Security Solutions on Amazon Web Services

Leveraging AWS Marketplace ISV Solutions

November 2016

awsmarketplace

Contents

Introduction

As IT continues to play a more central role in the modern enterprise, security is as great a concern as ever before. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of ISVs, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more. These products can be integrated with existing technologies, enabling you to deploy a comprehensive security architecture across your AWS and on-premises environments.

Software available in AWS Marketplace from software vendors is offered with pay-as-you-go pricing (hourly, monthly, yearly) and bring your own license (BYOL) options, to help you ensure you have the flexibility and performance to meet your workload requirements. Selected vendors take advantage of **AWS Marketplace Support for Clusters and AWS Resources**, which use AWS CloudFormation templates to launch deployments beyond a single AMI, using instance clusters and other AWS resources to improve performance and scalability. With AWS Marketplace, you can quickly acquire additional security solutions to help protect your systems and data without lengthy purchasing, infrastructure provisioning, or deployment cycles.

Infrastructure Security

The central concept of cloud computing is turning IT infrastructure into a utility—that is, enabling server, networking, and storage capacity to be provisioned remotely using code as opposed to using on-premises hardware. While this does offload many of the infrastructure maintenance tasks required on-premises, such as cabling, power/cooling, building security, etc., customers retain the same control over the underlying hardware—including responsibility for who can access it. AWS provides several security capabilities and services to help customers increase security of and network access to their AWS resources, including network and web app firewalls, 256-bit encryption, and dedicated network connections. Many customers find that they can augment the infrastructure security that these features provide by incorporating solutions from third party software vendors.

One of the more common infrastructure security initiatives among enterprises is the incorporation of Intrusion Detection and Prevention Systems (IDS/IPS) to prevent network attacks and breaches of their IT environments. Intrusion Detection entails monitoring inbound and outbound network traffic to discover unusual activity which may represent an attempt to gain access to an IT environment. Intrusion Prevention is a more proactive approach to security. Most IPSs provide the same monitoring and alerting features of an IDS, as well as policies that govern network traffic and functionality, enabling administrators to take specific actions when notified of a potential threat.

A very commonly deployed third-party solution for IDS/IPS currently available in AWS Marketplace is Trend Micro Deep Security™. Deep Security offers complete cloud protection that's easy to scale and helps you maintain continuous compliance. It's powerful security with pricing to match your elastic workloads, giving you powerful protection with the cost-effectiveness that cloud computing is known for. You can protect hybrid environments with the Deep Security AMI and pay hourly per workload protected. With protection starting at just $0.01 / hour, you can: defend your network against attack with host-based intrusion detection and prevention; stop patching live systems by shielding from vulnerability exploits; protect Windows and Linux workloads from malware; streamline the last mile of compliance with File and System Integrity Monitoring; and get alerts about potential security events in system logs.

