SentinelOne E-book

SentinelOne®

Practical Guidance for Cloud Defense in Depth

The speed, flexibility, and scale of cloud computing has fundamentally transformed business operations and competitive dynamics.
As organizations accelerate innovation and adversaries target cloud services, how can security leaders devise a multi-cloud security strategy that not only works with the business to enable agility but also protects vital corporate secrets and customer data?

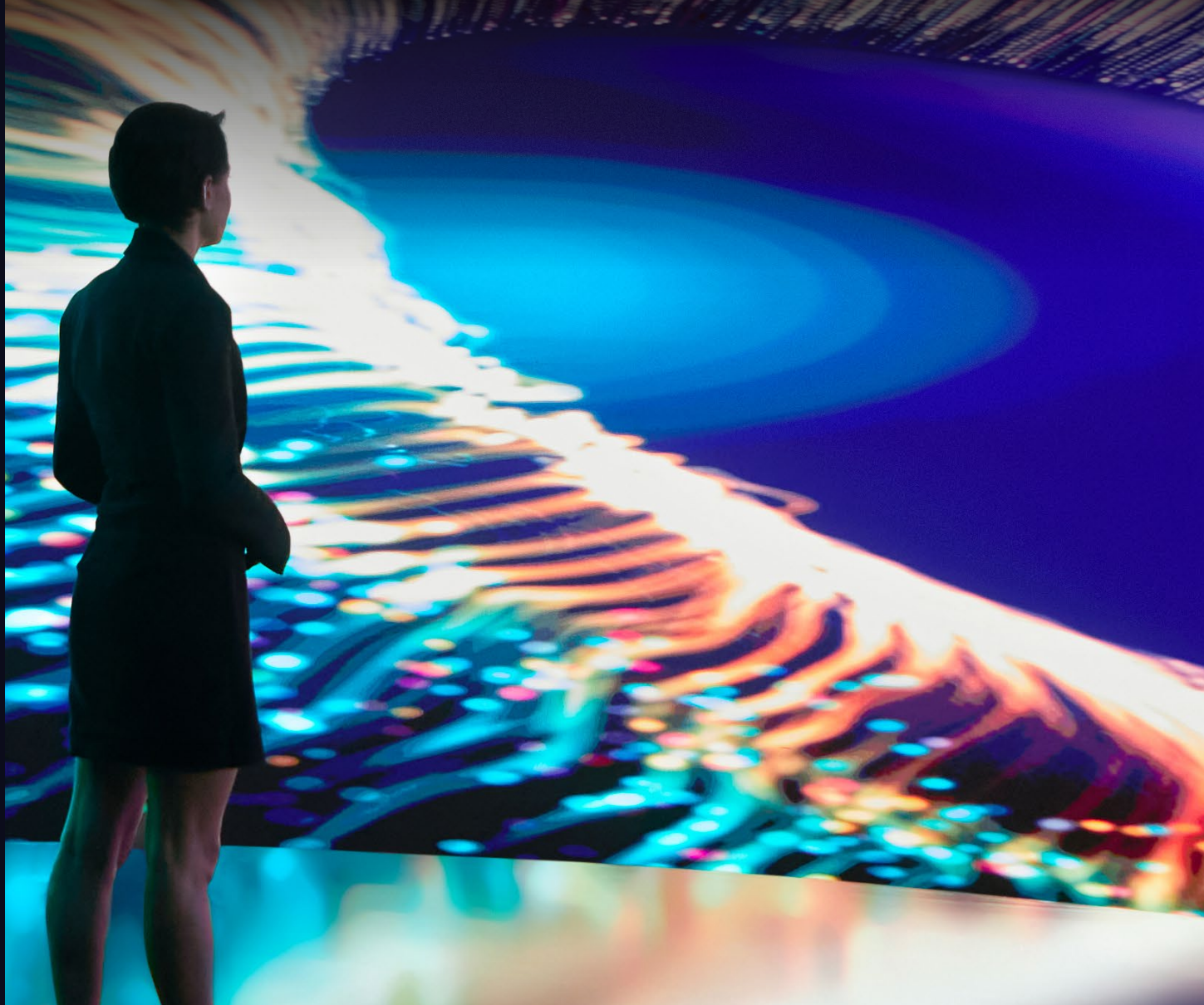


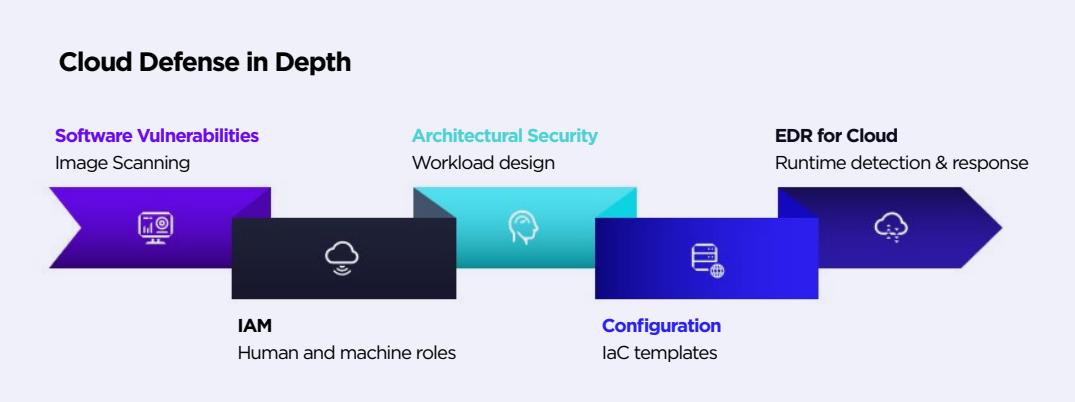
Table of Contents

Introduction

Most organizations (87%) use multi-cloud infrastructure as part of their business operations[1]. Cloud infrastructure spending in 2022 is projected to reach $120 billion[2] and shows no sign of slowing down, despite security being cited as the top cloud concern by IT executives for 10 of the last 11 years[3]. Innovation is king and the CIO's digital transformation initiatives continue full throttle, so then the question becomes:

> Are we more or less secure in the cloud, and what can we do to optimize our cloud security?

This is where multi-layered cloud security comes into focus. Defense in depth spreads risk management across various facets of workload development, deployment, and production. Such a strategy would "shift-left" when it comes to identifying and resolving software vulnerabilities, include a robust identity and access management (IAM) implementation, apply the appropriate configuration security controls, and provide for real-time, behavioral AI for cloud detection and response (aka, EDR for Cloud).



Omitted from this paper is an important aspect, architectural security, for 2 primary reasons. First, the architecture of cloud workloads is typically the remit of a Solution Architect, working in close cooperation with product developers. As such, and for all but the most mature of cloud natives, this is usually outside the purvey of IT Security. With that said, it does repre-

1 2022 Flexera State of the Cloud Report
2 Gartner press release, Gartner Forecasts Worldwide Public Cloud End User Spending..., April 2022
3 Flexera, page 41

