forward
Proactive	Identify	Configuration management	AppSec testing
		System management	GRC
		Vulnerability assessment	Penetration testing
		Awareness training	
	Protect	Access management	Encryption
		Data masking	Intrusion prevention systems
		DDOS filtering	Secure image/container
		Endpoint protection	Strong authentication
		Firewall	Firewall policy management
		Ops skills training	
Reactive	Detect	Intrusion detection systems	Data analytics
		Network monitoring	Data loss prevention
		SIEM	
	Respond	Incident response services	Endpoint detect/respond
		Trouble ticket systems	Forensic analysis
	Recover	System/endpoint backup	High-avail/mirroring services

[8] Risk Management, NIST, https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

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.

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.

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

NIST CSF Functions		Primary Product Categories	
		Due Diligence	Advanced/Lean Forward
Proactive	Identify	AppSec testing	GRC
		Configuration management	Penetration testing
		System management	
		Vulnerability assessment	
	Protect	Access management	Encryption
		Data masking	Intrusion prevention systems
		Firewall	Secure image/container
		Ops skills training	Strong authentication
Reactive	Detect	Intrusion detection systems	
		SIEM	
	Respond	Incident response services	Endpoint detect/respond
		Trouble ticket systems	Forensic analysis
	Recover	System/endpoint backup	High-avail/mirroring services

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,[9] 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.

[9] CIS Benchmarks, Center for Internet Security, www.cisecurity.org/cis-benchmarks

- **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.

Table 3. Security Control Set for Business App Launched on/Moved to IaaS

NIST CSF Functions		Primary Product Categories	
		Due Diligence	Advanced/Lean Forward
Proactive	Identify	Awareness training	AppSec testing
		Configuration management	GRC
		System management	Penetration testing
		Vulnerability assessment	Cloud management platforms
	Protect	Access management	Encryption
		DDOS filtering	Intrusion prevention systems
		Endpoint protection	Secure image/container
		Firewall	Strong authentication
		Ops skills training	Firewall policy management
Reactive	Detect	Intrusion detection systems	Data analytics
		Network monitoring	Data loss prevention
		SIEM	
	Respond	Incident response services	Endpoint detect/respond
		Trouble ticket systems	Forensic analysis
	Recover	System/endpoint backup	High-avail/mirroring services

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:

- 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 4. Security Control Set for the Hybrid Cloud

NIST CSF Functions		Primary Product Categories	
		Due Diligence	**Advanced/Lean Forward**
Proactive	**Identify**	Configuration management	AppSec testing
		System management	GRC
		Vulnerability assessment	Penetration testing
		Awareness training	
	Protect	Access management	Encryption
		Data masking	Intrusion prevention systems
		DDOS filtering	Secure image/container
		Endpoint protection	Strong authentication
		Firewall	CASB
		Ops skills training	
Reactive	**Detect**	Intrusion detection systems	Data analytics
		Network monitoring	Data loss prevention
		SIEM	
	Respond	Incident response services	Endpoint detect/respond
		Trouble ticket systems	Forensic analysis
			Network policy management
	Recover	System/endpoint backup	High-avail/mirroring services

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.

