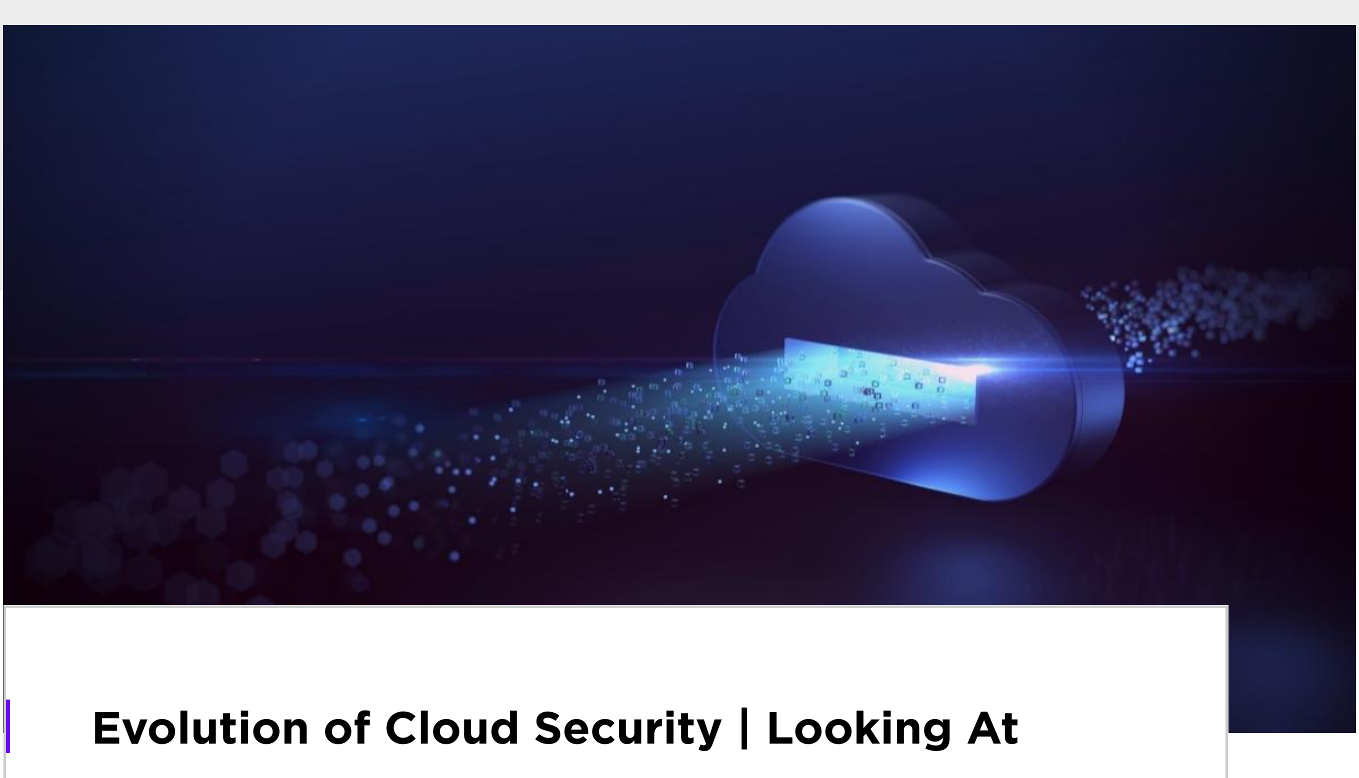


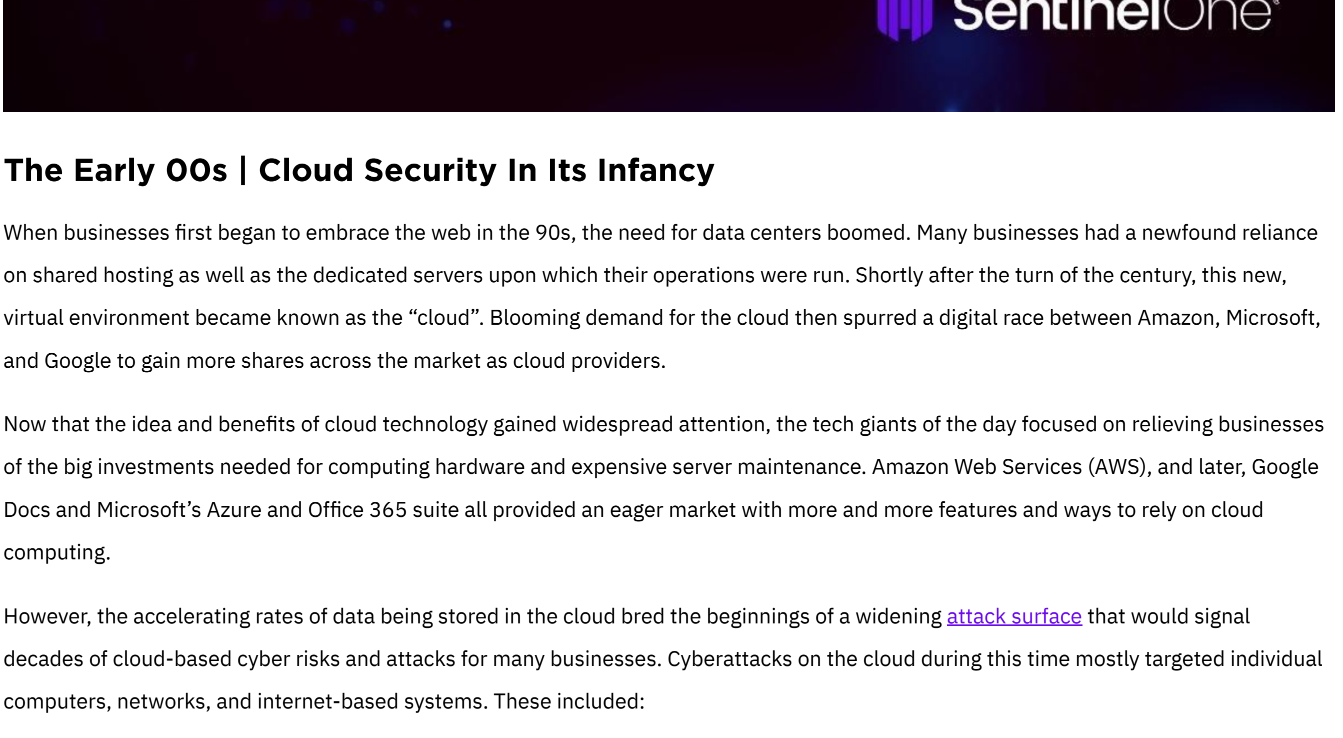
Evolution of Cloud Security | Looking At Cloud Posture Management Throughout the Decades

May 24, 2023
by SentinelOne

When cloud computing saw its earliest waves of adoption, businesses only had to decide whether or not they wanted to adopt it. The notion of cloud security in these first few years came as a secondary consideration. Though cloud computing has undergone many improvements since it made a splash following the advent of the World Wide Web, the challenge of cloud security has only become more complex and the need for it more acute.

Today's hyperconnected world sees the cloud surface face a variety of risks from ransomware and supply chain attacks to insider threats and misconfigurations. As more businesses have moved their operations and sensitive data to the cloud, securing this environment against developing threats continues to be an ever-changing challenge for leaders.

This post walks through a timeline of how cloud security has grown over recent years to combat new and upcoming risks associated with its use. Following this timeline, security leaders can implement the latest in cloud security based on their own unique business requirements.



The Early 00s | Cloud Security In Its Infancy

When businesses first began to embrace the web in the 90s, the need for data centers boomed. Many businesses had a newfound reliance on shared hosting as well as the dedicated servers upon which their operations were run. Shortly after the turn of the century, this new, virtual environment became known as the "cloud". Blooming demand for the cloud then spurred a digital race between Amazon, Microsoft, and Google to gain more shares across the market as cloud providers.

Now that the idea and benefits of cloud technology gained widespread attention, the tech giants of the day focused on relieving businesses of the big investments needed for computing hardware and expensive server maintenance. Amazon Web Services (AWS), and later, Google Docs and Microsoft's Azure and Office 365 suite all provided an eager market with more and more features and ways to rely on cloud computing.