sent an amazing opportunity for skills advancement and high-value consultation for those security professionals willing to invest the time and energy required. Secondly, architectural design for security is a hefty topic worthy of its own discussion, as there are myriad training courses, and career tracks, dedicated to this art and science. In summary, to enter into an architectural security discussion here would not do the topic justice, and would serve to dilute our primary focus.

CHAPTER 01

Software Vulnerability Management

Agile innovation begins with the development teams. Identifying software vulnerabilities early is important for 2 reasons, risk and cost. After all, it is cheaper to solve software security gaps in development than in production. Yet competitive pressures and KPIs prioritize pushing product to production, sometimes with known software vulnerabilities and sometimes with latent software supply chain risk from the use of 3rd party libraries. Using only trusted 3rd party image repositories is recommended, though not always practical; the flexibility for exception management is often desirable for scrum teams on the innovation treadmill.

76%

Of production images contain critical or high severity vulnerabilities

To mitigate this risk, image scanning and software composition analysis (SCA) solutions surface these vulnerabilities. This is good practice, though not without its own limitations. Image scanning can only identify **known** software vulnerabilities; it cannot solve for the unknown, for zero days and runtime threats. Software vulnerability scanning is a recommended first step, but is only a single point-in-time control. And by itself is insufficient to secure the enterprise's multi-cloud footprint. Were it sufficient, then it is highly unlikely that 3 of 4 workload images in production would still contain critical or high severity vulnerabilities. And so we press on with additional security controls.

RECOMMENDATIONS

- Use trusted image repositories
- Scan software images for known vulnerabilities
- Justify and document any vulnerability exceptions

CHAPTER 02

Protect the Control Plane

Protecting your cloud management control plane is **the highest priority** in a successful cloud security strategy. As if to punctuate this point, 2 of the Top 10 Cybersecurity Mitigation Strategies published by the NSA are specifically focused on this security aspect: tiered access and MFA.

