ANOMALIX

ANOMALIX
WHITE PAPER

Building a Business Case for Public Cloud Threat Protection



Building a Business Casefor Public Cloud Threat Protection

Around the clock and around the globe on a daily basis, bots, malware and offensive security software tools are being used by hackers in an effort to break into public cloud computing systems. Microsoft's cloud computing operations alone detects roughly 1.5 million attempts a day to compromise and access its Azure cloud platform1.

When malicious actors are able to breach an organization's defenses, the business losses include customer turnover, business disruption, system downtime and a damaged brand reputation, all factors that have a direct impact on a business's bottom line.

According to the IBM Security and Ponemon Institute 2019 Cost of a Data Breach Report2, the average cost of lost business for organizations was $1.42 million, representing 36 percent of the total average cost of a data breach which was $3.92 million. The IBM study also found that breaches caused abnormal customer turnover of 3.9 percent with data breaches originating from a malicious cyber attack being the most expensive.

Having cyber-threat risk mitigation and threat response business processes in place increases an organization's ability to respond effectively to a data breach or network intrusion and is strengthened by having an incident response (IR) team and plan. Organizations that conducted IR plan testing had an average total breach cost that was $1.23 million less than organizations that had no incident response team or did not test their incident response plan at all, according to IBM.

From a technology standpoint, IT investments in encryption, business continuity management practices, DevSecOps that integrate security into the internal software development process, and threat intelligence sharing all were found to be major breach cost mitigations as well.

Making business investments in both cloud security business processes and cloud security technologies themselves also helps organizations meet government compliance requirements such as the General Data Protection Regulation (GDPR) to match cloud service provider (CSP) compliance requirements.

1. https://news.microsoft.com/stories/cloud-security/
2. https://www.ibm.com/security/data-breach

To manage cyber risk compliance in the cloud, organizations must establish both governance and supporting business processes combined with the right cloud security technologies. However, executive management must not rely solely on IT teams to protect and defend their business, they must also take an active role in managing cybersecurity resources and allocating budgets to protect business assets against cyber attacks.[3]

Shared Security in the Cloud

Cloud computing, as defined by the US National Institute of Standards and Technology or NIST, is an online computing delivery model that includes three primary cloud services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Attributes of cloud computing include an environment where users can provision services on their own, extensive network access, resource pooling, and elasticity where IT resources can expand or contract on an as needed basis.

Security in the cloud has traditionally been the responsibility of both cloud providers and the organizations that utilize cloud computing and storage resources. Amazon Web Services (AWS), for instance, calls this concept the Shared Responsibility Model where security and compliance is owned by both AWS and the customer.

According to AWS, customers assume responsibility and management of cloud operating systems and security, third-party application software and the configuration of AWS firewalls and identity management and access while AWS provides security for the underlying infrastructure and network.[4]

AWS cloud services also under customer control that require security through identity and access management include AWS Infrastructure as a Service (IaaS) resources such as Amazon EC2, Amazon VPC, and Amazon S3. From an Amazon perspective, AWSnative network monitoring tools offer a line of defense to detect unusual or unauthorized activities and conditions, server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts but only at ingress and egress communication points.

The problem with the shared security model, however, is the everchanging cloud security threat landscape. IT security staff is in short supply and organizations must always be vigilant about new threats, vulnerabilities and compliance requirements beyond basic cloud infrastructure security.

3 https://assets.kpmg/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf

4 https://aws.amazon.com/compliance/shared-responsibility-model/

Protecting public cloud environments is unlike on-premises security where there's a physical network boundary that acts as a safeguard for known network perimeters. Instead, cloud application migration and new development is decentralized and fraught with risk of accidental data exposure, leakage and credential misuse.

Because public clouds afford increased agility by allowing users to create, modify and scale infrastructure such as storage, network and computing resources with any IT or Security oversight, the risk of accidental misconfiguration is also dramatically higher while the threat vector for malicious activity is easily exploitable.

The latest Cloud Security Alliance (CSA) report "Top Threats to Cloud Computing: The Egregious Eleven" highlights configuration and authentication cloud security risks as the top threats today versus vulnerabilities and malware cited in past research. 1The new CSA research also found that data breaches, misconfiguration and inadequate change controls, lack of cloud security architecture and strategy, insufficient identity, credential, access and key management and account hijacking as top cloud security threats.

"The complexity of cloud can be the perfect place for attackers to hide, offering concealment as a launchpad for further harm. Unawareness of the threats, risks and vulnerabilities makes it more challenging to protect organizations from data loss," said John Yeoh, Global Vice President/Research for the CSA.

This complexity challenge combined with vast amounts of big data generated by hacking attempts and online malicious activity means that organizations must augment their defences against cyber threats with more than the standard tools and technologies offered by public cloud providers today.

Leveraging AI and Machine Learning for Cloud Security

With cloud security complexity and threats on the rise, organizations must always keep up with not only threat intelligence but also the tools and technologies that will help them cope with growing and constantly changing cloud security and compliance requirements.

The most advanced technologies employed to defend against cyber attacks today come in the form of Artificial Intelligence and Machine Learning tools that leverage Big Data. With Big Data, very large data sets are analyzed to reveal patterns and trends that may not have been surfaced without the aid of computers.

