E-BOOK

The Evolution of Cloud Security

From Prevention to Detection and Response

sysdig

Contents

03 Introduction

04 The endpoint security odyssey through time

07 The cloud attack surface

08 History repeats: Prevention or bust

09 Detection and response: Beyond the cloud's front lines

11 Bring on the cloud security platform consolidation

12 The value of purpose-built cloud security

14 Conclusion

Introduction

Cloud security has undergone a profound evolution. In recent years, we've witnessed a transformation that mirrors a familiar history — one that might give seasoned security professionals a sense of déjà vu.

Remember the early days of endpoint security? Initial efforts were heavily focused on protection-only measures. It didn't take long before we realized that wasn't enough, and endpoint security strategies expanded to incorporate detection and response measures to adapt to a growing array of threats. Today, we find ourselves in a similar cycle with cloud security. We're learning the same hard lessons, only this time on a much larger and more complex stage.

This eBook embarks on a journey through cloud security, drawing parallels to the historical development of endpoint security. By examining this historical repetition, we'll uncover crucial insights and, importantly, delve into what steps security leaders should take to avoid past mistakes.

Let's learn from history and pave the way for a more secure cloud future.

The endpoint security odyssey through time

To understand what's happening in the cloud, we need a short refresher on the evolution of endpoint security. The journey from the first antivirus products to today's endpoint protection platforms (EPPs) started in the 1980s and went through a wild ride of progression and consolidation over the past 40 years.

Protection

Antivirus

In the early days, computer viruses wreaked havoc on unsuspecting systems. By the early 2000s, viruses had gone global, but antivirus (AV) software saved the day. AV products, armed with signature-based methods, were designed to detect and vanquish known viruses, effectively safeguarding systems for a time.

Better Protection

Next-Generation Antivirus

As malware evolved, traditional AV solutions struggled to keep up. The rise of polymorphic malware, which could change its code to evade detection, rendered signature-based protection increasingly ineffective. This led to the development of next-generation antivirus (NGAV). NGAV solutions moved beyond simple signatures, incorporating advanced techniques like machine learning and behavior analysis to detect and block threats before they could succeed. Still, the primary focus remained on protection.

Detection and Response

Endpoint Detection and Response

Despite the NGAV advancements, attacks continued to succeed. Once inside a network, there was no way to detect them, leading to long dwell times and delayed response efforts. This security gap gave rise to endpoint detection and response (EDR) solutions. EDR introduced capabilities for monitoring, detecting, and responding to threats in real time, complementing the NGAV protective measures.

Platform Consolidation

Modern Endpoint Protection Platforms (EPP)

As the cybersecurity landscape evolved, so did the need for more integrated solutions. The industry began to consolidate capabilities into unified platforms. Largely due to the MITRE ATT&CK evaluations, the concept of endpoint protection platforms (EPPs) was redefined to enhance the ability to detect adversary behavior comprehensively. Modern EPPs, sometimes referred to as consolidated EDR, encompass protection, detection, and response in a single, cohesive solution. These platforms represent the culmination of four decades of endpoint security evolution, providing robust defenses against sophisticated threats.

Now, let's shift our focus to the cloud and explore how it has rapidly evolved, drawing some fascinating parallels to the history of endpoint security.

The cloud attack surface

The journey with cloud security began with a stark realization: The cloud is its own beast as a new attack surface.

As businesses migrated to the cloud, the attack surface became increasingly complex. What started as a simple way to offload data and applications turned into a sprawling, intricate web of services and connections. This digital landscape, while offering unparalleled flexibility and scalability, also presented new and unique security risks.

We started hearing about cryptojacking and cloud data breaches. Suddenly, news of stolen credentials, misconfigurations, and overly permissioned identities flooded our feeds. Major breaches made headlines — Adobe, Facebook, CapitalOne — each incident starkly reminding us of the skyrocketing cyber attacks in the cloud. Attacks focused on supply chain compromise, and the abuse of human and machine identities, became alarmingly common.

Yet, in the midst of this digital chaos, organizations found themselves with limited visibility into their cloud environments. Breaches could go undetected for days, sometimes even weeks, as attackers roamed freely, siphoning off data. The speed and complexity of cloud attacks far outpaced traditional on-premises cyber threats, leaving defenders scrambling to keep up.

