aws marketplace

featuring **SOUNIL YU**

Protecting Your Sensitive Assets in AWS

Enhance security controls, maintain compliance, and safeguard your data by leveraging Amazon Web Services (AWS) services and solutions in AWS Marketplace.

AWS Marketplace Introduction

As operations and resource availability scales in the cloud, organizations should be mindful of upholding configurations and tracking their resource utilization. Implementing cloud security posture management (CSPM) and data loss prevention (DLP) solutions can help overcome potential challenges around resource management and data protection in your environment. In this whitepaper, Sounil Yu, creator of the Cyber Defense Matrix, provides prescriptive guidance on how to prioritize security controls to protect your sensitive assets in the cloud.

Expanding on Yu's perspective, AWS Marketplace will share how you can apply these practices to your AWS environment. They will cover relevant AWS services that can enhance your security controls and data protection. Finally, AWS Marketplace seller solutions will be featured as available options for securing the sensitive assets in your AWS environment.

The featured solutions for this use case that can be accessed in AWS Marketplace:

Trend Micro Cloud One™ – Conformity

Check Point CloudGuard Dome9

Digital Guardian Data Loss Prevention (DLP)

SOUNIL YU

How to Prioritize Security Controls for Sensitive Data and Applications in AWS

By Sounil Yu, Creator of the Cyber Defense Matrix

Overview

In this chapter, readers will understand why public cloud brings forth a wide array of new capabilities, but also new security considerations. Fortunately, these can be addressed through tools available both natively within AWS and through the AWS Marketplace. In addition, this whitepaper shows how security practitioners can prioritize which controls are most needed through a framework-based approach and by understanding whether we are dealing with “pets” or “cattle”. Through the framework of the Cyber Defense Matrix, we can quickly and easily find the relevant AWS Native and AWS Marketplace tools to help us to better secure our most sensitive data and applications (our “pets”).

Cloud as a New Operating Model

Amazon Web Services (AWS) has brought forth a fundamentally different model for how we build, operate, and secure IT infrastructure and applications. Three key aspects make the cloud radically different.

Highly Configurable: Everything can be defined programmatically and tailored to meet a wide variety of needs.

Comprehensive and Interoperable Features and Services: A wide array of on-demand features and services can be mixed and matched, each also highly configurable.

Centralized and Consolidated: Cloud environments can simplify operations and management while offering tremendous economies of scale.

However, these qualities impart new considerations when it comes to managing our security posture in AWS. These include the following:

- **Configuration Errors:** Because everything is highly configurable, we can be prone to errors that create unintended exposures and vulnerabilities, such as overly permissive access to sensitive resources.
- **Cloud Sprawl:** AWS regularly rolls out new capabilities and services, but this can create many more individual resources that need to be tracked, including microservices, containers, and serverless AWS Lambda functions. With each resource having its own configuration, the potential for a configuration error grows exponentially.
- **Eroding Network Perimeter:** With everything being in the same logical locations, network-centric boundaries are not as applicable. Instead of just relying solely on a network-centric identity, AWS forces us to consider other forms of identity and access management (IAM), such as API keys and other IAM credentials, that are not strictly network-centric.

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

The flexibility and scale we have in AWS also means that we can make mistakes at scale too. With thousands of distinct resources that need to be tracked, properly configured, and free of vulnerabilities, how can we be certain that those who set up those services did it properly? Now take all this and put it into an environment where everything is commingled together, and we can see how an incorrect misconfiguration or exposed vulnerability needs to be found and addressed quickly.

It is also no wonder that Gartner reports that "Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes."[1] As such, it is imperative that we maintain and enforce the correct configuration throughout our environment; keep track of what resources we actually have and are using; discover and mitigate vulnerabilities; and efficiently manage secrets and IAM credentials.

Potential Solutions

Fortunately, AWS also gives us new ways to tackle these security needs and at scale with native and third-party tools that help us to do the following:

- prevent misconfigurations and vulnerabilities as things are being built,
- provide extensive visibility into your running cloud environment,
- analyze that visibility to find misconfigurations and vulnerabilities in production,
- and fix and patch them before they are exploited.

