Strengthening Your Cloud Security With Managed Threat Detection and Response

ensono® | OPERATE FOR TODAY.
OPTIMISE FOR TOMORROW.

As organizations ramp up their use of cloud computing for tier-one workloads and put more sensitive data into the cloud, more attention needs to be paid to security threats that could result in catastrophic data loss or regulatory compliance violations. Managed threat detection and response can help bolster cybersecurity defenses, particularly in cloud environments driven by industry-leading Amazon Web Services.

More and more enterprises are adopting a cloud-first approach to their most critical use cases and most strategic workloads, or at very least have made the cloud an equal partner with on-premises resources in an increasingly hybrid IT environment. The performance, utility, scalability and economics of public cloud platforms—such as Amazon Web Services—have encouraged organizations to make cloud a strategic and vital platform for developing, deploying and delivering business critical applications.

Just how dramatic is that transition to the cloud for mission-critical data? A recent research report pointed out that 90% of organizations categorize most of their cloud-resident data as "sensitive."[1] But this heavy reliance on cloud platforms for essential data has elevated every organization's awareness of, and sensitivity to, mounting cybersecurity threats. One of the most troublesome results is the potentially overwhelming number of security alerts and notifications security teams must contend with.

In fact, the numbers may stagger you. For instance, a survey of security executives in the financial services industry indicates that 37% of banks receive more than 200,000 security alerts each and every day.[2] How are security professionals—whether they work in an internal security operations center or supplement the in-house team as a managed security service provider—supposed to sort through that much noise to detect the most problematic issues to confront, respond to and remediate?

Against the backdrop of this new reality, it is reasonable to wonder why organizations spend so much money on security technologies if they lack the skills and/or staff to efficiently remediate true problems. This makes the notion of using a managed security service an extremely wise choice, especially given the expense and effort required to put in place and manage a robust, yet flexible, security operations center.

Cloud platform providers like AWS have dramatically expanded their cybersecurity posture, adding scores of new security features each year. AWS' widely acclaimed shared responsibility model for cybersecurity does a lot to give enterprises confidence and peace of mind. Amazon GuardDuty was such a service launched at AWS re:Invent 2017. GuardDuty enables significantly better monitoring of the security threat landscape the AWS account is exposed to and alerting when it has detected suspicious activity. It does this by using built-in advanced analytics and machine learning capability.

Cloud platform providers like AWS have dramatically expanded their cybersecurity posture, adding scores of new security features each year. AWS' widely acclaimed shared responsibility model for cybersecurity does a lot to give enterprises confidence and peace of mind.

1 "Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018

2 "Alert: Are There Too Many Cybersecurity Alerts?," American Banker, June 2017

Still, the sheer volume of alerts, the rapid introduction of zero-day threats and the increased sophistication and "team play" approach of cybercriminals means organizations need even more. And one of the best approaches organizations can take to expand AWS' native security functionality is to adopt a managed threat detection and response service from experienced, industry-proven partners.

How and why the AWS shared responsibility model works

It's been said that cybersecurity is a team sport, particularly in today's dynamic, fast-moving and highly complex threat environment. That's why, in an increasingly cloud-centric IT environment, it's important for cloud service providers and their customers to view cybersecurity as a shared responsibility.

AWS, in particular, takes this model extremely seriously, and works very closely with both its customers and third parties that provide security tools and services to ensure that data, applications and all digital assets are protected comprehensively and around the clock.

This shared responsibility model is based on the premise that AWS handles security "of the cloud" environment, while enterprise IT and security professionals pay close attention to security "in the cloud." In other words, AWS protects the infrastructure that runs its cloud services, including hardware, software, networking and facilities, while customers using AWS services handle such tasks as security configuration and management tasks—the extent of which is largely determined by which AWS services the client is using.

This model is the most fundamental tenet of cloud cybersecurity, particularly in hybrid environments where workloads are deployed and managed in some combination of cloud- and on-premises-based environments.

One of the key benefits of the shared responsibility model is the ability to blanket—with predictable and manageable overlap—the full spectrum of security risks and customer vulnerabilities.

Why a managed detection and response service is necessary

One of the key benefits of the shared responsibility model is the ability to blanket—with predictable and manageable overlap—the full spectrum of security risks and customer vulnerabilities. The ability to take AWS' native security functions like Amazon GuardDuty and combine them with third-party security tools and services like Alert Logic Cloud Defender to create an augmented security framework is essential in the cyber risk environments of today and tomorrow.

