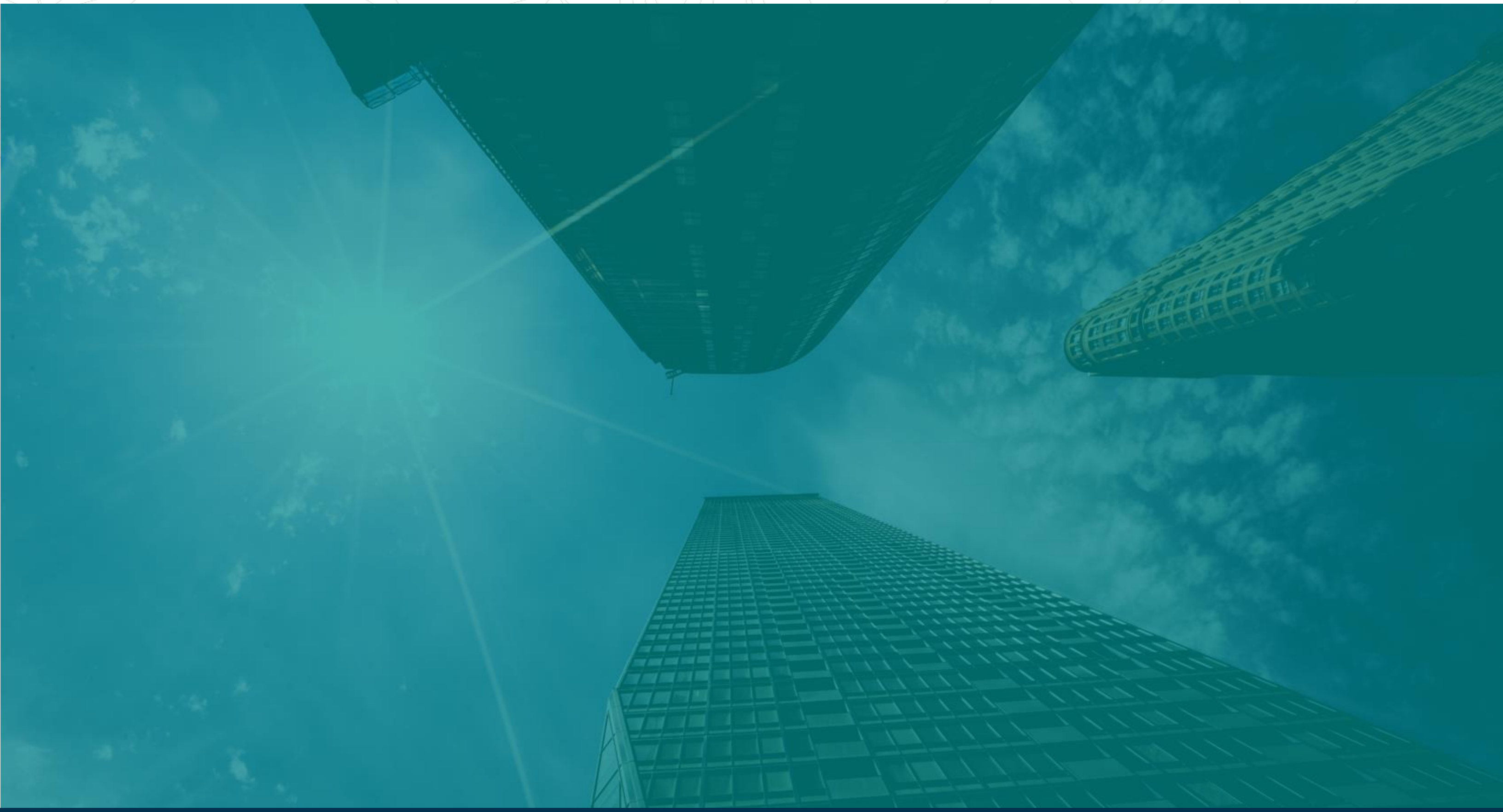
WHITE PAPER

KUDELSKI SECURITY

Cloud Security Reference Architecture

Reference Architecture Series



Info@kudelskisecurity.com | www.kudelskisecurity.com

Cloud Security Reference Architecture

Reference Architecture Series

June 2019

Executive Summary

Large enterprises are embracing public cloud services for a variety of reasons ranging from competitive positioning to improved operational efficiencies. Cloud services reduce the need for large capital investments in IT infrastructure, creating agility that allows businesses to continually and quickly adapt and scale their technology needs to their business needs.

While providing opportunities for business improvement, innovation and disruption, the erosion of the network perimeter to cloud platforms and SaaS applications creates a major cybersecurity threat vector for organizations today. As a result, cloud security and next generation IT network security are top of mind topics for CISOs and CIOs alike.

Security controls have shifted from being on-premise and mostly tangible in nature, to being software-based, built specifically for cloud environments. Security strategies and programs in these new hybrid environments need to be reimagined and designed to meet these new challenges to reduce the risk of exposure.

CISOs must also consider the need for elevated trust, as security responsibilities are no longer shouldered solely by the organization itself but are shared with third-party cloud service vendors as well. They need to assess the potential and relevance of the new security cloud security service offerings that have mushroomed over the last five years. These services provide additional capabilities to securely monitor, manage, and optimize cloud environments at the speed of business and so are of interest to every agile-minded CISO.

But how to make sense of this new paradigm?

This Cloud Security Reference Architecture maps out key challenges, industry-leading technologies, and frameworks, such as NIST. It provides clear and impartial guidance for security leaders seeking to secure their cloud environments – whatever stage they're at on their journey.

Table of Contents

Cloud Threats, Impacts, and Challenges

Accelerated adoption of public and private cloud applications, platforms, and services creates a major cybersecurity threat vector for organizations. More and more, attackers are opting to use cloud services instead of building custom attack infrastructure to launch attacks or exfiltrate data.[1]

On average, most cybersecurity attacks do not target cloud infrastructure, but rather operating system and application vulnerabilities. Gartner estimates that customers will be responsible for causing 95 percent of cloud security failures through the year 2020.[2] At cloud scale, these security issues are amplified.

Organizations are challenged to transition legacy systems (and legacy IT management or security practices) to new cloud paradigms, often inadvertently and unknowingly creating security risks in the process.