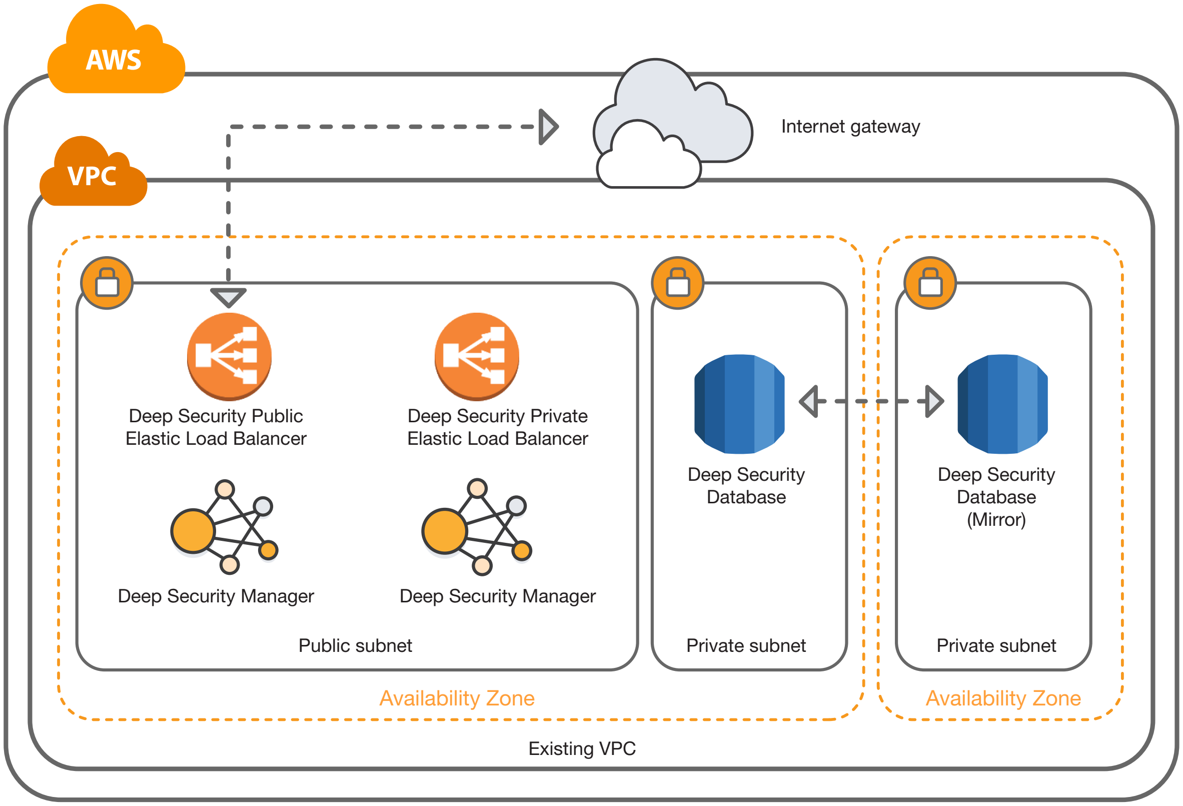

Fig. 1. Example of a combined batch and stream processing use-case

Another common requirement for organizations is the ability to protect themselves from Distributed Denial of Service (DDoS) attacks. While Amazon EC2 Auto Scaling and Elastic Load Balancing can be leveraged to mitigate DDoS risk, many AWS customers find that they can help further safeguard their systems using third-party solutions.

The Barracuda Web Application Firewall for AWS is one such offering—a scalable security solution that protects applications from targeted and automated attacks, including DDoS. Customers are able to protect web applications from data breaches, defacement, OWASP Top-10 Attacks, application layer DDoS and other attack vectors, receive automatic updates with defense against new threats and vulnerabilities with real-time protection, use strong authentication and access control capabilities to ensure security and privacy – restrict access to sensitive applications or data and able to bootstrap and auto scale as required with automated and clustered deployments using CloudFormation templates. Get secure connectivity with visibility and control by using the Barracuda NextGen Firewall F-Series, the next-generation firewall solution for deployments on Amazon Web Services.

Another popular WAF deployed on AWS is Imperva SecureSphere, which analyzes all user access to your business-critical web applications and protects your applications and data from attacks. SecureSphere dynamically learns your applications' "normal" behavior and correlates it with threat intelligence for Web applications to deliver superior protection. It also natively leverages important AWS services, including Amazon VPC, AWS CloudFormation, CloudWatch, and Elastic Load

Balancing. SecureSphere Database Activity Monitoring and Database Firewall provides enterprise-class protection, audit analysis, automated processes and customizable reports running natively on AWS. SecureSphere data protection solutions protect databases from attack, reduce risk and streamline compliance by enabling organizations to leverage common infrastructure, and thus common processes and reporting, both on AWS and on-premises.

Logging & Monitoring

While infrastructure security initiatives are focused on helping to prevent, identify and resolve breach attempts as they happen, the use of logging and monitoring practices help enable a more proactive approach to security. Through increased visibility and auditability of activity inside application infrastructure, organizations can leverage policy-driven alerting and reporting that helps improve their security posture. Enterprise-scale AWS environments are perpetually producing large volumes of log data. In the context of security, services such as AWS Config, AWS CloudTrail, and Amazon CloudWatch are particularly rich sources. By applying analytics to that log data, organizations can identify potential attack vectors before they are identified by hackers and remedy those attack vectors accordingly. Organizations who are looking to gain additional insight into their AWS log data can find a variety of easy-to-use, cost-effective logging and monitoring products from popular software vendors in AWS Marketplace.

Alert Logic Threat Manager with Alert Logic ActiveWatch for AWS is a fully managed, cloud-based security and compliance solution delivered as-a-service to help you streamline the security of your AWS environments. Threat Manager combines network intrusion detection (IDS) and vulnerability assessment technologies to enable rapid detection of suspicious activity and identification of threats to your AWS workloads. ActiveWatch includes 24x7 monitoring and proactive threat notification - by GIAC certified analysts - and continuous protection of your AWS environment. As an extension of your team, Alert Logic provides expert insight into the real threats against your AWS workloads. Threat Manager detects suspicious activity in network environments, quickly identifying threats to your assets so that you can respond.