Tiered Administrator Access

Not every administrator shares the same responsibilities or requires access to the same set of cloud resources. Mapping administrative privileges to areas of operational oversight manages risk in the event of credential compromise. Tiered administrative roles, each with additional layers of authentication, further mitigates the risk of abused credentials or malicious insider.

Using MFA

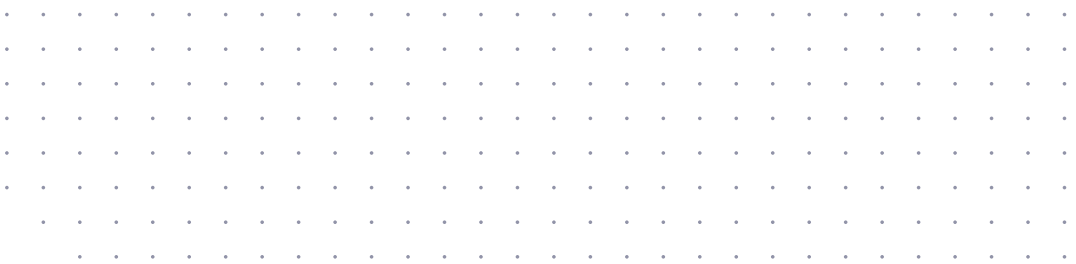
As mentioned in the previous paragraph, Multi-Factor Authentication should be used for every administrator account.

Logging Privileged Accounts

Persistent logging of the use of privileged accounts provides a forensic trail should such an account be compromised.

On- and Off- Boarding Process

If you do not already have a well-groomed process for swiftly off-boarding super users who are leaving the company, please create one. This is an issue which spans both protecting the control plane and managing authorized user identities.



CHAPTER 03

Reducing Identity Attack Surface

IAM (Identity & Access Management) helps cloud administrators specify who can access what and under which circumstances. The sheer number of users, accounts, roles, and scopes which a multi-cloud enterprise can create and manage at scale is a daunting but not insurmountable security challenge. Thankfully, cloud service providers (CSPs) offer IAM services so their customers can manage this risk more efficiently at scale. For example, AWS has an extensive IAM User Guide to equip customers with the tools they need to manage the security of their data residing in the cloud.

User authentication and access

Multi-factor authentication and federated identity provide a means of verifying a user identity before they can access enterprise cloud resources. You can also specify conditions which must be met in order to access these resources. A simple example is to require an encrypted cloud connection.

Roles & Least Privileges

A role is a means of assigning specific permissions to an identity, be it human or workload. Through judicious use of roles, Security can limit the actions that users can take, consistent with the Principle of Least Privileges and within a well-planned workload architecture.

EXAMPLE

Instead of a compute instance such as AWS EC2 directly connected to the internet, consider a drop bucket that will sit between the instance and the internet. An authenticated and conditionally authorized employee will upload a file to this bucket before it is sent for further processing. A machine role can be defined authorizing it to only retrieve new objects placed in the drop bucket, presumably after having scanned the file for malware. Once judged to be safe, the file is then passed by the machine role to the aforementioned cloud compute instance for processing. In this way, the EC2 instance remains safely within a VPC, accepting input only from authorized users via a specific drop bucket, and even then, only under certain conditions (ie, after the file is verified safe). This is but one simple example.

RECOMMENDATIONS

- Tier administrative access and log their use
- Use MFA
- Review accounts and roles regularly
- Retire unused accounts and roles
- Assign roles according to Least Privileges
- Do not hardcode identity secrets

DEFENSE IN DEPTH IS VITAL

No single security control mechanism is sufficient, but each has a part to play. In a recent virtual panel, an MSSP shared that 14% of incidents investigated in the last quarter involved an MFA requirement being satisfied by an attacker.

Review accounts and roles regularly

There should be an oversight mechanism in place to regularly review roles. Stale accounts should be offboarded, unused roles retired, and a well-oiled process in place to offboard former employees.

Key management

Access keys are a means of providing long-term access to cloud resources. Access keys should be changed (rotated) regularly. Do not store access keys in plain text or co-resident where the workload runs.

CHAPTER 04

Configuration Management

Any discussion of cloud defense in depth would be incomplete were it to exclude configuration security. Each CSP offers hundreds of services, with varying degrees of differentiating features and capabilities. For these services to be operated securely, they must be configured securely. The responsibility for configuration security falls solely to the customer.

Organizations of all sizes continue to struggle with configuration management of their cloud footprint, which is totally understandable given the speed and scale of change. Misconfigured resources are regularly cited as a leading cause of cloud security failures. An easily grasped example of such a misconfiguration would be making a private database containing customers' private data publicly accessible.