Adding to the security risk is confusion about similar resource types across multiple clouds. The table below is an example of the resource nomenclature across the 3 major cloud service providers:

Service	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Resource Grouping	Organization Account	Enterprise Subscription	Organization Project
Virtual Network	Virtual Private Cloud (VPC)	Virtual Network (VNet)	Virtual Private Cloud (VPC)
Compute Instance	Elastic Compute Engine (EC2)	Virtual Machine	Compute Engine
Load Balancing	Classic, Network, or Application Load Balancer	Load Balancer Application Gateway	Cloud Load Balancing
Domain Name System (DNS)	Route 53	Azure DNS Traffic Manager	Google Domains Cloud DNS
Object Storage	Simple Storage Service (S3) Bucket	Block Blob	Cloud Storage Bucket
Databases •Relational •Warehouse •No-SQL	•Relational Database Service (RDS) •Redshift •DynamoDB	•SQL Database •SQL Data Warehouse •Cosmos	•Cloud SQL •BigQuery •Cloud Bigtable

[1] Internet Security Threat Report, Symantec (April 2017), p. 74, https://www.symantec.com/security-center/threat-report

[2] http://www.gartner.com/newsroom/id/3143718

For example, several recent large-scale data breaches were the result of simple customer misconfigurations in AWS Simple Storage Service (S3) that exposed the personal information for millions of users.[3] Digital media publisher Cultura Colectiva exposed 146 gigabytes of data, containing 540 million Facebook records, through an unprotected S3 bucket[4]

The Ladders, a job search site, recently exposed 13 million user profiles when they failed to password protect an Elasticsearch database.[5] Similarly, 24.3 million CitiFinancial mortgage and credit reports were exposed due to a publicly accessible Elasticsearch.[6]

Code Spaces, a source code hosting provider, was forced out of business after hackers compromised their AWS credentials and deleted customer data that had not been backed up.[7] Ransomware can now spread exponentially using the sync and share capabilities of SaaS-based storage applications.[8]

Reported outages at AWS and Microsoft Azure as well as the Mirai botnet attack against Dyn DNS in October 2016 illustrate the critical role that public cloud platforms play and highlight the interconnected dependencies that they create.[9]

Using the Cloud Security Reference Architecture to Reduce and Manage Risk

This Cloud Security Reference Architecture consists of a two-phase methodology. The first phase identifies security controls and initiatives that are relevant to cloud environments based on the widely recognized and implemented National Institute of Standards and Technology

[3] See, for example, http://www.techrepublic.com/article/massive-amazon-s3-breaches-highlight-blind-spots-in-enterprise-race-to-the-cloud

[4] https://www.securityweek.com/aws-s3-buckets-exposed-millions-facebook-records

[5] https://techcrunch.com/2019/05/01/ladders-resume-leak/

[6] https://www.scmagazine.com/home/security-news/data-breach/24-million-credit-and-mortgage-records-exposed-on-elasticsearch-database/

[7] https://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan

[8] https://www.netskope.com/blog/the-cloud-malware-attack-fan-out-effect

[9] http://windowsitpro.com/security/how-defend-against-ddos-attacks-one-dyn-dns-service

Cybersecurity Framework (NIST CSF). The second phase provides recommendations for using market-leading cloud technologies to meet the NIST CSF standards and which work in concert with the native security services from leading IaaS, and SaaS providers.

It is easy to become overwhelmed by the quantity and variety of native and third-party cloud security offerings in the increasingly crowded market.

Kudelski Security has years of real-world experience evaluating, deploying, integrating, and managing technologies in on-premises, hybrid and cloud environments. That real-world expertise has been compiled into this Kudelski Security Cloud Security Reference Architecture – a set of best practices and recommended technologies to help clients reduce and manage risk in cloud environments.

The Cloud Security Reference Architecture takes a clean-sheet approach that presupposes no existing cloud security or management technologies. Recognizing that most organizations do not start with a blank slate, alternative technologies to the ones we have highlighted may make more sense based on current IT investments, business needs, regulatory considerations, etc. Organizations can also compare their current risk management activities and technology solutions to identify gaps in their existing cloud protection.

Implementing Best Practices with Kudelski Security's Cloud Services

Kudelski Security assists clients with understanding and addressing their cloud security challenges across these security functions:

- Identifying and addressing flaws in existing multi or hybrid cloud environments with a cloud security assessment.
- Developing a cloud security architecture that integrates seamlessly into hybrid and multi-cloud environments.
- Developing a cloud security roadmap to help bridge the gap between today and the future.
- Automating and orchestrating security operations and incident response.

Kudelski Security also enables clients to efficiently and effectively consume cloud security through Managed Security Services offerings from our Cyber Fusion Center, including:

- Threat Monitoring & Hunting, which extends visibility into public cloud platforms and applications
- Cloud Configuration Inspection to identify cloud platform and application configuration issues
- Endpoint Detection & Response that collects, enriches, correlates and analyzes security relevant information from endpoints, both on-premises and in the cloud

Documenting Governance in the Cloud

Organizations with underpinning cloud technologies should have governance policies incorporating their unique challenges and considerations that need to be specifically considered and addressed. For organizations with regulatory standards, compliance requirements can certainly impact cloud strategy, design, and operations. Although this paper does not address governance documentation for the cloud, Kudelski Security's Advisory Services practice can help organizations define and document the requisite policies and procedures to support cloud environments.

The Shift to Shared Security Responsibilities

With cloud computing comes the shared responsibility for security controls between the cloud service vendor and the customer organization. There are three primary types of cloud delivery models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Each type not only carries its own features and benefits, but also a certain level of security. Note that we limit our discussion in this Reference Architecture to IaaS and SaaS. PaaS security leverages many of the same cloud security capabilities discussed herein, often coupled with additional PaaS-specific controls and configuration best practices for each service.

Infrastructure-as-a-Service (IaaS)

IaaS vendors provide the computing infrastructure – both hardware and software – needed for organizations to host their environments in the cloud, often leveraging microservices and container-based deployments. Access to the infrastructure may be through a GUI-based or programmatic interface (e.g. REST API).

For IaaS, the cloud service provider is responsible for security *of* the cloud infrastructure (e.g. compute, storage, networking), while the customer maintains responsibility for security *in* the cloud (e.g. data encryption, OS hardening, application security). This cloud service model requires the highest amount of security controls to be managed by the customer organization, including Data Governance, Endpoints, Access Management, Identity Management, Data Protection, Application Development, and Operating System Management.

Examples of major IaaS providers include Amazon Web Services, Google Cloud Platform, Microsoft Azure, Rackspace, and IBM.

Software-as-a-Service (SaaS)

SaaS is the most commonly known and used cloud computing model in which vendors provide the computing infrastructure as well as the software application. Access to the solution is typically through a web portal and API.

For SaaS platforms, the cloud service provider assumes more of the responsibility for operating system and application security, leaving the customer responsible for data protection and, to some degree, identity and access management.

Examples of major providers include Office365, Salesforce, and Zoom.