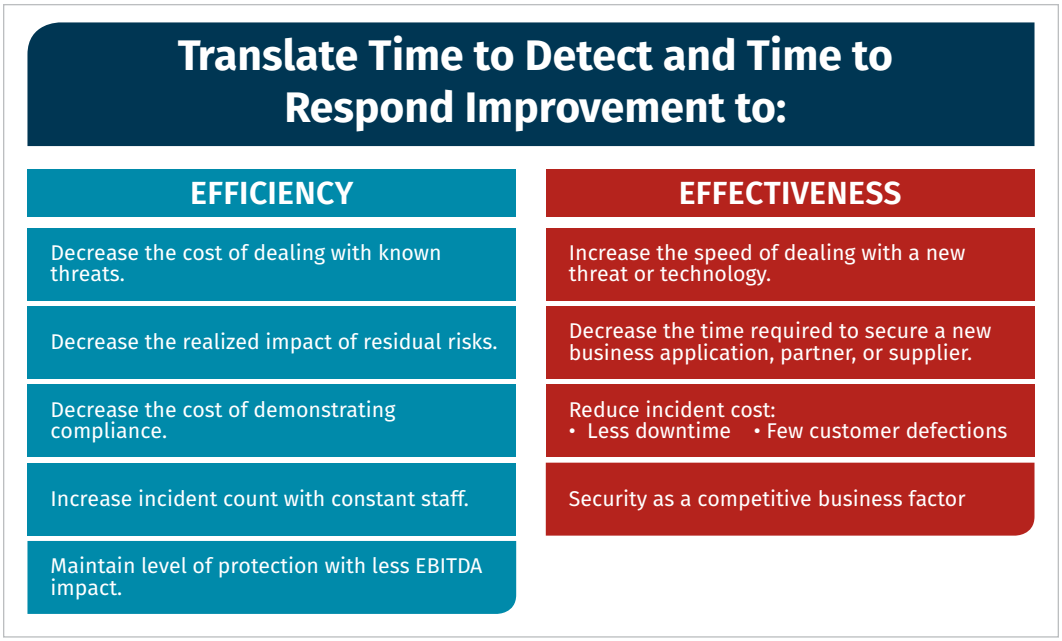


Figure 3. Connecting Metrics to Business Services

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.

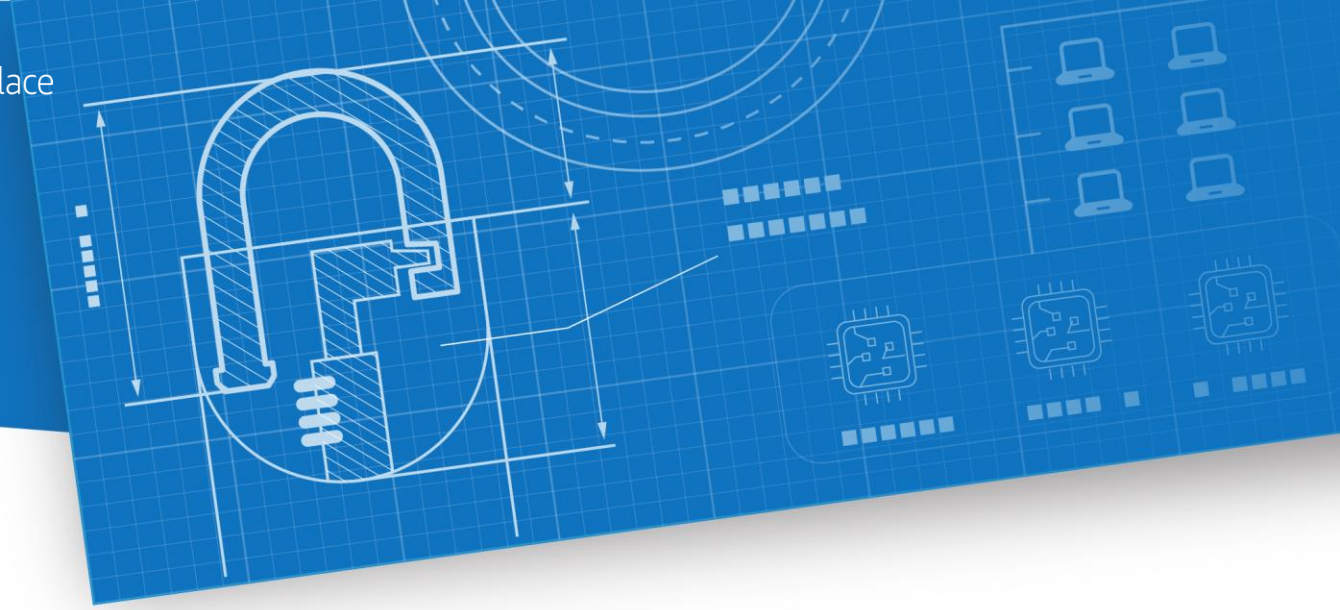
About the Author

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



Prioritizing Security Controls in the AWS Cloud

How organizations are enabling relevant security use cases in the cloud

Compliance frameworks and their controls do not have to be an afterthought when designing and implementing security solutions on Amazon Web Services (AWS). The first step in prioritizing your organization's security controls is understanding which AWS native services can most effectively be leveraged to achieve compliance and strengthen your overall security posture. AWS has developed guidance to help organizations of any size align with the NIST Cybersecurity Framework and build automated, innovative, and secure solutions by leveraging AWS services.