If we wish to address these security needs on our own, one or more of the following AWS native capabilities can be put to use:

- AWS Config: assess, audit, and evaluate the configurations of AWS resources,
- AWS Trusted Advisor: guide the provisioning of resources following AWS best practices,
- AWS Well-Architected Tool: review the state of workloads and compare them to the latest AWS architectural best practices,
- AWS Systems Manager: understand and control the current state of your resource groups,
- AWS Security Hub: view high-priority security alerts and security posture across AWS accounts.
- Amazon Macie: inventory and classify sensitive data in AWS storage buckets

We can also leverage AWS Marketplace independent software vendors (ISVs) who provide ready-to-use solutions to tackle these security needs. There are two primary classes of cloud security tools that provide protective capabilities for cloud service providers, such as AWS. As defined by Gartner, they include capabilities such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP). To understand the differences between CSPM and CWPP, it is helpful to look at frameworks to understand how they relate to each other. The Cyber Defense Matrix is one such framework that can help us understand the differences and ensure that we are addressing the complete set of security needs in the cloud.

[1]https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

A Framework for Understanding Options for Cloud Security

The Cyber Defense Matrix, as shown in Figure 1, is an adaptation of the NIST Cybersecurity Framework, but with an added dimension that captures various classes of assets that we care about. These assets are devices, applications, networks, data, and users. This added dimension will help us improve our ability to find and fill gaps in our understanding of completeness when it comes to managing our cloud security posture.

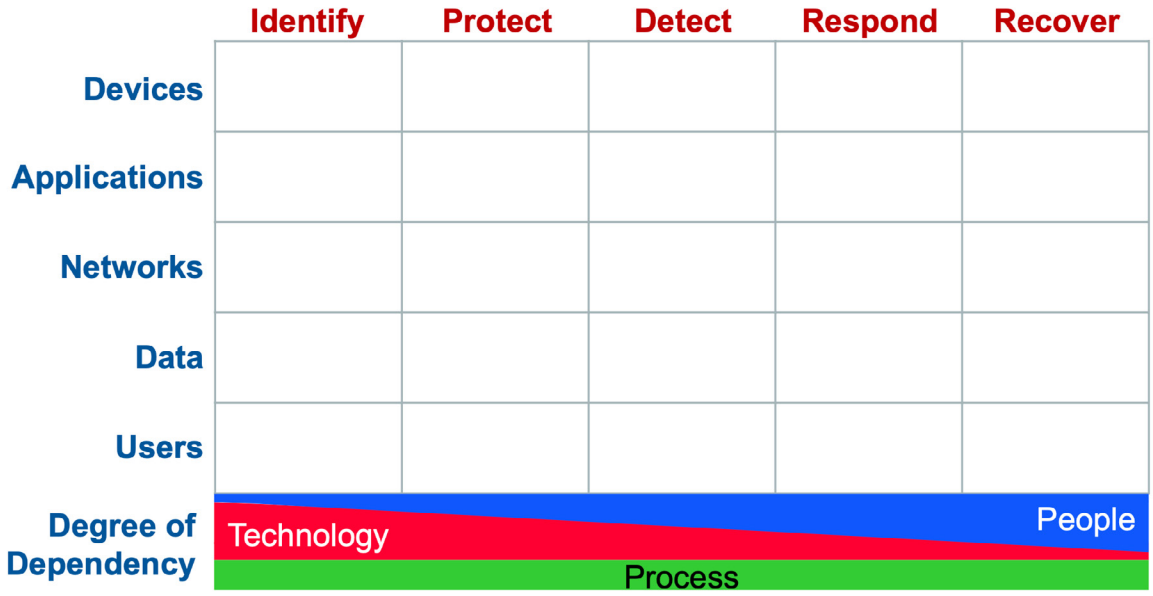


Figure 1: Cyber Defense Matrix

Each asset class in the Cyber Defense Matrix represents resources that needs to be protected in cloud environments. For the purposes of this whitepaper, we will focus primarily on the left side of “boom” of the Cyber Defense Matrix. “Boom” is the point between PROTECT and DETECT where some event occurs. We want to look at a range of cloud security solutions that allow us to avoid a “boom” scenario at all.