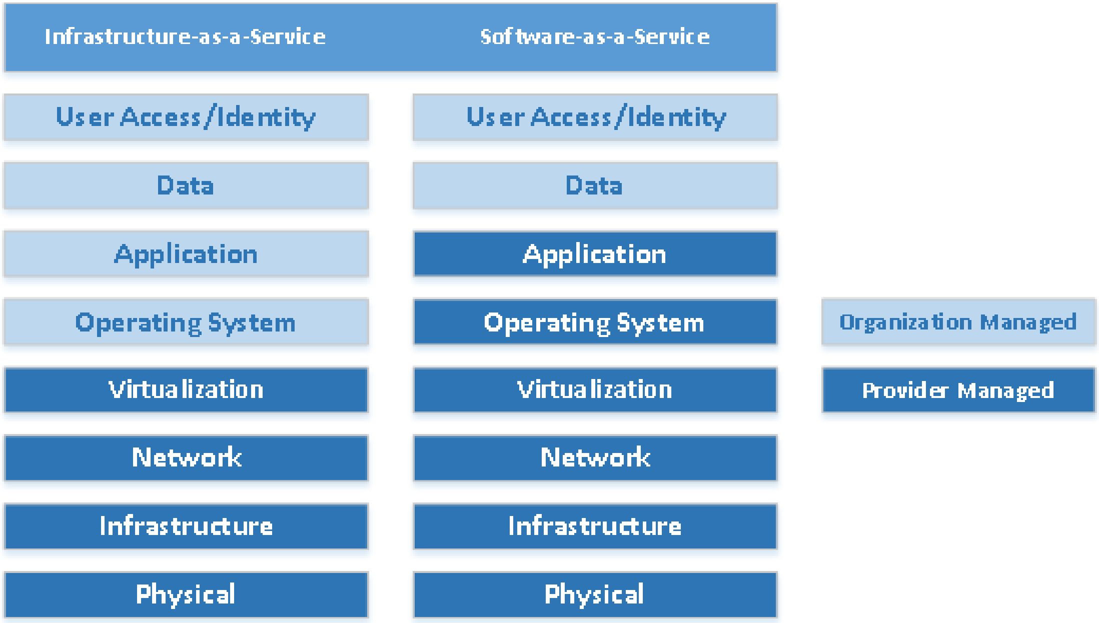
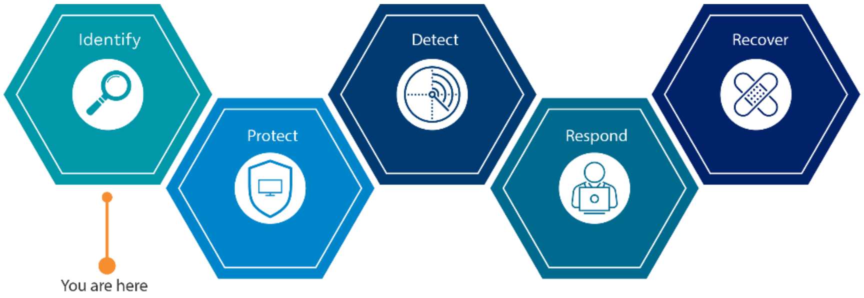


Figure 1: Cloud Security Shared Responsibility Model for IaaS and SaaS

With all cloud computing environments, organizations must clearly understand what their security responsibilities are and not incorrectly assume these activities are being performed by the cloud platform or application provider.

However, organizations can leverage the security foundation, and, in many cases, cloud-native security tools offered by the providers in securing operating systems, applications, network, and data.

NIST CSF Mapping and Recommendations



Identify

Asset Management

NIST CSF Function Alignment

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Overview

Rather than outright denial of new cloud-based apps, organizations are now under pressure to embrace cloud offerings and integrate them as sanctioned business tools to help employees get their jobs done more easily. Organizations seek continuous visibility into IaaS platforms and SaaS applications used throughout their business, including cloud services, data, and users. A comprehensive understanding of cloud utilization is a precursor to adequate technical and policy controls.

> At the end of 2016, the average enterprise organization was using 928 cloud apps, up from 841 earlier in the year. However, most CIOs think their organizations only use around 30 or 40 cloud apps.
>
> *Symantec Internet Security Threat Report (2017)*

Key Best Practices

Catalog External Information Systems

Cloud applications are designed to offer anywhere access from a variety of device and applications, from mobile phones to traditional "thick" productivity applications installed on endpoints. The relative ease with which employees can procure and use unsanctioned cloud applications – so-called Shadow IT – is a major IT headache. Identifying which cloud services are being used in an organization, by whom, and from what devices, is a tedious and incomplete process when using traditional perimeter-based network devices. As a result, cloud utilization can be a major blind spot.

Map Organizational Communication and Data Flows

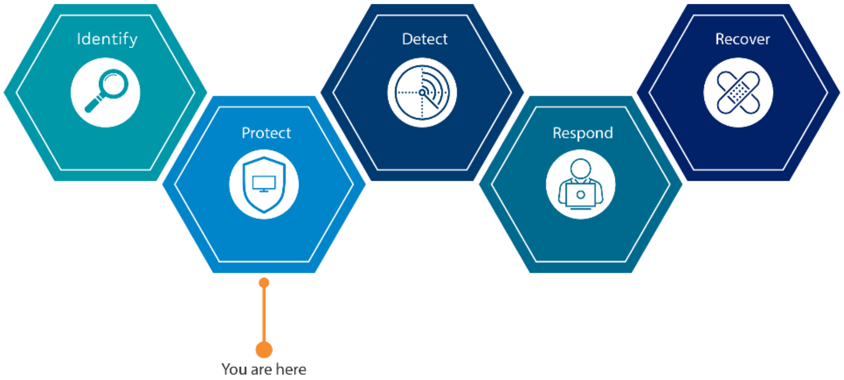
Knowing which cloud applications are being used is necessary, but not sufficient. Organizations must also understand *how* employees are using these IaaS and SaaS solutions. For example, a cloud storage application may be sanctioned if used with enterprise credentials, but unsanctioned if used with personal credentials for data upload. Understanding cloud activities at this contextual level requires an understanding of various cloud application programming interface (API)[10] interactions among cloud services and container-based architectures. For example, APIs from IaaS providers can provide detailed data about usage within those platforms.

Prioritize Resources Based on Criticality and Business Value

Once an organization discovers all of the cloud services being used, they can begin to rationalize cloud usage, reduce information silos, mitigate risk, and save cost by reducing redundant instances of the same cloud service. It is important to determine the relative value and enterprise-readiness for these applications and platforms, comparing the security attributes, cost, and usage metrics of cloud services.

For technology recommendations relating to *Identify* see Appendix 2

[10] https://moderncLiso.com/2017/04/25/api-security-awareness-in-a-cloud-connected-world



Protect

Identity and Access Management (IAM)

NIST CSF Function Alignment

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Overview

Over 80% of hacking-related breaches involve weak or stolen passwords.

Verizon Data Breach Investigations Report (2017)

IAM ensures that only authenticated and authorized users (human and non-human) are able to access resources, and only in the intended manner. The rise of different types of accounts and identities from public cloud services, including API token management, has increased the complexity of IAM and can result in fractured user authentication and authorization across cloud resources.

Key Best Practices

Manage Identities and Credentials for Authorized Users and Devices

Recent research by McAfee indicated that only 26% of organizations are using IAM to address Shadow IT.[11] Identity management in the cloud presents unique challenges because traditional on-premises systems

[11] Building Trust in a Cloudy Sky, McAfee (2017), p. 21

https://www.mcafee.com/us/solutions/lp/cloud-security-report.html such as Active Directory were not designed to be Internet-facing. Furthermore, logging into multiple applications can be time-consuming and frustrating.

Coupling a cloud centric IAM solution with multi-factor authentication helps protect credentials attacks and streamlines the authentication and authorization process for the variety of cloud solutions in use across the organization. Similarly, service-to-service network communication should be authenticated and authorized, using scalable IAM solutions that support microservices and container-based architectures.

Manage Access Permissions, Incorporating Least Privilege and Separation of Duties

Understanding who has access to what data in the cloud is difficult if the organization has limited or no visibility into cloud applications. Architecting and implementing fine-grained access control across cloud services, based on the principle of least privilege, limits the impact of lost, stolen, or inappropriately used credentials. However, with a variety of disparate applications and platforms, this type of control can be tedious to implement without centralized access management.

Network Integrity

NIST CSF Function Alignment

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Overview

The abstracted networking constructs of the cloud may require organizations to adapt their approach to cloud network architecture and include security measures to protect Cloud Public Services. In order to protect cloud services which cannot necessarily be segmented like legacy on-premise environments, organizations must clearly define their network infrastructure with considerations for what and how traffic gets in and out of the cloud and how internal workloads communicate.