ActiveWatch monitors network traffic and analyzes billions of events, using AlertLogic's patented ActiveAnalytics. Using intelligent multifactor correlation, it identifies security events requiring attention. After validation by a SOC analyst, AlertLogic notifies you with recommended actions/responses within 15 minutes for critical issues. When needed, senior specialist teams are engaged to assist you. You can also implement automated blocking through integration with your network firewalls. Threat Manager also provides key elements to address the requirements of PCI DSS, HIPAA/HITECH, GLBA, Sarbanes-Oxley, and other mandates.

In addition to identifying potential attack vectors, logging and monitoring tools allow customers to help gain a better understanding of user activity to identify behavior that could compromise the security of the environment or indicate malicious intent.

Configuration & Vulnerability Analysis

While infrastructure security initiatives are focused on helping to prevent, identify and resolve breach attempts as they happen, the use of logging and monitoring practices help enable a more proactive approach to security. Through increased visibility and auditability of activity inside application infrastructure, organizations can leverage policy-driven alerting and reporting that helps improve their security posture. Enterprise-scale AWS environments are perpetually producing large volumes of log data. In the context of security, services such as AWS Config, AWS CloudTrail, and Amazon CloudWatch are particularly rich sources. By applying analytics to that log data, organizations can identify potential attack vectors before they are identified by hackers and remedy those attack vectors accordingly. Organizations who are looking to gain additional insight into their AWS log data can find a variety of easy-to-use, cost-effective logging and monitoring products from popular software vendors in AWS Marketplace.

For example, it is not uncommon for security scans to take longer to complete than for a dev team to complete their next build. In such a case, by the time the scan is done, it is irrelevant. Another challenge arises from the difficulty of manually inspecting and auditing virtual infrastructure. Unlike on-premises datacenters, which generally maintain the same configuration for the entirety of a hardware refresh cycle (typically 3-5 years), cloud environments are dynamic by nature, and their configurations can change at any time. An entire datacenter worth of virtual machines can be spun up and shut back off in minutes. This rate of change makes it essential to automate vulnerability analysis scans.

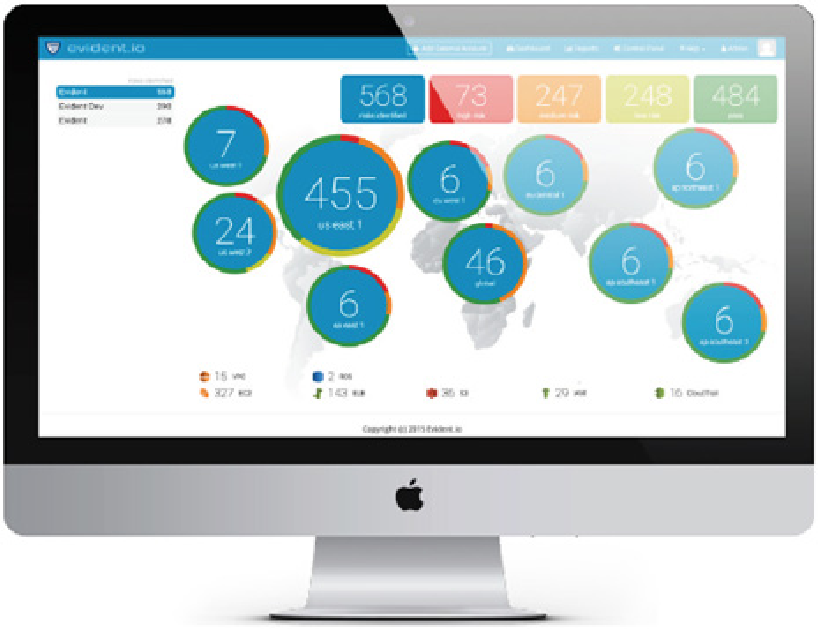

Fig. 2. Evident.io’s Risk Assessment Dashboard

Evident.io's Evident Security Platform (ESP) is one of the solutions that can help an organization achieve this automation. It's the first and only infrastructure security solution to provide complete coverage of an organization's entire AWS environment, combining automated detection of security risks with guided remediation and audit capabilities to meet compliance requirements. ESP is a cloud-native infrastructure security solution providing full coverage of all AWS accounts, services and regions. It combines the detection and analysis of misconfigurations, vulnerabilities, and risk with guided remediation and audit capabilities to meet compliance requirements-all in one solution. ESP was designed specifically to help modern IT and DevOps teams implement and maintain security within the AWS Shared Responsibility Model. By giving IT, Security, Engineering, and Operations a continuous, global view of security risk, and actionable intelligence needed to rapidly remediate and secure their entire AWS Infrastructure, ESP makes it easier for organizations to protect their valuable assets on AWS.