The Cyber Defense Matrix provides a systematic approach for evaluating threats against each type of resource and considering controls that help mitigate any vulnerabilities associated with those resources. The types of assets listed on the left of the matrix are generically defined, but these classes of assets are represented in cloud environments, albeit some with different labels. For AWS in particular, these resources can be described with labels such as Amazon EC2 instances for DEVICES or Amazon S3 Buckets for Data. While there may be some overlapping features, CSPM and CWPP generally address different types of assets, as shown in Figure 2. Specifically, CSPM typically secures the configuration of the underlying infrastructure, such as storage buckets (Data), IAM roles (Users), and network security groups (Networks). CWPP typically secures the operating system (Devices). Both CSPM and CWPP have roles in security applications, with CSPM securing PaaS and serverless while CWPP secures containers.

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

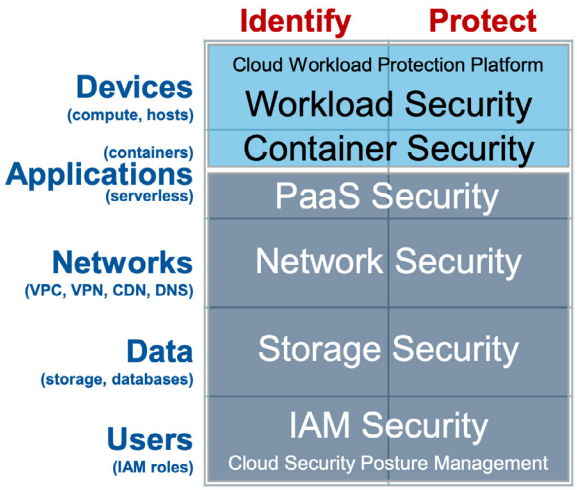


Figure 2: Mapping CWPP and CSPM to the Cyber Defense Matrix

The Cyber Defense Matrix provides pattern matching opportunities to understand the extent to which these capabilities meet various security needs and to find potential gaps. Figure 3 provides a more detailed breakdown of how capabilities map to different need areas for cloud security under the functions of IDENTIFY and PROTECT.

		Devices (compute, hosts)	Applications (containers, serverless)	Networks (VPC, VPN, CDN, DNS)	Data (storage, databases)	Users (IAM Roles)
Identify	Inventory	EC2 Instances, Stopped Machines	Software Bill of Materials, Installed Applications	IP Addresses, VPCs	S3 Buckets, Databases	Accounts
	Classification	Unsupported O/S			Classification of viruses, malware, PII, PHI, PCI	Admin Accounts
	Vuln Assessment	O/S Vulnerabilities, Weak PWs, Insecure SSH Keys	Open Source Library Vulnerabilities	Unintentionally Open Ports, Improper Routing	Unintentionally Open S3 Buckets, Exposed Keys	Weak Passwords, No MFA
	Identity Mgt	SSH Key Management	Secrets Management	DNS, DHCP, IP Address Management	Key Management	IAM Role Management
Protect	Access Mgt	EC2 Connect		Firewall Manager	S3 Bucket ACLs	IAM Role Management
	Patching / Fixing	O/S Patch	Code Fix, Component Update	Network Segmentation	Encryption	Password Reset
	Exploit Mitigation	Memory Protection	Web Application Firewall	Network Intrusion Prevention System		MFA Enablement
	Logging, Monitoring	System Logs	Application Logs	Flow Logs	Access Logs	Account Activity History

Figure 3: Breakdown of Capabilities to Support Cloud Security Needs

The sub-functions of IDENTIFY capture security requirements that are often described as “visibility”, but this type of breakdown ensures that when we use the word “visibility”, we can be more precise in terms of the type of visibility that we desire. This can include visibility into what we have (inventory), how important it is to us (classification), and whether or not it has any exposures that we should be concerned about (vulnerability assessment). These sub-functions manifest differently across each asset domain, typically using words that specific to that domain, but the

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

sub-function generally remains the same. For example, when it comes to the function of inventory, this can include activities such as asset management (devices), headcount (users), and route discovery (networks). When it comes to vulnerability assessments, this can include the discovery of various types of vulnerabilities, such as misconfigured storage buckets, operating system vulnerabilities, and users susceptible to phishing attacks.

For PROTECT, there are also many specific sub-functions, including access control, patching, exploit mitigation, audit logging, blacklisting, whitelisting, hardening, segmentation, integrity monitoring, and many others. These manifest differently for each asset domain as well. If capabilities to perform these functions are not available directly from the cloud provider, we can often find the capabilities available through ISVs. The Cyber Defense Matrix can continue to be used to map those ISVs as well to gain an understanding of security control coverage across all types of assets in the cloud.