Key Best Practices

Protect Network Integrity, Incorporating Network Segmentation Where Appropriate

Organizations that are migrating services to the cloud have existing application delivery controllers, web application firewalls, and DDoS protection that are critical components of their on-premises deployments, and they may desire to keep these solutions consistent across environments. Leading providers have public, private, and hybrid cloud offerings that enable customers to maintain this investment in technology and in-house expertise and allow them to leverage the advanced traffic management and security features that may not be currently available in the native cloud solutions.

Granular control over this east-west network traffic flow can detect and prevent lateral movement. Instance and container-level segmentation enables more flexible and precise network security policies but must be manageable at scale in a dynamic environment.

Baseline Configurations

NIST CSF Function Alignment

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Overview

As with on-premises assets, one of the most important steps an organization can take toward securing its cloud servers is to ensure that their operating systems and applications are patched and properly hardened against attack. Maintaining attack-resistant configurations across the cloud stack makes it much more difficult for intruders to gain a foothold in the systems.

> Cloud is attractive to attackers as, depending on how it is used and configured, it allows them to bypass local security…
>
> *Symantec Internet Security Threat Report*

Key Best Practices

Create and Maintain a Baseline Configuration of Information Technology

Security configuration tools for public cloud IaaS platforms check configuration settings and policies of the platform (e.g. account settings, storage ACLs, firewall rules) based on vendor and industry best practices. Cloud platform providers may offer native tools for basic configuration checking (e.g. AWS Trusted Advisor). There are also several open source projects (e.g. Netflix Security Monkey) and commercial offerings (e.g. Netskope for IaaS), which support multiple cloud platforms, including AWS and Google Cloud Platform. Standardized configuration baselines for container-based environments are also important to ensure consistency and provide security "guardrails" across these very dynamic environments.

SaaS tools also have security configuration settings that are unique to each solution. In some cases, the SaaS provider provides native tools to assist with secure configuration;[12] though these are certainly not universal.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Data Protection

NIST CSF Function Alignment

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Overview

Organizations can tailor and apply their existing data classification policies to data in the cloud – understanding what data types are available, where the data is located, and what access levels and protection of the data have. Based on these business rules and commensurate with the sensitivity level of the data and compliance requirements, organizations can apply

74% of organizations reported storing some or all of their sensitive data in public clouds.

McAfee, Building Trust in a Cloudy Sky (2017)

[12] *See, for example* https://support.office.com/en-us/article/Introducing-the-Office-365-Secure-Score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef

appropriate data protections (including encryption) in order to secure data at rest or in transit.

Protect Data-at-Rest

Protecting data-at-rest in the cloud is a multi-faceted consideration since data is stored in any number of forms, including block storage, object storage, databases, etc. Major IaaS providers provide key management services to enable cryptographic protection and management for data stored in the various mediums they offer. In most instances, organizations may also use a dedicated or third-party key management platform for higher assurance.

Protect Data-in-Transit

As indicated in the recent McAfee report on cloud security, protecting sensitive data as it moves into and out of SaaS cloud platforms is a primary concern for organizations.[13] Encrypting data as it is transmitted from one system to another, within or outside of the cloud platform, ensures the confidentiality and integrity of the data. Major IaaS and SaaS providers protect data in transit between datacenters and also enable organizations to use Transport Layer Security. For API calls, it is important to use HTTPS endpoints for communication, expected for most of today's browser-based traffic. VPN connectivity between cloud platforms and on-premises datacenters can be enabled with VPN solutions that organizations already use, including leading vendors such as Palo Alto Networks, Fortinet, and Juniper, coupled with various public and private connectivity options with major cloud services providers.

Protect Against Data Leaks

According to Symantec, "25 percent of all shadow data (business data stored in the cloud without IT's consent) is "broadly shared," meaning it is shared internally, externally, and/or with the public."[14] Three percent of that data contained compliance-related data (PII, PCI, PHI). However, according to McAfee, only 24% of organizations are using DLP and encryption technologies to address the issue.[15]

[13] Building Trust in a Cloudy Sky, McAfee, p. 18

[14] Symantec Internet Security Threat Report, p. 73

[15] Building Trust in a Cloudy Sky, McAfee, p. 21

A DLP solution must be able to understand cloud services at a very granular level, distinguish between sanctioned and unsanctioned cloud services accurately and efficiently, and consider the context surrounding cloud access such as the user, the device, the location, the activity, and the content.

Data Backups

NIST CSF Function Alignment

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Overview

Although IaaS platforms may be designed for multiple 9s of infrastructure availability, organizations remain responsible for the availability of the systems and data they host there. Native backup, replication, and recovery features of IaaS platforms enable organizations to protect their systems and data, often enabling data backups in different fault domains. However, these capabilities are not application-aware and do not necessarily protect against accidental or malicious data loss. Therefore, organizations should ensure that their cloud architecture and data protection strategies align to the business's reliability and retention requirements.[16]

Key Best Practices

Conduct, Maintain, and Periodically Test Backups of Information

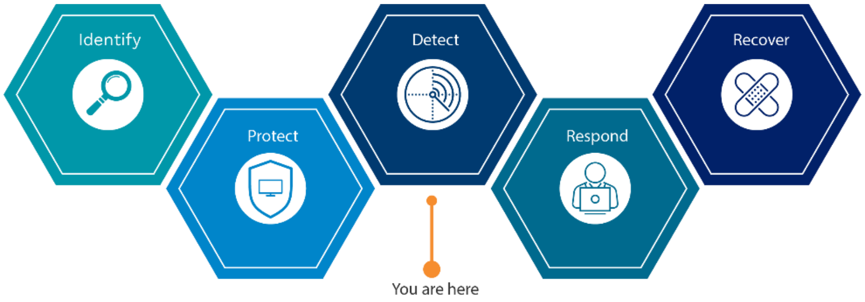
Although SaaS application providers are responsible for the availability of data under the shared responsibility model, data loss is usually the result of accidental deletion, not catastrophic loss at the platform level. For example, by default, user-deleted emails in Office 365 may only be retained for up to 14 days before being permanently deleted from the platform.[17] Organizations may have business or compliance requirements

[16] *See, for example* https://d0.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf

[17] *See* https://support.office.com/en-us/article/Overview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#how

that dictate longer retention periods. Therefore, organizations should consider SaaS retention policies and backup options in their business continuity and disaster recovery planning.

For technology recommendations relating to *Protect* see Appendix 2



Detect

Vulnerability Management

NIST CSF Function Alignment

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Overview

Vulnerability identification in cloud workloads can be a tedious process when done using traditional scanning tools that were not designed for dynamic cloud workloads and do not have full visibility inside the cloud environments.

> Visibility into cloud infrastructure security is one of the top three biggest headaches for IT security professionals.
>
> *ISC^2 Cloud Security Spotlight Report (2016)*

Key Best Practices

Identify, Document, and Mitigate Asset Vulnerabilities

Major cloud service providers have ongoing vulnerability identification and remediation programs in place for the portion of the cloud stack they are responsible for. In IaaS environments, the customer maintains much of the vulnerability scanning and remediation responsibility that they have from on-premises environments. For container-based architectures, ensuring the integrity of container images and only allowing approved and scanned images to be deployed limits the exposure created from unpatched software.