5. https://cloudsecurityalliance.org/articles/csa-releases-new-research-topthreats-to-cloud-computing-egregious-eleven/

Artificial Intelligence (AI) employs software algorithms and computers to mimic human intelligence. In addition to cybersecurity, AI use cases include image analysis, speech recognition, and natural language processing and natural language generation. AI algorithms "learn" from large data sets and produce insights such as with text classification, reason or self-correction.

Machine learning is a subset of AI and method of data analysis that automates and simultates model building to iteratively learn and improve from large data sets without being programmed.

According to Ann Johnson, Corporate Vice President, Cybersecurity Solutions Group at Microsoft, "machine learning engines that are built to scale and augmented with AI can evolve and learn in real-time and have the capability to build models that can work in milliseconds."

These machine learning models can be used to accurately identify malicious content or malware in real time that non-machine learning based cyber threat mitigation technology may not pick up.

Analyst firm Gartner believes that organizations using Machine Learning for security "should focus on improved outcomes and specific use cases when evaluating the suitability of ML-based security tools. ML approaches are most suitable in situations where traditional methods are intractable, inefficient or simply impossible, and where relevant data of high quality is sufficiently available."

The advantage of leveraging machine learning and AI for cybersecurity in the cloud is that the tools are usually cloud-native applications that can be easily integrated into cloud platforms and perform security tasks alongside organizational workflows to protect and defend resources against attackers.

Getting Started

Using machine learning and AI for public cloud threat protection is a process of determining what key resources should be protected and what tools to use, whether it's a third-party platform or machine learning tools provided by a cloud provider such as Amazon, Microsoft or Google.

According to Gartner's PPDR model[6], all security tasks can be divided into five categories: prediction; prevention; detection; response and monitoring. From a technical perspective, the following areas must also be considered: the network for network traffic analysis and intrusion detection; endpoint protection; application firewalls; users and identity management; and workflows or process

for fraud detection. Machine learning is applicable to all of these categories and can accelerate threat protection in the cloud. Identifying specific risks to data, hardware and cloud resources will also help identify vulnerabilities and where investment in time and resources is needed with present cyber risks and potential threats that may arise, be considered and planned for.

Identifying specific risks to data, hardware and cloud resources will also help identify vulnerabilities and where investment in time and resources is needed with present cyber risks and potential threats that may arise, be considered and planned for.

After cyber risks have been identified, choosing the right machine learning tools and platforms to mitigate cyber threats is critical as well as their integration into the organization's overall cloud workflow.

Developing proprietary or in-house machine learning algorithms and workflows for cyber-threat protection can be costly and requires experts in data science that know what data should be analyzed and what threats must be monitored to protect cloud resources and workflows. Therefore, organizations should consider third-party machine-learning enabled cybersecurity platforms that accelerate the adoption of machine learning and AI-enabled cybersecurity tools.

Public cloud threat protection is a critical piece of any IT security and business strategy today and many IT security managers already accept that data breaches are inevitable and plan for it.

The new issues found by the CSA portends a technology environment in which IT professionals are rapidly migrating workloads to the cloud but are finding that although public cloud infrastructures are becoming more secure, threat actors and malware are also becoming more sophisticated necessitating more advanced technologies such as machine learning and AI for cybersecurity.

Securing Executive Buy-in for Public Cloud Security

The business case for public cloud threat protection is clear: the cost of a data breach can be extremely high, not only from a technology point of view but also an operational, compliance, brand marketing and customer viewpoint as well. So how does a Chief Information Security Office (CISO) gain program support and buy-in from executive management?

6. https://www.gartner.com/document/3286317

The challenge of a CISO is convincing executive teams that cybersecurity programs and budgets are critical to protecting a business's revenue and operational priorities.

One CISO from a medium to large US state commented, "From what I have seen the issue is not necessarily that the money is not there, typically the issue is that security almost always competes with other operational priorities."[1]

CISO's should position the importance for IT security programs with third-party data on breach cost risks and business impacts, threat intelligence from public and private sources, internal and public cloud analytics that state the need for specific cloud security programs, and even use outside opinions from security and compliance auditors that analyze systems for organizational security holes and risks.

For cybersecurity programs and budgets to be treated as a critical business function they must be presented to executives as if they were similar in priority to functions like marketing, sales, product development or operations that align with key overall business goals and objectives.

Conclusion

Anomalix leverages machine learning and AI to create solutions that allow organizations to establish an omni-channel view of identity information that improves sales and marketing campaigns; enhances security administration and simplifies governance compliance and reporting.

The IdGeniusTotal Cloud Protection Platform, Anomalix's next generation AI and machine learning platform, can identify, correlate, monitor and audit security and compliance activity across public clouds including Amazon Web Services, Microsoft Azure, and Google Cloud Platform to govern security and enable security operations.

As a cloud native Software-as-a-Service (SaaS) solution, IdGenius addresses cloud security scenarios relating to visibility, security governance and compliance assurance including visibility and management of all cloud resources, configuration and access management, identity and access governance, host threat and vulnerability management as well as network threat visibility and remediation.

The business benefits derived from IdGenius include reduced financial risk due to security breaches, reduced cost of compliance reporting as well as reduced security operations associated with manual and redundant activity. And from a compliance perspective, organizations can reduce time and resources related to meeting compliance mandates such as NIST, PCI, SOC 2, HIPAA and GDPR.



Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144