Approaches for Securing Pets vs. Cattle

How we prioritize security controls may differ depending upon whether we are dealing with “pets” or “cattle”. The notion of “pets” vs. “cattle” was popularized by Randy Bias and has gained adoption in the cloud-native world, but let’s first make sure we all understand what are pets and what are cattle.

Pets are assets to which we give names that we can remember and pronounce. When it gets sick, we take it to the vet and we like giving it hugs. Pets are like our personal laptops or that server under our desk or our social security number. Cattle, on the other hand are branded with an obscure string of letters and numbers, which we cannot pronounce and we do not really care to remember. And when it gets sick, it gets culled from the herd. Cattle are like containers and serverless functions and credit card numbers that change with every transaction.

This understanding of pets and cattle is important because the approach that we take for securing pets is very different than the approach that we take for securing cattle. Before AWS, we traditionally built pets. They are hard to manage. They take up a lot of time and resources. And they get run over often, requiring a lot of manpower to get them healthy again.

Securing pets take a lot of time and effort. But if you build systems to be more like cattle, securing them is substantially easier. Cloud-native security capabilities like CWPP and CSPM help reinforce the usage of design patterns that build infrastructure and applications like cattle instead of pets.

Now we will always have pets. And we can put our pets in the cloud, but we have to make sure that we are protecting them accordingly, and so we need tools to secure them and to treat

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

them well. The type of tools that we need can be broken down into the traditional CIA triad: confidentiality, integrity, and availability. As shown in Figure 4, there is a wide array of capabilities available natively within AWS (and in the AWS Marketplace) to help us do CIA for our pets.

Figure 4: AWS Native Capabilities Aligned Against the CIA Triad

In fact, there's an extensive array of native capabilities mapped against the Cyber Defense Matrix, as shown in Figure 5, that we can use to secure our pets in the cloud.

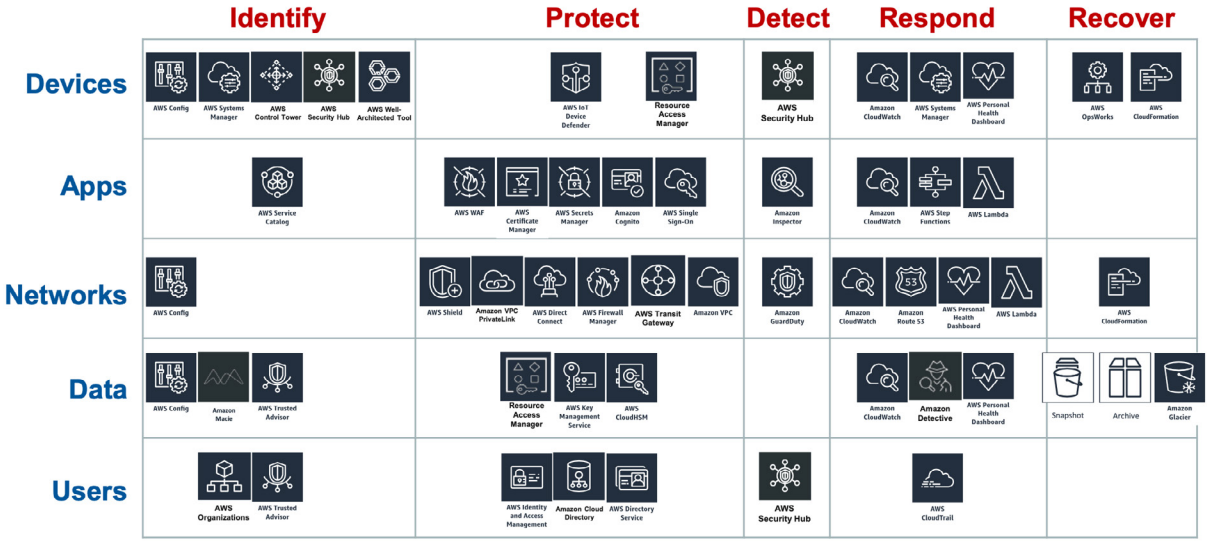


Figure 5: AWS Native Security Capabilities Mapped to the Cyber Defense Matrix

However, if we want to build cattle instead, we need to operate with a different paradigm and a different set of design principles. These design principles are: distributed, immutable, and ephemeral, as shown in Figure 6. These attributes confer security benefits, addressing some of the main challenges that we have had in security, but more interestingly, these attributes can actually counter the need for the CIA triad. If something is distributed, then why do we need any one asset to be available? If something is immutable, then why do we need to worry about its integrity? If something is highly ephemeral, then why do we need to worry about its confidentiality?