However, the accelerating rates of data being stored in the cloud bred the beginnings of a widening attack surface that would signal decades of cloud-based cyber risks and attacks for many businesses. Cyberattacks on the cloud during this time mostly targeted individual computers, networks, and internet-based systems. These included:

- Malware Attacks – Malicious software, such as viruses, worms, and trojans, were prevalent in this decade. These attacks often spread through email attachments, infected software, or compromised websites and posed significant risks to individual computer systems connected to the internet and cloud.
- Network Exploits – Exploits targeting vulnerabilities in network protocols and services were common in the 1990s. Attackers would exploit weaknesses in network infrastructure, operating systems, or software applications to gain unauthorized access, perform privilege escalation, or conduct data exfiltration.
- Social Engineering Attacks – Social engineering attacks, such as phishing and impersonation, were prevalent throughout the 90s. Attackers would manipulate users through deceptive tactics to trick them into revealing sensitive information, such as login credentials or financial details.

Cloud security, in this decade, thus put their focus on network security and access management. Dedicated attacks targeting cloud environments became more prominent in the following decades as cloud computing gained traction across various industries.

The Roaring 2000s | The Millennial Age of Cloud Security

In the 2000s, the cybersecurity landscape continued to evolve rapidly, and the specific types and sophistication of attacks targeting cloud environments expanded. Cloud computing was becoming more popular, and cyberattacks specifically targeting cloud environments started to emerge. This decade marked a new stage of cloud security challenges directly proportional to the significant increase in the adoption of cloud.

While past its infancy, cloud computing was not as prevalent as it is now, and many businesses still relied on traditional on-premises infrastructure for their computing needs. Consequently, the specific security concerns related to cloud environments were not widely discussed or understood.

Cloud security measures in the 2000s were relatively basic compared to today's standards. To secure network connections and protect data in transit, security measures for cloud primarily focused on Virtual Private Networks (VPNs); commonly used to establish secure connections between on-premises infrastructure and the cloud provider's network. Further, organizations relied heavily on traditional security technologies that were adapted for these new cloud environments. Firewalls, intrusion detection systems, and access control mechanisms were employed to safeguard network traffic and protect against unauthorized access.

The 2000s also saw few industry-specific compliance standards and regulations explicitly addressing cloud security. Since compliance requirements were generally focused on traditional on-premises environments, many businesses had to find their own way, testing out combinations of security measures through trial and errors since there were no standardized cloud security best practices.

Cloud security at the beginning of the millennium was largely characterized by limited control and visibility and heavily reliant on the security measures implemented by the cloud service providers. In many cases, customers had limited control over the underlying infrastructure and had to trust the provider's security practices and infrastructure protection. This also meant that customers had limited visibility over their cloud environments, adding to the challenge of monitoring and managing security incidents and vulnerabilities across the cloud infrastructure.

The 2010s | Cloud Security Gaining A Global Momentum

In the 2010s, cloud security experienced significant advancements as cloud computing matured and became a staple of many businesses' infrastructures. In turn, attacks on the cloud surface had also evolved into much more sophisticated and frequent events.

Data breaches occupied many news headlines in the 2010s, with attackers targeting cloud environments for cryptojacking or to gain unauthorized access to sensitive data. Many companies fell victim to compromises that leveraged stolen credentials, misconfigurations, and overly permissive identities. A lack of visibility into the cloud surface meant breaches could go undiscovered for extended periods.

Many high-profile breaches exposed large amounts of sensitive data stored in the cloud including:

- 150 million breached records from Adobe found on a hacker site in 2013,
- The Apple iCloud breach in 2014 resulting in a mass amount of private photos leaked, and
- 300 million compromised Facebook accounts found listed for sale on the dark web in 2019.
- 100 million credit card customers affected by a breach at Capital One in 2019.

The severity of cloud-based attacks lead to increased awareness of the importance of cloud security. Organizations recognized the need to secure their cloud environments and began implementing specific security measures. As cloud adoption continued to grow, so did the motivation for attackers to exploit cloud-based infrastructure and services. Cloud providers and organizations responded by increasing their focus on cloud security practices, implementing stronger security controls, and raising awareness for globally recognized countermeasures.

Enter the Cloud Shared Responsibility Model. Introduced by cloud service providers (CSPs) to clarify the division of security responsibilities between the CSP and the customers utilizing their services, the model gained significant prominence and formal recognition in the 2010s.

During this period, major providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) began emphasizing the shared responsibility model as part of their cloud service offerings. They defined the respective security responsibilities of the provider and the customer, outlining the areas for which each party was accountable. This model helped a generation of businesses better understand their role in cloud security and enabled them to implement appropriate security measures to protect their assets.