Secondly, organization's moving their workloads to the cloud will need to prioritize the controls that extend past the available AWS native services. In these cases, third-party solutions exist to address this concern via AWS Marketplace. AWS Marketplace, a digital software catalog where security practitioners can find, try, buy, deploy, and manage software that runs on AWS, offers third-party software solutions that can be integrated with AWS native services and other existing technologies. This can enable organizations to deploy a comprehensive security architecture across the AWS cloud and within traditional on-premise environments.

The following details a few of the security use cases that matter most in the cloud and how security teams are using third-party security solutions in AWS Marketplace to enable them. These use cases include:

1	**Automate Integrated Risk Management (IRM) (also known as Governance, Risk, and Compliance)** by defining and executing policies that align with organizational goals and ensuring that external and internal regulatory compliance standards are met.
2	**Ensure Security Visibility** through holistic awareness of resources across cloud environments and sufficient visibility into their use or possible abuse.
3	**Achieve Endpoint Security** through persistent malware detection, prevention, and remediation for advanced threats, policy violations, applications, and file-based malware.
4	**Safeguard Network Access** with firewalls and proxies that monitor network and application activity, actively block advanced threats, and prevent lateral movement.

1. Automate Integrated Risk Management (IRM)

Global payment services company, Western Union, saw accelerated productivity among its application developers with its move to AWS but also incurred greater challenges for its security engineers—who write and measure compliance rules—to ensure the growing number of applications are compliant. To help mitigate the challenges, Western Union turned to Dome9, a comprehensive software platform for public cloud security and compliance orchestration, which offers an out-of-the-box solution for automated security and compliance controls, as well as visibility into AWS and on-premises infrastructure.

Dome9 brings in the configuration and logs across multiple AWS accounts for actionable insights into Western Union's security posture. Dome9 also enables simpler compliance management through automation and alerting on high-risk changes, allowing Western Union to lock down and prevent un-approved AWS regions from being used, detect and block security group changes, and provide alerts on high-risk changes such as opening firewall port 22. Using Dome9, Western Union has achieved operational insights at scale—and freed up security teams to ensure compliant applications—as the organization grows with hundreds of assets on AWS.

Learn more about Dome9.

Tips from the Pros: Dome9

> At least once a week we have seen someone expose very sensitive data to the outside world. This is not surprising when you have hundreds of knobs to turn (essentially configurations and parameters that you need to set in your environment) in order to implement and maintain security posture. It's not a problem of not knowing what to do. It's just that when you have a lot of different things to configure, it's a problem of scale and it's easy to get something wrong when it's done manually. So, really what you need are automated tools that help you manage configurations, identify vulnerabilities, and tools that are able to set the right parameters and fix any misconfigurations before they become exposures or breaches.[i]

Other solutions in AWS Marketplace that can be used to automate Integrated Risk Management (IRM) include:

CloudSploit Hosted Scanner	CloudPassage Halo Cloud Secure	Telos Xacta 360
CloudSploit helps organizations that use AWS maintain a secure, compliant environment. CloudSploit securely connects to AWS accounts and uses AWS APIs to scan for security vulnerabilities and misconfigurations that put infrastructure at risk. With over 50 tests, each CloudSploit scan covers the breadth of AWS services, producing actionable results for DevOps, security, and management teams. CloudSploit scans in the background with no impact to hosted services and can be configured with alerts and third-party integrations, such as Slack, so risks are made apparent as soon as they are detected. Learn more here.	Halo Cloud Secure is an automated public cloud infrastructure security solution that delivers comprehensive visibility, protection, and continuous compliance monitoring for compute, storage, database, networking, and identity services. Organizations can use Halo Cloud Secure to automatically discover all of their public cloud assets in a unified view across accounts, services, and regions. Learn more here.	Xacta 360 operationalizes security risk and compliance frameworks such as the NIST Risk Management Framework (RMF), NIST Cybersecurity Framework (CSF), FedRAMP, and ISO 27001. Xacta 360 streamlines and automates many labor-intensive tasks associated with these frameworks such as asset inventory and automated report/document generation; identifies, tracks, tests, and helps remediate security risks for the system, program, or enterprise; and continuously monitors compliance with the appropriate standards. Learn more here.