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

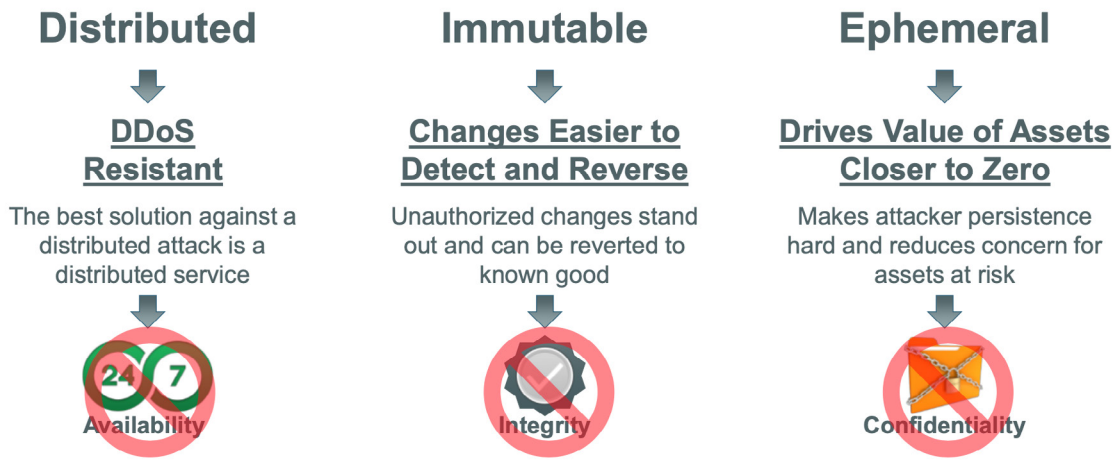


Figure 6: The DIE Triad – Distributed, Immutable, Ephemeral

Here too, AWS offers cloud-native capabilities that allow us to build with cattle like designs. For example, Amazon CloudFront helps us ensure that we can deliver services in a highly distributed fashion. AWS CloudFormation templates help ensure that things are built exactly to specifications in a repeatable and immutable way. And AWS Lambda provides a way to build applications based on very short-lived and ephemeral functions. And as shown in Figure 7, there are many more native capabilities that AWS offers that enable us to build systems to be more like cattle by adhering to the DIE design principles.