This decade also popularized the services of cloud access security brokers (CASBs); a term coined by Gartner in 2012 and defined as:

> "On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on."

To help businesses navigate and address the changing cloud security landscape, CASBs emerged as a critical security solution for organizations, acting as intermediaries between cloud service providers and consumers. Their main goals were to provide visibility, control, and security enforcement across cloud environments through services such as data loss prevention (DLP), cloud application discovery, encryption and tokenization, compliance, and governance.

The 2010s saw the emergence of Cloud Security Posture Management solutions and was also the starting point for improved compliance and standardization for the use of cloud in modern businesses. Industry-specific compliance standards and regulations began to address cloud security concerns more explicitly. Frameworks such as the Cloud Security Alliance (CSA) Cloud Controls Matrix and both ISO 27017 and ISO 27018 now sought to provide guidelines for cloud security best practices.

The 2020s | Paving the Future of Cloud Security

In current times, cloud technology has laid down a foundation for a modern, digital means of collaboration and operations on a large scale. Especially since the COVID-19 pandemic and the rise of remote workforces, more businesses than ever before are moving towards hybrid or complete cloud environments.

While cloud technologies, services, and applications are mature and commonly used across all industry verticals, security leaders are still facing challenges of securing this surface and meeting new and developing threats. Modern businesses need a cloud posture management strategy to effectively manage and secure their cloud environments. This involves several key elements to ensure agile and effective protection against today's cloud-based risks.

Cloud Security Posture Management (CSPM)

CSPM solutions have now gained a large amount of traction, enabling organizations to continuously assess and monitor their cloud environments for security risks and compliance. CSPM tools offer visibility into misconfigurations, vulnerabilities, and compliance violations across cloud resources, helping organizations maintain a secure posture.

An essential element of CSPM is cloud attack surface management. Since cloud environments introduce unique security challenges, a cloud posture management strategy helps businesses assess and mitigate risks. It allows organizations to establish and enforce consistent security controls, monitor for vulnerabilities, misconfigurations, and potential threats, and respond to security incidents in a timely manner. A robust strategy enhances the overall security posture of the cloud infrastructure, applications, and data.

CSPM also encompasses what's called the "shift-left" paradigm, a cloud security practice that integrates security measures earlier in the software development and deployment lifecycle. Rather than implementing security as a separate and downstream process, the shift left addresses vulnerabilities and risks at the earliest possible stage, reducing the likelihood of security issues and improving overall security posture. It emphasizes the proactive inclusion of security practices and controls from the initial stages of development, rather than addressing security as an afterthought or at later stages.

In addition, Cloud Infrastructure Entitlement Management (CIEM) tools have emerged to help organizations manage access entitlements across multicloud environments, helping to reduce the risks associated with excessive permissions.

Kubernetes Security Posture Management (KSPM)

As cloud adoption rates continue to increase, many businesses have turned to Kubernetes (K8s) to help orchestrate and automate the deployment of containerized applications and services. K8s has risen as a popular choice for many security teams that leverage its mechanism for reliable container image build, deployment, and rollback, which ensures consistency across deployment, testing, and product.

To better assess, monitor and maintain the security of k8s, teams often use the Kubernetes Security Posture Management (KSPM) framework to evaluate and enhance the security posture of Kubernetes clusters, nodes, and the applications running on them. It involves a combination of various activities including risk assessments of the k8 deployment, configuration management for the clusters, image security, network security, pod security, and continuous monitoring of the Kubernetes API server to detect suspicious or malicious behavior.

Additionally, Cloud Workload Protection Platform (CWPPs) and runtime security helps protect workloads against active threats once the containers have been deployed. Implementing K8s runtime security tools protects businesses from malware that may be hidden in container images, privilege escalation attacks exploiting bugs in containers, gaps in access control policies, or unauthorized access to sensitive information that running containers can read.

Zero Trust Architecture

The zero trust security model has gained prominence in the 2020s. It emphasizes the principle of "trust no one" and requires authentication, authorization, and continuous monitoring for all users, devices, and applications, regardless of their location or network boundaries. Zero trust architecture helps mitigate the risk of unauthorized access and lateral movement within cloud environments.