To fully leverage the shared responsibility model—and to acknowledge the resource limitations of their own internal security teams—many organizations have identified the need for a managed service to detect and respond to threats in real time, wherever the threat may attack. This is particularly important as organizations put tier-one workloads into a public cloud environment, where a data breach or another type of security incident could jeopardize an entire enterprise from a compliance, governance or legal

perspective. Internal monitoring tools, combined with AWS' significant native security features, have done a good job in plugging the gap. But the security threats are coming fast and furious, putting more pressure on enterprises to further augment the security features of their AWS environment.

Traditional managed service providers, for the most part, have failed to keep up with this rapid acceleration of threat vectors, exemplified by the enormous and often-overwhelming number of security alerts received at any time. In-house security professionals, along with managed security service provider teams, have struggled to triage, investigate and remediate new threats, many of them zero-day attacks.

Clearly, a new approach is necessary.

Defining the ideal managed threat detection and response solution

A managed threat detection and response service should address a number of key requirements—and organizations should look for these requirements when evaluating potential services.

These include:

- Designed to work with, and leverage, the native security functionality of AWS, the market-leading public cloud service provider.
- Detect threats and incidents in real time.
- Respond to those threats promptly, efficiently and thoroughly.
- Provide SOC-as-a-service functionality to monitor, analyze and provide actionable alerts, such as:
  - Monitoring and reviewing suspicious network traffic to identify zero-day attacks and reduce false positives.
  - Performing analysis and assessment.
- Align with public cloud and DevOps environments for quick solutions deployment through proven application programming interfaces.
- Operate and thrive in a hybrid IT environment, juggling the demands of both cloud- and on-premises-based security infrastructure and risk management.
- Enable centralized management across all deployment environments for comprehensive visibility, control and transparency.
- Support container security by collecting and analyzing network traffic to, from and between containers, to identify whether exploits are actively targeting container environments.

Traditional managed service providers, for the most part, have failed to keep up with this rapid acceleration of threat vectors…

The Ensono/Alert Logic/AWS partnership

Providing a seamless, agile and reliable managed service for threat detection and response requires the teamwork and collective expertise of three market leaders—AWS; Ensono, a leading AWS Audited Managed Service Partner; and Alert Logic, an experienced and trusted provider of security and compliance services in AWS environments.ecurity solutions purpose-built for AWS environments.

Together, the three organizations' technologies, services and security expertise represents a real-world embodiment of the shared responsibility model for cybersecurity. This integrated solution helps AWS customers stay ahead of the curve in detecting and responding to threats, without the need to take on major Capex and Opex costs to build out their internal security staffs and SOCs.

The service is built upon AWS's GuardDuty and Alert Logic's Cloud Defender, an integrated suite of security tools and compliance controls. It uses sophisticated machine learning algorithms to process and analyze event streams. This improves detection accuracy, because it is accomplished in conjunction with "human in the loop" supervision that trains and redeploys those algorithms for continuous improvement.

"Knowing and not doing is the same as not knowing." The most important step in your security posture is what you do with the information you've now been given. Ensono M.O., the company's proprietary service management platform, is integrated with Alert Logic, enabling 24/7 instantaneous raising of security incidents. Ensono's operations and support teams, with deep and wide experience and expertise in AWS, handle the actual response and remediation of threats.

"Knowing and not doing is the same as not knowing." The most important step in your security posture is what you do with the information you've now been given.

Summary

As the sheer amount of data—and the increasingly strategic nature of much of that data—balloons year after year, organizations need to step up their game when it comes to detecting and responding to threats. But many enterprises lack the in-house resources, expertise or flexibility necessary to fully confront current and future security threats, making managed threat detection and response—especially in the increasingly utilized AWS cloud environment—an essential service.

Leveraging its proven partnership with and expertise in AWS, Ensono has developed a forward-looking managed threat and detection service designed to enhance AWS' clients existing security posture, particularly in increasingly hybrid IT environments.

By combining the native security and third-party tools used for AWS with its knowledge of AWS environments and security challenges, Ensono offers enterprises a managed threat detection and response service that takes existing managed security services to new levels of comprehensiveness, flexibility and responsiveness. Instead of devoting substantial financial and staffing resources to building out SOCs, enterprises can leverage the end-to-end solution to detect and respond to fast-emerging security threats in real time.

https://www.ensono.com/cloud/managed-aws/automation