Logging and Event Management

NIST CSF Function Alignment

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Overview

Cloud-based platforms generate a wealth of vital log data about activities in the cloud. Since actions in cloud applications and platforms are API-driven, collecting accurate and timely API activity logs and metadata from these services can be programmatically executed in just a few steps. Organizations may need to complement these native capabilities with other technologies to achieve the optimum level of visibility.

Key Best Practices

Aggregate and Correlate Event Data from Multiple Sources

For a holistic view of the enterprise, organizations should ingest and correlate cloud events along with their existing on-premises assets. Logs can be stored centrally in the cloud environment and also aggregated with the organization’s existing security information and event management (SIEM) system for further analysis and correlation. In IaaS platforms, server and application-based logging is still performed using agent-based or log shipping (e.g. syslog) methods, though more and more applications are now exposing logs via API.

Monitor the Network to Detect Potential Cybersecurity Events

A precursor to identifying threats is having the appropriate level of visibility into the cloud network traffic. Cisco estimates that by 2020, 86% of all datacenter traffic will be within and between datacenters (east-west traffic), instead of north-south traffic exiting the datacenter to the internet or wide-area network.[18] This is especially relevant from a security perspective because many cybersecurity attacks propagate laterally through networks and either go undetected or bypass traditional perimeter-based protections. There may be limited options available to gain deep visibility into IaaS traffic because of network abstraction and because of scalability and performance concerns in dynamic workloads, especially in container-based architectures.

Monitor Personnel to Detect Potential Cybersecurity Events

According to Symantec research, “66 percent of risky user activity in the cloud indicated attempts to exfiltrate data.”[19] This includes excessive downloads, account sharing, and frequent document previews (allowing attackers to screenshot data). Common behavior-based security scenarios out-of-the-box (e.g. insider threat) using advanced statistical analysis with baseline profiling for deviation measurement are needed.

Monitor for Unauthorized Connections, Devices, and Software

Monitoring cloud workloads for unauthorized or malicious changes to important system binaries and configuration files can be challenging with tools that are not designed to work with automated deployment tools or multiple instance baselines. Traditional host-based intrusion detection tools that are not optimized for cloud workloads can impact performance and do not scale elastically with these types of workloads. Technologies developed specifically for cloud are needed.

[18] Cisco Global Cloud Index: Forecast and Methodology, 2015–2020 (2016), p. 7, http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

[19] Symantec Internet Security Threat Report, p. 73

Malicious Code

NIST CSF Function Alignment

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Overview

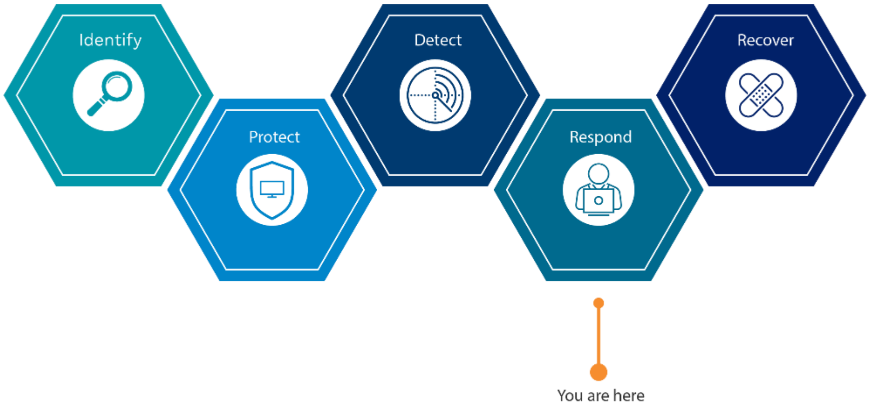
Cloud services are not immune from the threats posed by malware. For example, ransomware, a particularly damaging form of malware, can spread quickly through cloud storage services via their synchronization and sharing capabilities, creating a dangerous fan-out effect.

Key Best Practices

Detect Malicious Code

Endpoint protection solutions should be capable of scaling to the cloud and have protection capabilities designed to address dynamic threats posed by cloud platforms and applications. CASB vendors are also integrating malware protection into their platforms to aid in identifying and blocking the spread of malware through SaaS applications.

For technology recommendations relating to *Detect* see Appendix 2



Respond

Incident Response

NIST CSF Function Alignment

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.

There is greater than 50% chance of getting malware from a SaaS application.

McAfee, Building Trust in a Cloudy Sky (2017)

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Overview

Organizations must be well-positioned to deal with security incidents that involve cloud systems and cloud data just as they are for situations on premises or with traditional endpoints. This includes instituting the appropriate access, tools, processes, and training to contain and mitigate different types of incidents.

Key Best Practices

Contain and Mitigate Incidents

Automating security tasks as part of incident response helps ensure that incidents are contained efficiently, and that response staff can focus on critical issues both on-premises, hybrid, and cloud-native environments. A security automation and orchestration (SA&O) platform integrates existing security technologies, automating repetitive tasks, and orchestrating multiple concurrent workflows. This can include a range of security scenarios, from phishing investigations to insider threat mitigations.

Kudelski Security's Automation and Orchestration for IT and Security Operations solution helps operations and/or security teams achieve near-term value from an automation and orchestration solution – for both cloud and on-premises environments. Organizations can leverage our domain expertise in operations and security, along with our custom software development capabilities, to bring tailored, commercially supported automation and orchestration solutions to our clients' cloud and on-premises environments.

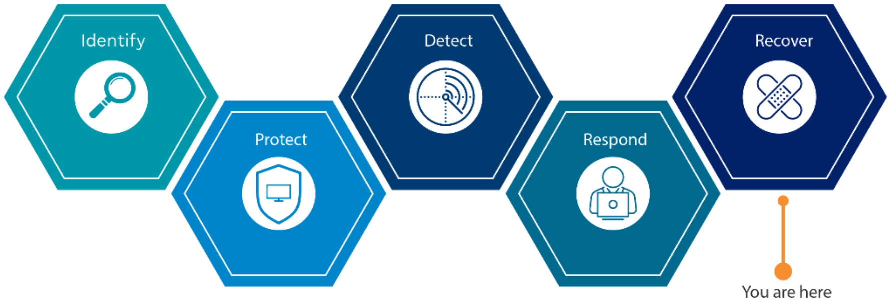
Native features in IaaS platforms can enable incident response capabilities, such as performing forensics using instance snapshots or deploying a trusted "clean room" environment for response activities using infrastructure-as-code. On instances themselves, workload protection tools can initiate corrective actions based on indicators of compromise (e.g. modifications to system files). Coupling this with a SA&O platform, a coordinated response can be executed with other technologies for network containment and remediation capabilities via a lightweight agent that can be deployed on cloud instances. This also allows threat hunters to apply newly observed indicators to historical data in order to retrospectively identify incidents. The option of integration with a SA&O platform or direct integration to security controls are available to enable containment.

For SaaS applications, it's not only important to understand how the SaaS provider handles security incidents *of* the application,[20] but also to have the appropriate tools in place to deal with security incidents *in* the SaaS application.

[20] *See, for example* http://download.microsoft.com/download/2/F/1/2F16A9CA-8D4F-4BB5-8F85-3A362131A95B/Office%20365%20Security%20Incident%20Management.pdf

Once identified, known or suspected malware in SaaS applications can be blocked or quarantined with automated policies.