Implementing the zero trust security model means taking a proactive and robust approach to protecting cloud environments from evolving cyber threats. Compared to traditional network security models, which relied on perimeter-based defenses and assuming that everything inside the network is trusted, zero trust architecture:

- Eliminates the concept of implicit trust to minimize the risk of unauthorized access, data breaches, and lateral movement within the infrastructure.
- Makes identity the cornerstone of security by focusing on strong authentication mechanisms.
- Enables fine-grained access controls, allowing organizations to enforce access policies based on various contextual factors such as user roles, device health, location, and behavior.
- Leverages technologies like user and entity behavior analytics (UEBA), threat intelligence, and real-time monitoring to detect anomalous behavior, potential threats, and security incidents.
- Promotes the use of encryption and data protection mechanisms to secure data within cloud environments, using end-to-end encryption for data in transit and at rest to protect sensitive information from unauthorized access or interception.

Cloud-Native Security Tools, Continuous Monitoring & Incident Response

Cloud-native security solutions continue to evolve, providing specialized tools designed specifically for cloud environments. These tools offer features such as cloud workload protection, container security, serverless security, and cloud data protection. Many businesses leverage cloud-native tools to address the unique challenges of modern cloud deployments in a way that is scalable, effective, and streamlined to work in harmony with existing infrastructure.

Cloud-native security tools often leverage automation and orchestration capabilities provided by cloud platforms. Based on predefined templates or dynamically changing conditions, they can automatically provision and configure security controls, policies, and rules to reduce manual effort. Since many cloud breaches are the result of human errors, such tools can help security teams deploy consistent and up-to-date security configurations across their businesses' cloud resources.

Continuous monitoring of cloud environments is essential for early threat detection and prompt incident response. Cloud-native security tools enable centralized monitoring and correlation of security events across cloud and on-premises infrastructure. As they are designed to detect and mitigate cloud-specific threats and attack vectors, cloud-native solutions can cater to characteristics of cloud environments, such as virtualization, containerization, and serverless computing, identifying the specific threats targeting these technologies.

Cloud Security Intelligence Using AI & ML

The use of advanced analytics, threat intelligence, artificial intelligence (AI) and machine learning (ML) is on the rise in cloud security. These technologies enable the detection of sophisticated threats, identification of abnormal behavior, and proactive threat hunting to mitigate potential risks.

Both AI and ML are needed to accelerate the quick decision-making process needed to identify and respond to advanced cyber threats and a fast-moving threat landscape. Businesses that adopt AI and ML algorithms can analyze vast amounts of data and identify patterns indicative of cyber threats. They can detect and classify known malware, phishing attempts, and other malicious activities within cloud environments.

By analyzing factors such as system configurations, vulnerabilities, threat intelligence feeds, and historical data, the algorithms allow security teams to prioritize security risks based on their severity and potential impact. This means resources can be focused on addressing the most critical vulnerabilities or threats within the cloud infrastructure.

From a long-term perspective, the adoption of AI and ML in day-to-day operations enable security leaders to build a strong cloud security posture through security policy creation and enforcement, ensuring that policies adapt to changing cloud environments and truly address emerging threats.

Conclusion

Securing the cloud is now an essential part of a modern enterprise's approach to risk and cyber threat management. By understanding how the cloud surface has evolved, businesses can better evaluate where they are on this development path and where they are headed. Business leaders can use this understanding to ensure that the organization's security posture includes a robust plan for defending and protecting cloud assets. By prioritizing and investing in cloud security, enterprises can continue to safeguard their organizations against developing threats and build a strong foundation for secure and sustainable growth.

How SentinelOne's AI-Powered Platform Supports Cloud Security Strategies

SentinelOne focuses on acting faster and smarter through AI-powered prevention and autonomous detection and response. SentinelOne's Singularity™ Cloud ensures organizations get the right security in place to continue operating in their cloud infrastructures safely.

Learn more about how Singularity helps organizations autonomously prevent, detect, and recover from threats in real time by contacting us or requesting a demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Detecting a Rogue Domain Controller – DCShadow Attack
- Avoiding the Storm | How to Protect Cloud Infrastructure from Insider Threats
- Surviving the Storm | Defending Against Cloud Misconfigurations, Vulnerabilities, and Insider Threats
- Defending Cloud-Based Workloads: A Guide to Kubernetes Security
- Accelerating Your Cloud Security with Workload Protection
- EDR for Cloud Workloads Running on AWS Graviton