2. Ensure Security Visibility

United States-based specialty outdoor retailer, REI, wanted to extend its security posture to include edge protection for its AWS virtual private clouds (VPCs) as it migrated applications to AWS. However, REI's technology organization lacked a solid investigation workflow for its on-premises and AWS deployments, with teams spending up to a week logging into different accounts and exporting and aggregating data with spreadsheets using various products and no formal process. REI conducted a proof-of-concept to centralize log management and edge protection services across teams, integrating AWS Shield and Amazon GuardDuty in conjunction with Splunk Cloud for fast insights.

Splunk, a cloud service for searching, monitoring, and analyzing machine-generated big data, aggregates data across Amazon VPC flow logs, AWS Application Load Balancer Logs, and Amazon GuardDuty logs for easy correlation, visualization, and alerting. This gave REI its biggest advantage in securing the edge in a repeatable way. REI also uses a variety of Amazon native services to meet its intrusion detection systems requirements for blocking common exploits. Using the Amazon GuardDuty Add-on for Splunk, REI's security team can filter through alerts for all accounts and get information in real time, providing additional context for early detection, rapid investigations, and remediation of potential threats. REI has integrated this solution into its DevSecOps practice, utilizing HashiCorp Terraform and Jenkins, to ensure the same standard is applied across all new accounts or VPCs. REI now has the real-time, end-to-end visibility to close security gaps as it continues moving applications to AWS.

Learn more about Splunk.

Tips from the Pros: Splunk

> You're getting plenty of [cybersecurity] alerts. But are you getting insights with those alerts? Do you have enough context to make a good decision? For example, for a misconfiguration alert, is it an honest mistake or an insider at work? How do you know what's actually happening? Not having quick and easy answers leads to "alert fatigue," and once you're "de-sensitized", you can end up making few good decisions—or worse—no decisions at all. At the core of the issue is the heterogeneous aspect of a multi-layered approach—different teams have different tools and perspectives, which means siloed tools and siloed opinions.
>
> So how can you get everyone speaking the same language? You can start with four easy examples of data that you probably already have today. The key is to get them into a single place first. This approach allows everyone to operate from a single source of truth—to see across the entire environment and verify alerts to determine whether there is an actual issue—and then, you'll be able to relate pieces of information with each other quickly and easily.
>
> – Jae Lee, Product Marketing Director, Security Markets, Splunk[ii]

Other solutions in AWS Marketplace that can be used to ensure security visibility include:

Sumo Logic Machine Data Analytics for Logs and Metrics	Cisco Stealthwatch Cloud | Public Cloud Monitoring	AlienVault Unified Security Management (USM)
The Sumo Logic service centralizes and unifies log data and time-series metrics and leverages machine learning analysis, such as pattern identification, outlier detection, and predictive trending, to quickly alert and troubleshoot app and infrastructure performance and security issues. Sumo Logic has already pre-built analytics and dashboard support for AWS services including Amazon EC2, Amazon S3, AWS CloudTrail, Amazon CloudFront, Elastic Load Balancing (ELB), Amazon VPC Flow Logs, AWS Config, and AWS Lambda. Learn more here.	Stealthwatch Cloud Public Cloud Monitoring is an AWS native security visibility service that consumes VPC flow logs, Amazon CloudTrail, IAM, and inspector log files to deliver low-noise alerts. Machine learning and modeling algorithms learn normal behavior for a resource or a user. When a behavior change that should be investigated is observed, the service generates an alert with various details. Learn more here.	AlienVault USM automates threat detection across cloud environments, cloud applications, and on-premises physical and virtual critical infrastructure for comprehensive security visibility. USM delivers multiple security technologies in one easy-to-use solution, including asset discovery, vulnerability assessment, intrusion detection, SIEM, log management, and behavioral monitoring. USM also eases compliance and forensics requirements with secure long-term cloud log storage, meeting PCI DSS, HIPAA, and SOC 2 standards. Learn more here.

3. Achieve Endpoint Security

Pokémon Company International is responsible for the brand management, licensing, and marketing of Pokémon products to a global audience numbering in the hundreds of millions. In 2017, the company expanded its online business, due in part to the success of its PokémonGo mobile game. Detecting security vulnerabilities and protecting its environment is paramount to Pokémon building and maintaining the trust of its users, which are mainly children and parents. And like countless other organizations, Pokémon utilizes DevOps to move fast—but this introduces the risk of DevOps engineers not deploying all the correct solutions. Pokémon partnered with CrowdStrike, a cloud-based endpoint protection service, to gain visibility and establish baselines for its AWS compute platform.