For technology recommendations relating to *Respond* see Appendix 2



Recover

Recovery Planning

NIST CSF Function Alignment

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Overview

In tandem with the incident response initiatives, organizations must be ready to restore cloud operations within defined metrics to continue business operations, just as they are for situations on premises or with traditional endpoints. This includes instituting the appropriate access, tools, processes, and training to recover from different types of incidents.

Key Best Practices

Execute Recovery Plan

In tandem with incident response and data and system backup activities, organizations should test and verify that recovery plans have clearly defined responsibilities and are tested periodically through tabletop exercises and other simulations.

For technology recommendations relating to *Recover* see Appendix 2

Conclusion

Large enterprises across industry verticals are increasingly embracing public cloud services for a variety of competitive business reasons. Companies get to focus their limited time and resources on developing and growing their core business competencies by leveraging cloud providers whose own core competencies (and economic motivations) are to provide cost effective, reliable, and secure IT service delivery. Cloud services reduce the need for large capital investments in IT infrastructure, creating agility that allows businesses to continually and quickly adapt and scale their technology needs to their business needs.

With shared responsibility, customers can leverage the security foundation, and, in many cases, cloud-native security tools offered by the providers to focus their efforts on securing operating systems, applications, and data. Gartner expects that by 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.[21] Coupling effective cloud security tools with proper design, implementation, training, and policy will improve the security of cloud operations, and thus empower security professionals to better implement cloud transformation and support overall business objectives.

[21] http://www.gartner.com/smarterwithgartner/seven-tips-for-staying-secure-in-the-cloud

Appendix A – Reference Architecture Methodology

Technology Recommendations

The Kudelski Security Cloud Security Reference Architecture highlights best-of-breed technologies from leading vendors that integrate to enable effective protection for the cloud. Our architecture is designed to address a variety of threat scenarios, including sophisticated, cloud-centric attacks that are typically targeted at larger enterprises or public-sector organizations.

The cloud risks for every organization are different. Our Reference Architecture presents market-leading security solutions that either discretely or collectively fulfill security activities to mitigate the identified risks. Organizations can compare their incumbent cloud risk management activities and technology solutions to identify gaps in their existing cloud protection. We do not target particular regulatory environments (e.g. PCI DSS), although the solutions we recommend are generally used or approved for various regulated industries.

Leveraging the NIST CSF for Best Practices

The NIST CSF is a voluntary, industry-led initiative to improve overall cybersecurity preparedness by focusing on risk management and security program maturity. While the CSF was specifically developed for organizations that own or operate critical infrastructure, and not cloud environments, its guidance is applicable across industries and hosting technologies. NIST CSF is designed to complement, not replace, existing cybersecurity controls and procedures in use, such as Cloud Security Alliance's Cloud Controls Matrix.[22]

NIST CSF has a flexible, risk-based methodology which can be applied to identify cloud-specific security activities across a spectrum of risk categories and business segments.[23] According to McAfee research, having consistent security controls across clouds and traditional

[22] https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview

[23] http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

datacenters is a top concern for organizations today.[24] A technology-agnostic framework like NIST CSF provides this level of consistency across the enterprise.

Kudelski Security has integrated the NIST CSF into its Secure Blueprint SaaS platform, which integrates security program maturity and risk management into an easy-to-use tool. Secure Blueprint may be used for cloud environments to help define, reduce, and manage risk from cloud vendor platforms. For more info, visit www.secure-blueprint.com.

The NIST CSF defines five high-level strategic functions for a comprehensive cybersecurity risk management program – identify, prevent, detect, respond, and recover. Mapping cloud security requirements to the NIST CSF functions ensures that the cloud environment is integrated into the overall security program and initiatives.

Kudelski Security's Cloud Security Reference Architecture maps cloud controls to the NIST CSF Functions, as follows:

Identify Cloud Assets & Data

Organizations begin by developing the organizational understanding of the cloud assets, the contained data, and organizational security program and risk management capabilities. This is the foundational step for the introduction of the other functions.

Protect Cloud Assets & Data

Organizations develop and implement safeguards to ensure the identified cloud assets can function as expected to meet business needs. These controls help to limit, prevent, and/or contain the impact of a cybersecurity attack on cloud resources.

Detect Events in the Cloud

Organizations develop and implement measures to identify the occurrence of potential or actual attacks against cloud assets and, by extension, the larger enterprise. This ensures faster discovery of events to initiate appropriate preventative or remedial actions.

[24] Navigating a Cloudy Sky, McAfee (2018), p. 18, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf

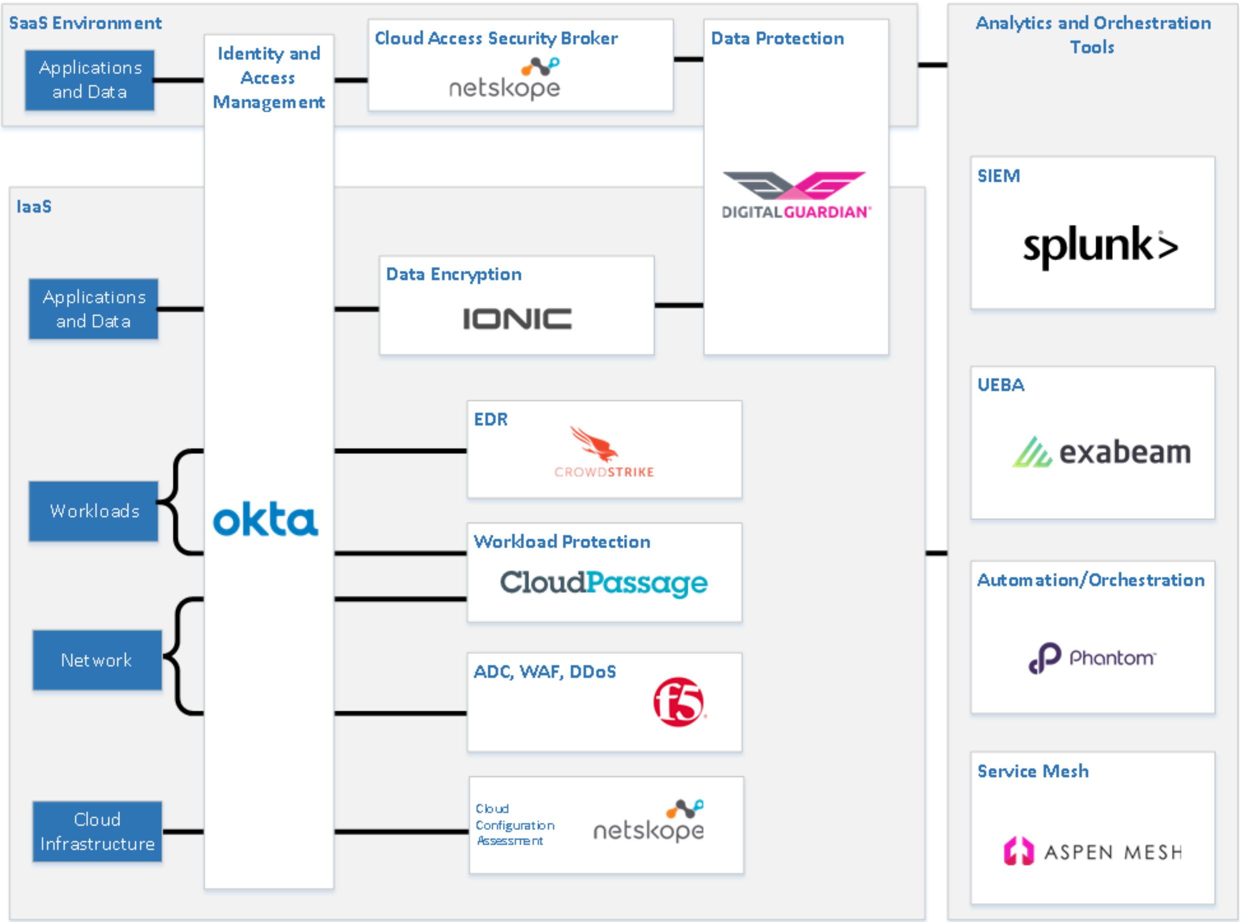
Respond to Attacks in the Cloud

Organizations develop and implement measures to take action against the detected attacks on cloud assets to contain the impact of attacks on cloud resources.