It became clear that cloud attacks were not only fast but also required a different approach to security. Simply relying on traditional EPP tools as a "good enough" solution for cloud security was far from sufficient (more on that later). Thankfully, the cybersecurity industry began to adapt. Organizations started adopting stronger cloud security practices.

Phrases like "shift left" and "shield right" entered the lexicon, emphasizing the need for proactive and reactive measures. We began hearing about cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), cloud workload protection platforms (CWPP), and container security — all terms that signaled a shift towards more tailored cloud security strategies.

History repeats: Prevention or bust

Just like the early days of endpoint security, the initial approach to cloud security was all about prevention. The goal was to build a cloud fortress — one that could repel attackers before they even had a chance to breach the walls.

Cloud threat prevention began with cloud security posture management (CSPM) and cloud infrastructure entitlement management (CIEM). These tools were designed to enforce security controls and monitor for vulnerabilities, misconfigurations, and potential threats.

Cloud security posture management is like having a proactive security consultant always on the job. It ensures that security is baked into every layer of the cloud infrastructure, identifying weaknesses before they can be exploited. With CSPM, teams can enforce security policies across their cloud environments, making sure that every access point and vulnerability is addressed.

Meanwhile, CIEM plays the role of the gatekeeper, managing who is allowed to have access to what. It keeps a close eye on permissions, ensuring that no identity — human or machine — has more access than necessary. By monitoring and adjusting entitlements, CIEM helps prevent unauthorized access and potential breaches.

Undeniably, when these cloud threat protection controls were first introduced, they were a game-changer. However, the cloud's complex environment required more. The next stage in the cloud security journey would reveal that prevention, while essential, was only one piece of the puzzle.

Detection and response: Beyond the cloud’s front lines

Spoiler alert: Prevention measures weren’t (and aren’t) enough for the cloud. Cloud attacks unfold with breathtaking speed — sometimes within minutes, making the difference between containment and catastrophic damage. And the attacks are often successful at gaining a foothold across an organization’s cloud footprint. In fact, 39% of breaches span multiple cloud environments, racking up an eye-watering average cost of $4.75 million.[1]

Just like we saw in the historical progression of endpoint security, the cloud demanded the ability to detect and respond to threats at lightning speed. However, the initial road to achieving this took a scenic detour through some trial-and-error territory. While cloud detection and response (CDR) capabilities were evolving as part of cloud-native application protection platform (CNAPP) solutions, many organizations opted for a makeshift cloud security strategy by expanding their current EDR solutions to cover their cloud environments. We promised to point out historical mistakes not to repeat, and this is one of those pitfalls you’ll definitely want to sidestep.

[1] IBM. Cost of a Data Breach Report 2023.

Why isn't EDR the right fit for your cloud security?

Imagine navigating a maze blindfolded — EDR faces a similar challenge in the cloud. It lacks crucial visibility into elements like containers and Kubernetes, which is essential for spotting and tackling cloud-native threats. While EDR excels at pinpointing threats on the host level, it often misses the bigger picture of the cloud environment. This creates significant gaps in cloud detection and response capabilities.

And the EDR approach to detecting attacks just isn't fast enough for the cloud. Cloud environments move at breakneck speed where the average lifespan of a container is just five minutes — shorter than your morning coffee break. Imagine threats exploiting weaknesses in mere minutes, rapidly advancing attacks for maximum impact. In an attack scenario, if the analyst does not see the detection within those five minutes, they will be unable to understand the scope of the event beyond just the alert.

Because incidents in the cloud are as complex and multidimensional as a tangled web, EDR can't connect the dots across various domains to meet the essential 555 Benchmark for Cloud Detection and Response: five seconds for detection, five minutes for correlation and triaging, and five minutes for response.

CDR: The reliable path for cloud detection and response

The unique nature of the cloud demands fit-for-purpose detection and response capabilities, and thankfully, the security market evolved to deliver just that with CDR. Organizations that made the inadvertent detour with EDR for their cloud needs are now course-correcting towards these purpose-built CDR capabilities.

Integrated within a CNAPP, CDR offers advanced detection and response across a wide array of cloud technologies: containers, Kubernetes, serverless computing, cloud logs and trails, and both Linux and Windows servers.

And CDR isn't just about keeping an eye on things; it's about having a full-scale security operation that can detect, investigate, and respond to threats faster than a hacker can say "breach." With end-to-end capabilities, CDR ensures that security teams can match the rapid pace of cloud environments, meeting the 555 Benchmark to tackle cloud threats head-on and in real time.