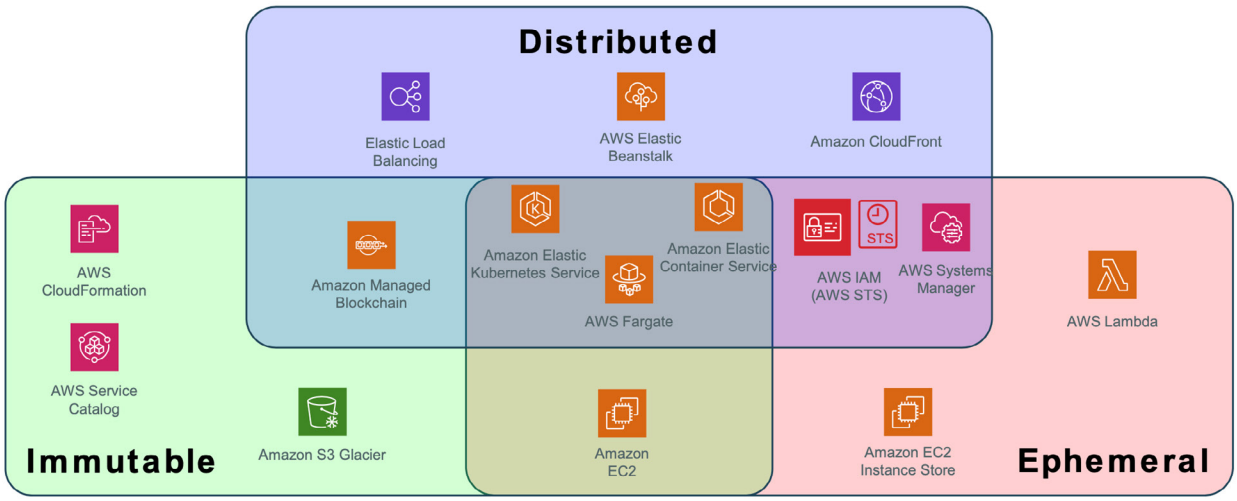


Figure 7: AWS Native Capabilities Mapped to the DIE Triad

As much as we may want to build cattle-like systems, we have to recognize that we will always have pets. However, we should aim to have a minimal number of pets so that our security obligations can be addressed with the few cyber veterinarians that we have. Interestingly the distribution of pets and cattle shifts in ways that align with the Shared Responsibility Model. As shown in Figure 8, this model was intended to help customers understand that AWS will be responsible for security of the cloud, but customers are responsible for security in the cloud.

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

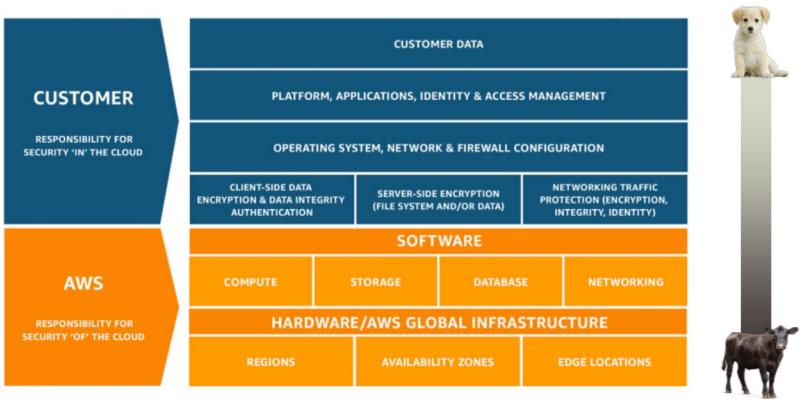


Figure 8: AWS Shared Responsibility Model and Distribution of Pets and Cattle

Since AWS is responsible for security of the cloud, the underlying components that make up the cloud can be seen as "cattle" by AWS customers. Compute, storage, databases, networking, hardware, even whole regions and availability zones, at the macro level, they are all cattle. From the customer's standpoint, they are disposable. They manifest the attributes of the DIE triad. However, as we move up to the part of the model where customers are responsible for security, we typically start seeing more pets. We should set a goal to try to keep them like cattle instead.

Over time and with tools like CSPM and CWPP, we can start our journey towards higher levels of cloud-native maturity so that we end up with more cattle in the cloud and for the pets that we do have in the cloud, they are actually secure. Over the longer term, we should continue to make design decisions that aim to have our environment in the cloud be all cattle. Again, we will always have some pets, but such an explicit goal helps us make better design choices while minimizing the burdens that we would otherwise face if we ended up with too many pets. It may be possible to gauge the maturity of an organization's adoption the cloud based on the proportion of pets that we find, where more mature organizations will have fewer and fewer assets resembling pets and many more that look like cattle.

Also, it is noteworthy that Customer Data sits at the top of this model. Customer data seems to resist being turned into cattle. But that may not be forever the case. A number of privacy-enhancing technologies (which ironically enough has the acronym PET) are emerging that allow us to turn customer data from pets into cattle. These tools include differential privacy, homomorphic encryption, multi-party computation, trusted execution environments, and federated learning. As shown in Figure 9, these approaches may point to the future of data security (and cloud security in general), where we are able to make data more like cattle so that we don't even need to protect it at all, and we can instead let it DIE instead.