Recover from Attacks in the Cloud

Organizations develop and implement measures to restore cloud capabilities after an attack to help business to keep running as usual with the least impact on operations.

Appendix B – Technology Recommendations



IDENTIFY:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Asset Management (ID.AM) Best Practices for Cloud Environments		
Catalog External Information Systems	Shadow IT Data Loss/Exfiltration	netskope
Map Organizational Communication and Data Flows		
Prioritize Resources Based on Criticality and Business Value	Microservices Configuration Management and Detection	ASPEN MESH

PROTECT:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Access Control (PR.AC) Best Practices for Cloud Environments		
Manage Identities and Credentials for Authorized Users and Devices	Credential Theft/Compromise Insider Threat Data Exposure	okta
Manage Access Permissions, Incorporating Least Privilege and Separation of Duties		
Protect Network Integrity, Incorporating Network Segmentation Where Appropriate	Network-based Attacks	f5 CloudPassage
	Container Based Runtime Security	CloudPassage
Information Protection Processes and Procedures (PR.IP) Best Practices for Cloud Environments		
Create and Maintain a Baseline Configuration of Information Technology	Vulnerability-based Attacks	CloudPassage netskope
Conduct, Maintain, and Periodically Test Backups of Information	Data Theft, Loss, or Destruction Ransomware	amazon web services Cloud Service Providers Google Microsoft Azure
Data Security (PR.DS) Best Practices for Cloud Environments		
Protect Data-at-rest	Data Theft/Loss Data Exfiltration	IONIC netskope
Protect Data-in-transit		DIGITAL GUARDIAN
Protect Against Data Leaks		

DETECT:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Security Continuous Monitoring (DE.CM) Best Practices for Cloud Environments		
Identify, Document, and Mitigate Asset Vulnerabilities	Vulnerability-based Attacks	CloudPassage netskope
	Benchmark Checking	netskope

Monitor for Unauthorized Connections, Devices, and Software	Insider Threats Advanced Persistent Threats Malware-based Attacks Ransomware Phishing	splunk> exabeam Gigamon netskope McAfee PROTECTWISE™ CROWDSTRIKE CloudPassage
Anomalies and Events (DE.AE) Best Practices for Cloud Environments		
Aggregate and Correlate Event Data from Multiple Sources	Insider Threats Advanced Persistent Threats Malware-based Attacks Ransomware Phishing Network-based Attacks	splunk> exabeam McAfee netskope Gigamon CROWDSTRIKE PROTECTWISE™ CloudPassage
Monitor the Network to Detect Potential Cybersecurity Events		
Detect Malicious Code		
Monitor for Unauthorized Connections, Devices, and Software		

RESPOND:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Response Planning (RS.RP) Best Practices for Cloud Environments		
Contain and Mitigate Incidents	Malware-based Attacks Data Exfiltration Lateral Movement	Phantom CROWDSTRIKE PROTECTWISE™ netskope CloudPassage

RECOVER:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Recovery Planning (RC.RP) Best Practices for Cloud Environments		
Recovery Planning	Contain	CROWDSTRIKE

Appendix C – Technology Vendor Descriptions

Asset Management (ID.AM)

netskope

Cloud access security brokers (CASBs), such as Netskope, provide continuous visibility into SaaS solutions used within an organization. Netskope's patented all-mode traffic steering technology allows users to decrypt and inspect cloud traffic. It provides several out-of-band and inline options ensuring complete coverage for users on premises, mobile, and remote – whether they are using a browser, mobile app, desktop app, or sync client.

Using the patented Netskope Context Engine, billions of API transactions across thousands of cloud services can be analyzed to identify not just what cloud services are being used, but also how they are being used. With built-in understanding of APIs for leading SaaS and IaaS solutions (e.g. Office 365, Google Cloud Platform), Netskope can provide invaluable information about the activities of users that traditional web proxies cannot, such as "share," "send," "post," or "upload." This level of granularity provides rich context around cloud usage and permits fine-grained access permissions to protect against data exfiltration or cloud attack vectors.

For SaaS applications, Netskope provides API-level visibility into SSL-encrypted cloud SaaS applications, including traffic from sync clients and mobile apps.

ASPEN MESH

The industry is moving toward containers, microservices, Kubernetes, service mesh and other cloud-native constructs. A service mesh integrates application services that modern web applications need into the container environment, rather than into the code itself. The service mesh toolbox provides a bevy of features that can address different microservices challenges but may not address all the needs of enterprise security teams. Aspen Mesh makes it easy for the enterprise to run service mesh in production with features that address policy, configuration, and a uniform view across large distributed teams.

Access Control (PR.AC)

okta

Okta is a cloud-based identity management platform that provides secure and unified access to both on-premises and cloud applications.[25] Single sign-on for end users provides them with one place to easily access the cloud and on-premises applications they need. Cross-application analytics spanning usage, utilization, and cost can provide the insight to optimize cloud investments and understand user access behavior.

Okta's adaptive multi-factor authentication capability enables access management based on contextual data about the user, device, network, location, and resource. It can integrate with many third-party physical and virtual tokens, including Duo Security and SecureAuth.

Okta provides user management integration with existing on-premises AD/LDAP and includes automated and customizable provisioning workflows for user accounts and cloud application and platform access, improving efficiency and reducing credential misuse by former employees. For example, Okta has a unique integration with Amazon Web Service's IAM system that allows a user to assume various IAM roles or access multiple AWS accounts, while maintaining the same identity and fine-grained permissions.

CloudPassage

The CloudPassage Halo agent, combined with Halo's host firewall orchestration system, allows granular network segmentation policies and protection against lateral movement inside datacenters and cloud environments. Traffic Discovery helps create dynamic firewall policies, ensuring that desirable traffic is not being blocked. Security policies can be defined and enforced on the basis of logical server groups so that host firewalls are automatically updated as the environment changes.

[25] *See* Magic Quadrant for Access Management, Worldwide, Gartner (2017) https://www.gartner.com/doc/3741018 (Registration Required)

Information Protection Processes and Procedures (PR.IP)

CloudPassage

For IaaS workloads, CloudPassage Halo includes pre-built configuration policies spanning a wide range of operating systems (Linux, Windows) and applications. Halo assesses the configuration of workloads by comparing them to standard benchmarks, including Center for Internet Security (CIS). For network devices within on-premises and cloud platforms, such as application delivery controllers, an automation and orchestration platform (AppViewX) enables organizations to maintain configuration control and auditability, while also enabling granular delegation of tasks.