Bring on the cloud security platform consolidation

We’re at the final chapter of our history-repeat-story. This is where the endpoint market smartly consolidated protection, detection, and response into a single endpoint protection platform (EPP). Taking a cue from this playbook, the cloud security market strategically consolidated its arsenal of tools into CNAPP.

This milestone arms organizations with true cloud-centric security tooling that ensures security teams have all of the following:

- **Coverage across multi-domain and multi-cloud environments** with comprehensive protection, no matter how sprawling or complex your cloud footprint is.
- **Speed to detect, investigate, and respond in fewer than 10 minutes,** keeping you ahead of the attack curve and shutting down threats before they can do damage.
- **Context to effectively respond to threats,** giving you the depth of information and insight needed to take decisive action.
- **A unified solution for cross-functional teams** that facilitates seamless collaboration, breaking down barriers between different teams and ensuring everyone’s on the same page.

The value of purpose-built cloud security

With the arsenal of cloud security tools consolidating into CNAPP, organizations now wield a formidable defense system tailored for the cloud age. Here's what this milestone means for security teams everywhere:

Real-time detection of known and unknown threats

A robust cloud detection and response solution that's purpose-built for the cloud detects both known and unknown threats across your organization's entire cloud estate in real time. Of course, in today's most innovative CNAPPs you'll get the most advanced capabilities. For example, a modern CNAPP automatically correlates posture and runtime insights for true cloud-native context, which is instrumental in accelerating workflows and eliminating skill gaps. It also unlocks feedback loops for key stakeholders, removes friction across fractured business lines, and provides teams with a single source of truth. By implementing a true cloud detection and response solution that provides these capabilities, security leaders and practitioners can reap the benefits in analyst efficiency, risk reduction, and cost optimization.

Multi-domain correlation to machine and human identities

Threats in the cloud rarely confine themselves to a single domain. Effective cloud threat detection provides multidomain correlation across assets, users, activity, and risk to identify threats in real time. By layering instant detections with insights into vulnerabilities and permissions in use, a CNAPP connects the dots across environments, preemptively diffusing threats before they escalate.

Identify and contextualize events for rapid investigations

Ever felt like you're solving a cyber puzzle on your cloud estate with missing pieces? Not anymore. A CNAPP automates the correlation of cloud and workload events to identities, giving you the full context on command histories, network traffic, and file activity. Automated captures tie digital forensic evidence to events, providing a comprehensive view of threats. Additionally, MITRE-mapped and filterable investigations streamline workflows, empowering you to swiftly pinpoint and address vulnerabilities and misconfigurations.

Break silos for cross-team workflows

Let's face it: Silos are for grain, not for security teams. A single purpose-built cloud security platform breaks down barriers between incident responders, developers, and everyone in between. You can quickly collaborate with lightning-fast investigation findings that arm your team with actionable insights within minutes. This isn't just about stopping attacks; it's about fine-tuning your defenses for the long haul. By sharing incident debriefs and enhancing preventive controls, you don't just mitigate risk — you elevate your approach to cloud security.

Conclusion

As we look at the journey through cloud security's innovation, one thing is clear: the landscape has transformed dramatically, echoing the evolution of endpoint security in pursuit of speed and resilience against cloud threats. From the pioneering days of cloud security, fixated on prevention, to the evolution towards robust detection and response capabilities, and culminating in the consolidation of tools within CNAPPs, the parallels are striking.

EDR paved the way for endpoint security, but CNAPPs with CDR capabilities have emerged as the guardians of the cloud. While EDR is an excellent tool for workstations, security teams need CDR solutions to swiftly identify and neutralize threats across vast cloud environments. CDR not only detects and responds to threats in real time, but also provides the agility and depth to combat modern threats.

Above all, CNAPPs empower security teams to meet the 555 Benchmark: 5 seconds for detection, 5 minutes for correlation and triaging, and 5 minutes for response. This strategic approach not only safeguards your cloud infrastructure but also future-proofs your defenses against emerging threats. Embracing this cloud security strategy isn't just about protecting data; it's about empowering your organization to confidently harness the full potential of the cloud, fostering innovation, growth, and resilience in the face of an ever-changing digital landscape.

See how Sysdig helps you secure every second.

Take the next step.

REQUEST A DEMO →

sysdig

E-BOOK

EBK-013 REV. A 7/24