Tenable Nessus is also a very commonly deployed solution for configuration and vulnerability analysis. It's pre-authorized for vulnerability, compliance and threat scans of AWS environments with the largest collection of network security checks and configuration and compliance audits. Nessus assessment and management solutions are pre-authorized for vulnerability, compliance and threat scanning for AWS developers and customers, and provide patch, configuration, and compliance auditing; mobile, malware, and botnet discovery; sensitive data identification; and vulnerability analysis for Amazon EC2 environments and instances.

Data Protection

Many organizations have established policies or are subject to regulations that require they protect their data from unauthorized disclosure or modification. Some of the most common tactics include encryption/ key management and policy-driven controls.

Encryption is the process by which data is encoded in such a manner that only authorized parties can read it. Encryption does not prevent interception of data by unauthorized parties—it simply denies them the ability to make sense of it. To decode encrypted data into its original form requires encryption keys, which are random strings of bits created explicitly for encrypting and de-encrypting specific datasets. Key Management is the process by which an organization creates, stores, and secures encryption keys so that they only end up in the proper hands. AWS Key Management Service (KMS) is a managed service that can make it easier to create and control the encryption keys used to encrypt data, and uses Hardware Security Modules (HSMs) to protect the security of keys. When used in conjunction with AWS KMS, third-party key management solutions can help organizations achieve advanced protection of their keys.

Policy-driven controls are data protection measures that are built into the overarching management framework. Clearly defined policies can reduce the influence of human error by clearly defining permissions for users/ groups of users, where specific applications/data can reside, how specific situations are to be handled, etc. In an on-premises datacenter, it is not uncommon for policies to be communicated very casually—verbally, via email, or stashed away in an employee handbook that new IT personnel are supposed to read on day one. In a public cloud like AWS, policies can be coded in (including policies that determine how encryption keys are stored and who can access them), making them much easier to enforce.

You can access several data protection solutions with pay-as-you-go pricing from AWS Marketplace to make it even simpler to encrypt data, manage encryption keys, and enforce security-oriented policies on AWS.

Vormetric Transparent Encryption for AWS secures cloud data-at-rest with on-premises key management, granular data access controls, and detailed data event logs to meet compliance audit requirements and protect what matters most—your data—within AWS. With Vormetric Transparent Encryption, your organization can safely make use of the flexibility and scalability available from Amazon, while meeting compliance requirements and safeguarding intellectual property.
The solution encrypts data within your AWS instances, provides policy-based data access controls, integrated key management, and detailed security intelligence information about data access patterns. The solution is transparent to applications and to system management processes making it easy to deploy and operate. Data is only accessible by authorized users and processes; therefore, policy can allow privileged users (even cloud administrators) to manage systems without the risk of them having visibility to the data. The Vormetric Transparent Encryption for AWS 5-Client includes a single secure, hardened, management instance plus data protection for up to 5 client systems within your AWS environment.