CrowdStrike's Falcon Discover can identify Amazon EC2 instances that do not have the agent installed, which helps when Pokémon is rapidly scaling infrastructure. CrowdStrike also provides additional insights into each Amazon EC2 instance once the CrowdStrike agent is installed. This reduces the time in detecting and responding to a security event by allowing Pokémon's analysts to seamlessly pivot between on-premises and AWS without having to switch products, providing a single pane of glass across the entire enterprise and enabling Pokémon to ensure global availability while protecting a growing number of customers worldwide.

Learn more about CrowdStrike.

Tips from the Pros: CrowdStrike

4 key considerations for choosing the right EDR solution from Con Mallon, Sr. Director of Product Marketing, CrowdStrike[iii]

1. **Endpoint Detection & Response is a journey:** Organizations need to assess their internal resources, their expertise, and the types of threats they are facing to determine a level of EDR implementation that will best suit their needs.
2. **Look closely at the level of automation provided:** The level of automation regarding detection and remediation is crucial as well as having a seamless handoff between the security operations center and security teams.
3. **Look for strong behavioral detection and blocking capabilities:** One of the biggest mistake's organizations make is to focus too much on detection and failing to understand that if they can detect, they can also block.
4. **EDR enables hunting – and that's a very good dynamic:** Organizations need to assess their internal resources and expertise but having a solution that includes managed hunting can enable them to add this capability without burdening their internal staff.

Other solutions in AWS Marketplace that can be used to achieve endpoint security include:

Trend Micro Deep Security	Symantec Cloud Workload Protection	McAfee Cloud Workload Security
Deep Security's SaaS solution defends networks against attacks with intrusion detection and prevention, hardens servers, and speeds patching and response to zero-day issues like Shellshock and Heartbleed. Deep Security also protects Windows and Linux workloads from malware, monitors unplanned or suspicious changes to systems, and stops SQL injection and XSS attacks on applications. Learn more here.	Cloud Workload Protection (CWP) discovers, visualizes, and protects all of an organization's Amazon EC2 instances with anti-malware, intrusion detection and prevention (IDS/IPS), and real-time file integrity monitoring (FIM) in a single agent. CWP also delivers cloud-native security to protect and monitor workloads including Docker containers, preventing unauthorized changes and elevated privileges to system resources. Organizations can automate security by integrating with DevOps tools like Splunk, Chef, and Puppet via CWP's RESTful APIs. Learn more here.	Cloud Workload Security discovers Amazon EC2 instances across all VPCs, and deploys protection designed for an elastic cloud environment to safeguard against advanced malware, remote exploits, and data theft. Cloud Workload Security detects and imports virtual instances, security groups, and virtual networks to the McAfee ePO server. The solution also discovers, assesses, and remediates docker containers running on a Kubernetes cluster, and secures them using network segmentation. Learn more here.

4. Safeguard Network Access

Canadian non-profit automotive membership organization, the Alberta Motor Association, wanted to ensure that their AWS-hosted applications were protected against attacks by using behavioral analytics, proactive bot defense, and application-layer encryption of sensitive data. Like many organizations, the Alberta Motor Association has a combination of on-premises and AWS cloud infrastructure and had moved to AWS in order to increase deployment speed while also decreasing time to market and increasing efficiency. Already using F5 Networks' firewall technology on-premises, the Alberta Motor Association realized it could leverage F5 Web Application Firewall (WAF) to provide similar protection in the cloud.

Deploying F5 WAF in AWS Marketplace allows organizations to start with a pre-configured F5 Amazon Machine Image (AMI). This AMI is ready to be deployed via AWS CloudFormation templates, which are available in GitHub, directly into an AWS account in minutes and in a highly available manner. This AMI also incorporates best practices for such a deployment as defined by AWS Partner and F5 Solutions Architects, meaning organizations can have confidence knowing they have implemented best practices and fine tuning. Furthermore, since F5 WAF provides the same features as its on-premises equivalent, security teams can get up and running quickly with the same level of protection as their on-premises firewall.

In the case of the Alberta Motor Association, implementing F5 WAF enabled them to bolster protection against web attacks, improve traffic visibility, and easily integrate into its application development lifecycle to simplify migrations as the company moves additional workloads to AWS.