CloudPassage Halo scans for software vulnerabilities across platforms and against a number of sources, including the NIST database of Common Vulnerabilities and Exposures (CVE). Using its lightweight agent, Halo collects information from the cloud systems but performs security analytics on CloudPassage servers. Halo's integration with leading infrastructure orchestration, such as Puppet, allows automated remediation of vulnerabilities.

CloudPassage Halo Detect alerts if a workload has been compromised by monitoring whether important files have changed and by monitoring important server log files to detect intrusions. By examining specific, high-value events, the load added to cloud workloads is significantly reduced.

netskope

The Netskope Cloud Confidence Index (CCI) contains objective criteria adapted from the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM),[26] which allows organizations to see and compare more than 50 service attributes in the areas of security, legal, audit and third-party certifications, vulnerabilities and exploits, financial viability, and privacy features. The CCI enables organizations to understand the appropriateness of cloud services for their organization, identify service gaps against their security and compliance requirements, determine whether to allow services, and identify compensating controls.

[26] https://cloudsecurityalliance.org/group/cloud-controls-matrix

Data Security (PR.DS)

IONIC

For high assurance environments that may span on-premises and cloud environments, the Ionic Security data rights management platform protects data throughout its lifecycle and at scale. With application integrations, Ionic can provide subfile-level data protection (e.g. protect individual words, phrases, or paragraphs within a Microsoft Word document). Ionic provides additional contextual protection – data can only be seen by the right people at the right time in the right place. If cloud data is leaked, either maliciously or inadvertently, Ionic's platform provides both protection against exposure and notification to organizations that leaked data is trying to be accessed.

netskope

Netskope allows organizations to identify sensitive data flowing through SaaS applications, whether users are on premises, remote, or on a web browser, mobile app, or sync client.

DIGITALGUARDIAN®

Digital Guardian is an enterprise DLP solution that provides a holistic view of data access across the organization, including data stored in the IaaS platforms outside the scope covered by CASB DLP. Digital Guardian's unique fingerprinting technology allows efficient and accurate identification and control of sensitive information with minimal initial configuration.

Security Continuous Monitoring (DE.CM)

CROWDSTRIKE

The CrowdStrike Falcon next-generation AV platform seamlessly spans all datacenter environments, from on-premises to IaaS platforms. It includes known malware prevention, vulnerability exploit mitigations, and advanced machine learning to detect and prevent known and unknown malware, all through a single, lightweight agent.

exabeam

Exabeam is a User and Entity Behavior Analytics (UEBA) platform that addresses common behavior-based security scenarios out-of-the-box (e.g. insider threat) using advanced statistical analysis with baseline profiling for deviation measurement. Exabeam Cloud Connectors enable turnkey ingestion of cloud user activity logs from several popular SaaS and IaaS platforms. Exabeam can also integrate with CASBs and cloud-based identity management tools to provide full visibility of user activity in the cloud.

Gigamon®

Cloud customers in hybrid or transitional states, or those with certain regulatory requirements, may require IaaS network visibility akin to what is available on premises, perhaps to be compatible with their existing enterprise security tools. The Gigamon Visibility Platform provides network visibility into workloads on certain private and public cloud IaaS platforms. With Gigamon, network traffic can be selected, forwarded, and delivered to existing security and monitoring tools.

netskope

For SaaS applications, Netskope's multi-layered threat protection includes static antivirus analysis and heuristic analysis as well as dynamic sandbox analysis. The tools can be integrated to share indicator information about the malicious files each system may discover. Netskope provides comprehensive, step-by-step forensic audit trails of all cloud transactions. Ad hoc queries can be used to drill down into data following a suspected event such as data exfiltration by a departing employee, or for compliance reporting.

For SaaS applications, Netskope includes multiple threat intelligence feeds to identify malicious URLs and IPs, command and control servers, compromised user credentials, and more.

Phantom®

For both on-premises, hybrid, and cloud-native environments, a SA&O platform like Phantom can enable efficient incident management, leveraging a variety of available security technologies in the environment, including cloud platforms and applications. The Phantom platform was designed for openness and extensibility – new security scenarios and technologies can be easily integrated with Phantom playbooks and REST APIs. Phantom supports having a human in the loop as well, depending on the task at hand, to ensure that critical operations are not impacted.

PROTECTWISE™

As additional coverage for public cloud and IaaS providers, Gigamon's partnership with Protectwise ensures that the Protectwise platform can seamlessly receive traffic for analysis. Protectwise has built a SaaS visibility platform that captures traditional network IDS and full packet-capture use-cases, while adding efficiencies for analysts detecting, investigating, and remediating anomalous and malicious events.

Protectwise's platform is constantly evolving and currently leverages multiple IPS engines to detect network-based threats. Correlated events are associated to the Lockheed Martin kill chain model for rapid prioritization by analysts.

McAfee™

For certain private and public cloud environments, McAfee’s Virtual Network Security Platform provides an intrusion prevention system (IPS) that intercepts and redirects north-south and east-west traffic for inspection using a variety of techniques to detect and prevent threats.

splunk>®

Splunk provides security visibility by ingesting, correlating, and visualizing data from a variety of cloud and on-premises data sources to deliver robust security reporting and analysis. The Splunk platform can be enhanced and extended with apps for leading IaaS platforms, SaaS applications, and cloud security applications (e.g. CloudPassage). These apps include pre-built dashboards, reports, alerts, and workflows that make Splunk immediately useful for security professionals.

About the Author

Bo Lane

Bo Lane is the VP of Solution Architecture at Kudelski Security, a leading global information security solutions firm focused on innovation. He is responsible for establishing and driving the technology strategy and solutions architecture for Kudelski Security's information security solutions. Prior to joining Kudelski Security, Lane was a senior researcher in the information security-focused R&D laboratory at Georgia Tech. In this role, he served as a technical lead for a number of efforts in enterprise security architecture development, public/private cloud initiatives, and pre-market cybersecurity product evaluations. Lane has a Juris Doctor degree from the University of Georgia School of Law and an undergraduate degree from the Georgia Institute of Technology. He is a Certified Information Systems Security Professional (CISSP).

About Kudelski Security

Kudelski Security is an independent provider of tailored cybersecurity solutions to enterprises and public sector institutions, delivering workable solutions to the toughest security challenges they face.

As part of the Kudelski Group, Kudelski Security embodies the same innovative spirit that has inspired the company since its creation in 1951. Our innovation is purposeful; we strive to create and deliver cybersecurity solutions that answer real problems. We help our clients in their journey to design, deploy, and manage effective cybersecurity through a combination of advisory services, technology deployments, managed security services, and custom research and development.

We build on the concrete expertise of the Kudelski Group and their creation of ground-breaking technology that has shaped the evolution of the digital content ecosystem. Together with the Group, we hold thousands of patents and apply the rich engineering expertise of 3,900+ employees worldwide to the solutions we create and deliver in the cybersecurity marketplace.

Our global reach and comprehensive cyber solutions focus are reinforced by key international partnerships. These include alliances with the world’s leading security technology firms as well as with experts in specialized services, so clients have access to all the tools and talent they need in order to plan, deploy, and run effective cybersecurity programs.