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

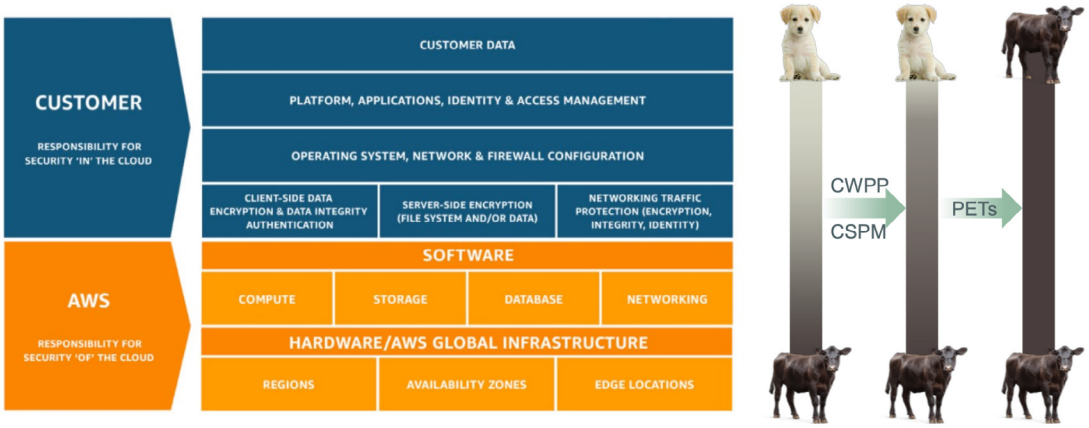


Figure 9: The Future Path For Data and Cloud Security

Summary

AWS brings many benefits that can propel business and innovation forward. As shown in the Shared Responsibility Model, while Amazon is responsible for security of AWS, the customer must not forget that they are responsible for security in AWS. If we are putting pets into the cloud, then we can meet our security obligations through the use of native AWS security capabilities and through commercial CWPP and CSPM offerings.

However, an alternative approach is to minimize the number of pets that we have to deal with. We should be conscious of when we are creating new pets and only resort to pet-like designs when a cattle-like design pattern is not available. We should discourage or disincentivize pet creation, and to the degree possible, encourage removal of pets when we can. Unfortunately, this can be a very emotional decision for the business and for the owner. Once we have a pet, we really do not want to lose it.

As such, it is important that we encourage and incentivize cattle creation instead. We also want to prevent cattle from turning into pets. How does that happen? Well, if we make changes to that cattle, we violate the principle of immutability. Or we let it live longer than it needs to, we violate the principle of ephemerality.

Exercising stringent pet controls also includes making people aware when they are about to adopt a pet. In the world of IT, we often do this unknowingly and accidentally. But going forward, we want to make owners more aware when they are about to adopt a pet. We want to present them with the awareness that something that they are responsible for is turning into a pet. Before it becomes a full-fledged pet, they are asked to sign an adoption certificate where they promise to love, care for, and attend to, AND SECURE this pet for the rest of its life. We want owners to make wise decisions and understand their commitments before adopting new pets, because the future of security may rest more in controlling how many pets we have than how well we secure them.

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

aws marketplace

Protecting your sensitive assets in the cloud with AWS services and third-party solutions.

Ensuring the strength of your security posture for sensitive AWS assets requires an understanding of how sensitive data can be accessed, who has access to it, and what they are doing with their privileges. Implementing both AWS services and AWS Marketplace seller solutions can help protect these sensitive assets.

For example, AWS Security Hub aggregates, organizes, and prioritizes alerts and findings from multiple AWS services to give you a centralized view of your overall security posture. With Amazon Macie, you can leverage machine learning and pattern matching to identify and protect sensitive, vulnerable information that may exist in your Amazon S3 buckets. AWS Key Management Service (KMS) creates cryptographic keys that provide you with a central control point to define policies and manage permissions for your AWS resources. And by using AWS CloudHSM, you can export all your keys to other hardware security modules, saving time on tasks such as hardware provisioning and software patching.

As you deploy more applications and services in the cloud, it becomes increasingly important to track resource configuration and prevent vulnerabilities that may affect sensitive data. Leveraging a combination of CSPM and DLP solutions can increase access control over your data while managing the configuration of all your assets to help maintain compliance. With both of these solutions in place, you can better manage who has access to resources in your environment while mitigating risk that may occur as a result of misconfigurations. Trend Micro Cloud One™ – Conformity delivers actionable, step-by-step remediation rules to help ensure compliance as you commit more resources to the cloud.