Learn more about F5 Networks.

Tips from the Pros: F5 Networks

Web application firewalls (WAFs) are an integral component of application protection. In addition to being a requirement for complying with PCI-DSS, WAFs are excellent at protecting against the OWASP Top 10. They're also a go-to solution for addressing zero-day vulnerabilities either through rapid release of signature updates or, in some cases, the use of programmatic functions to virtually patch applications while a long-term solution is being deployed. The question is, where do you put such protection?

The data path contains multiple insertion points at which a WAF can be deployed. But that doesn't mean every insertion point is a good idea. Some are less efficient than others, some introduce unacceptable points of failure, and others introduce architectural debt that incurs heavy interest penalties over time. Ideally, you'll deploy a WAF behind your load balancing tier. This optimizes for utilization, performance, and reliability while providing the protection necessary for all apps – but particularly for those exposed on the Internet… With the right tools, comprehensive WAF coverage can significantly reduce your exposures, as well as your operating costs."

– Lori MacVittie, Principal Technical Evangelist, F5 Networks[iv]

Other solutions in AWS Marketplace that can be used to prevent unauthorized access to networks include:

Palo Alto Networks VM-Series Next-Generation Firewall	Barracuda Networks CloudGen WAF	Fortinet FortiGate Next-Generation Firewall
Cloud security architects and developers can use native AWS automation features and workload tags combined with a VM-Series bootstrapped configuration stored in an Amazon S3 bucket to create "touchless" deployments. App whitelisting and segmentation policies can be dynamically updated based on AWS tags, allowing organizations to reduce the attack surface area and achieve compliance while threat prevention policies can stop both known and unknown attacks. Advanced architecture designs include support for a Transit VPC as well as full integration with AWS Auto Scaling and Elastic Load Balancing. Learn more here.	CloudGen WAF detects all inbound web traffic and blocks SQL injections, cross-site scripting, malware uploads, volumetric and application DDoS, and other attacks against your web applications. It also inspects HTTP responses from the configured back-end servers for data loss prevention. The integrated access control engine enables admins to create granular access control policies for Authentication, Authorization, and Accounting (AAA) for strong authentication and user control. Onboard L4/L7 load balancing capabilities enable organizations to quickly add back-end servers to scale deployments as they grow. Learn more here.	FortiGate protects networks and content by combining stateful inspection with a comprehensive suite of powerful security features to meet PCI DSS compliance. IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection which alerts users to any traffic that matches attack behavior profiles. Learn more here.

What is AWS Marketplace?

AWS Marketplace is a digital software catalog where security practitioners can find, try, buy, deploy, and manage software that runs on AWS. AWS Marketplace simplifies software licensing and procurement by offering more than 4,200 products from over 1,280 sellers in software categories like Security, Networking, Storage, Business Intelligence, Machine Learning, Database, and DevOps. Organizations can leverage offerings from independent security software vendors in AWS Marketplace to secure applications, data, storage, networking, and more on AWS and enable operational intelligence across their entire environment.

Customers can use 1-Click deployment to quickly launch pre-configured software and choose software solutions in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with software entitlement options such as hourly, monthly, annual, and multi-year.

AWS Marketplace is supported by a global team of security practitioners, solution architects, product specialists, and other experts to help security teams connect with the software and resources needed to prioritize security operations in AWS.

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:

1. Speak with an AWS Solutions Architect for guidance on solutions aligned to your security priorities
2. Learn how to get started, browse free trials, and subscribe to products in AWS Marketplace

---

[i] "AWS Security and Networking: Configuration and Vulnerability Analysis", https://pages.awscloud.com/rs/112-TZM-766/images/AWSMP-SecNet-Configuration-Vulnerability-Analysis.pdf

[ii] Jae Lee, "Central Logging: The first Step to Improving Security Visibility", https://www.splunk.com/blog/2017/11/13/central-logging-the-first-step-to-improving-security-visibility.html

[iii] Con Mallon, "The Maturing of Endpoint Detection and Response (EDR): Choosing the Right Solution", https://www.crowdstrike.com/resources/crowdcasts/the-maturing-of-endpoint-detection-and-response-edr-choosing-the-right-solution/

[iv] Lori MacVittie, "Where does a WAF fit in the data path?", https://www.f5.com/company/blog/where-does-a-waf-fit-in-the-data-path