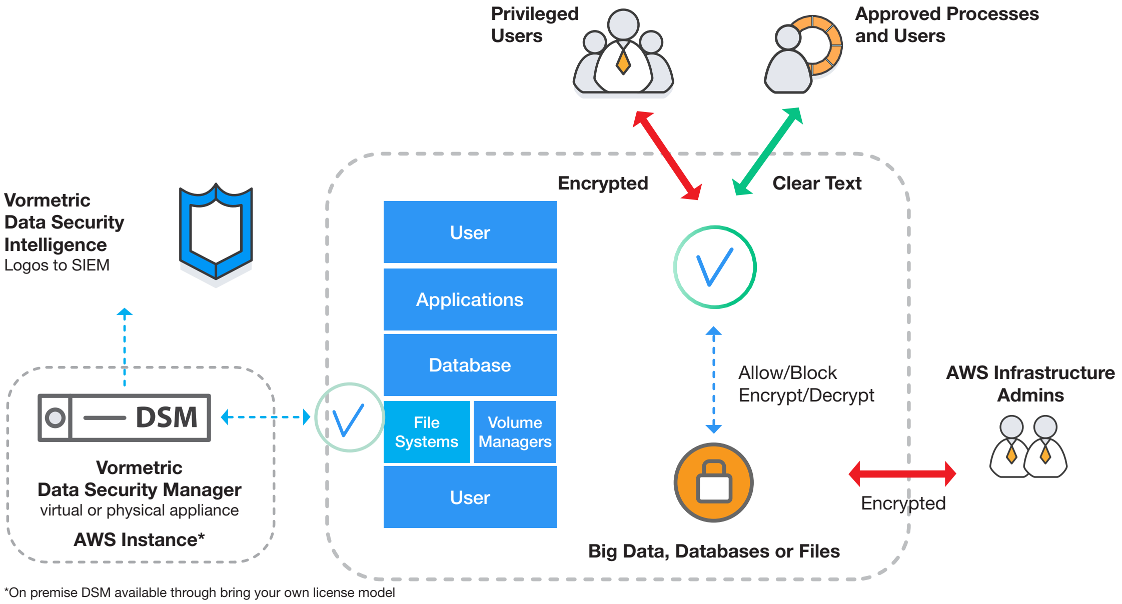
Privileged Users
Approved Processes and Users
Encrypted
Clear Text
Vormetric Data Security Intelligence
Logos to SIEM
User
Applications
Database
File Systems
Volume Managers
User
Allow/Block Encrypt/Decrypt
AWS Infrastructure Admins
DSM
Vormetric Data Security Manager
virtual or physical appliance
AWS Instance*
Encrypted
Big Data, Databases or Files
*On premise DSM available through bring your own license model

Fig. 3. Vormetric Transparent Encryption for AWS

For customers who are looking to retain as much control of their encryption keys as possible, Gemalto's SafeNet ProtectV is a high-availability encryption solution for securing sensitive and highly-regulated data that resides in Amazon EC2 instances and Amazon EBS volumes. SafeNet ProtectV and SafeNet Virtual KeySecure allow you to own your data and encryption keys—and prove it. ProtectV encrypts the entire machine instance and attached storage volumes. No machine instance is launched without proper authorization from ProtectV StartGuard pre-boot authentication.

By encrypting entire virtual machine instances and attached storage volumes, SafeNet ProtectV allows your organization to separate security administration duties, enforce granular controls and establish clear accountability with audit trails and detailed compliance reporting. With SafeNet ProtectV, data is safeguarded and completely isolated from AWS, other tenants, and any other unauthorized parties. Additionally, the solution ensures that no virtual machine instance can be launched without proper authorization from SafeNet ProtectV StartGuard pre-boot authentication. The solution ensures that your organization maintains complete ownership and control of not only your data, but also your encryption keys. Learn what customer ownership of data and encryption keys means and how the security of your data depends on it by visiting the customer-owned Keys in AWS.

Identity and Access Management

On top of the four key areas detailed above, identity and access control policies are another important component of any sound enterprise IT security strategy. Ensuring that users are identified by the system correctly and only given access to the appropriate resources are of critical importance. Several factors create a very dynamic business environment, making this a larger challenge than it has ever been, in the cloud and on-premises. For one, mergers and acquisitions are tasking IT departments with integrating disparate corporate IT environments securely and cost-effectively. Employees are also increasingly mobile, and tend to work from a variety of devices, meaning passwords and sensitive data are stored in more places than they've ever been and spend more time being transmitted through unsecure networks. The use of contract workers presents another set of challenges: organizations must on-board new users quickly, grant them access to the proper resources, then revoke that access after a given period. With AWS Marketplace, you can easily procure solutions from leading ISVs to help establish a secure, cost-effective, identity and access control practice on AWS.

Okta is an integrated identity and mobility management service that enables easy employee access and IT control for business apps. Okta simplifies and secures the internal administration of AWS users and access by connecting to existing infrastructure used to manage people like Active Directory. Okta also helps developers launch products quickly by offering pre-built authentication and user management. Another popular solution is OneLogin, a cloud Identity and Access Management offering that provides secure single sign-on (SSO), multi-factor authentication, integration with common directory infrastructures such as Active Directory, LDAP and Workday, automated user provisioning and de-provisioning, and more.

Conclusion

AWS Marketplace makes it simple, easy, and cost-effective for organizations to acquire security software from popular software vendors that helps them improve their security posture on AWS. These products complement the existing AWS services to help organizations deploy a comprehensive security architecture and achieve a more seamless experience across their AWS and on-premises environments.

Visit AWS Marketplace Security Solutions at https://aws.amazon.com/mp/security