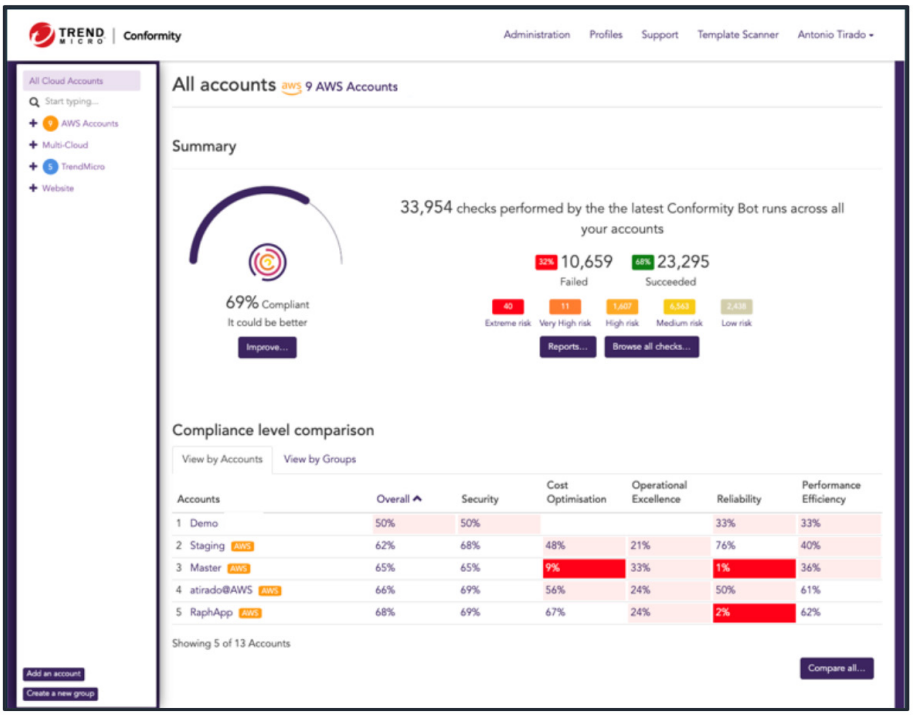
How AWS customers are leveraging Trend Micro as part of their security architecture

Trend Micro solutions help you enhance visibility and control over sensitive assets, strengthening your security foothold in the cloud. Some of the ways that customers are leveraging Trend Micro to enhance their security posture include:

- **Manage misconfigurations of cloud resources:** With Conformity, you can centrally manage and monitor misconfigurations of resources in your AWS environment. It uses over 600 rules based on the AWS Well-Architected Framework to deliver misconfiguration reports with actionable remediation steps.

- **Complete visibility with a single dashboard:** Conformity centralizes the discovery of misconfigurations, policy management, and reporting into a single view. In the solution's dashboards, you can receive actionable insights to help accelerate incident detection and response within your environment. By scheduling and running reports with custom filters, you can conduct comprehensive infrastructure audits on a regular basis and distributed as you need them.

- **Continuous assurance:** Conformity performs continuous compliance checks against best practices to uphold your security posture while saving time by eliminating manual tasks and upkeep. Ensuring this compliance provides you with the assurance that your infrastructure is configured and deployed securely from build pipeline to runtime.



Check Point Software Technologies and Digital Guardian are other solutions available in AWS Marketplace that can help you achieve compliance and data protection. Check Point CloudGuard helps create a single view to inspect inbound and outbound traffic while enabling always-on enforcement of security policies. The Digital Guardian Data Loss Prevention solution gathers intelligence on your security events to enhance visibility and create DLP policies that help protect your sensitive data.

aws marketplace

Why use AWS Marketplace?

AWS Marketplace simplifies software licensing and procurement by offering thousands of software listings from popular 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 one-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, solutions 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 network security solutions in AWS Marketplace

Security teams are using AWS native services and seller solutions 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 solutions can help you get started:

TREND MICRO

Trend Micro Cloud One – Conformity
Real-time security, governance, and compliance posture management.

DIGITAL GUARDIAN

Digital Guardian Data Loss Prevention (DLP)
Leverage data analytics to create, enforce, and report on data protection policies across your environment.

CloudGuard Dome9

Check Point CloudGuard Dome9
Agentless solution that integrates threat prevention and policy orchestration through AWS native controls and APIs