Some attackers have a targeted strategy to gain access, establish persistence, and move laterally across their victim's infrastructure. Others are simple opportunists, programmatically checking the configuration of internet-facing data stores, to see who left their front door unlocked so that they can quickly exfiltrate data. Against the latter, there is no hiding in obscurity. Your cloud footprint is simply an IP address. Bad actors need not know anything about your business, only that they can take your data and assess its value later.

CIS Benchmarks

Luckily, the Center for Internet Security (CIS) publishes best-practice recommendations for the secure configuration of cloud services. Simply compare the configuration settings of your cloud resources against the relevant CIS Benchmarks to assess your risk level. Here too, CSPs and a number of vendors offer services to help automate this oversight process.

Infrastructure as Code (IaC)

Speaking of automation, as any DevOps engineer worth their salt will tell you, if you're going to do something more than once, automate it. And so it goes with cloud infrastructure provisioning. With IaC, infrastructure deployment is not only automated via a sequence of machine-readable instructions, but so is its configuration. Any number of templates which conform to enterprise security guardrails can be developed, refined, and, when ready, entered into a production library under revision control. In this way, quality and repeatability across the organization is achieved. As new requirements are identified, new templates are created, refined, and released.

DEV - STAGE - PROD

"Begin with the end in mind," where the end is production operations of cloud infrastructure, and the beginning is the development account. Use the same configurations for DEV, STAGE, and PROD. Take care not to cut corners for convenience in DEV, because the best intentions sometimes become misplaced in the race to meet high-pressure deadlines, and those "temporary" settings can find their way to PROD. "As it will be in PROD, so let it be in DEV:" use those checked-in IaC templates. There will be less stress and risk later.

CHAPTER 05

Cloud Detection & Response (EDR for Cloud)

After so many security layers and controls, one might reasonably ask what role runtime security would play. Runtime protection, detection, and response is the last line of defense for cloud workloads. It catches what other compensating controls miss. It provides a forensic trail for security analysts to follow, so that they can continuously improve their defenses. It provides organizations the opportunity to innovate quickly, at scale, confident in the knowledge that runtime security will detect and stop anything amiss in real-time, at machine speed. It keeps your cloud operations in business, defending against runtime threats such as ransomware and crypto mining malware.

Cloud ransomware

Businesses increasingly rely upon cloud infrastructure to run their business, and so attackers increasingly target cloud infrastructure for illicit gain. To prove the point, there has been a marked 146% increase year-on-year in Linux ransomware code variants[4]. Ransomware is a behavioral threat, not a section of vulnerable code. If a file is zipped, no problem. If it is copied, moved, and the original deleted, still no problem. If, however, this process repeats over a certain period of time, a cloud workload security solution with behavioral AI will detect the malicious activity and autonomously respond according to policy set by the security admin. Therefore, scanning images for known software vulnerabilities, while good, will not protect against behavioral threats such as ransomware. Similarly, misconfiguration alerts do not provide a sequenced OS-level forensics trail to reveal what the attackers did.

The true cost of ransomware goes well beyond the ransom. The average cost of a ransomware attack, excluding the ran-

$4.54 mln

The average cost of a ransomware attack, excluding the ransom

Source:
IBM Security Cost of a Data Breach Report 2022

4 2022 IBM X-Force Threat Intelligence Index Report

som, is $4.54 million[5]. Costs include business disruption, incident response, notifications, legal, and regulatory matters. But there is a silver lining. This research goes on to report that organizations which have deployed security AI and automation, such as that in a cloud EDR, realize a $3.05 million average cost savings for data breaches. Although the report switched from ransomware to data breach in quantifying results, one can follow the logic: AI detects the ransomware attack and automated response thwarts it. Machine speed attacks demand a machine speed response, and that is the true power of EDR for cloud workload protection.

Crypto mining malware

Yet another runtime threat is crypto mining malware. Mining digital currency like Bitcoin is computationally intensive. Rather than pay for their own infrastructure costs, attackers will stealthily deploy a crypto mining rig to a legitimate enterprise's cloud infrastructure and siphon off compute cycles, often capping the percentage of compute capacity stolen in order to evade detection. These cryptojacking criminals keep the Bitcoin, and customers keep the surprise cloud bill. Cloud security professionals can create value for their organization by choosing a cloud workload protection which will detect and kill such a runtime threat, thereby eliminating the cost of pirated infrastructure.

Other runtime malware

Beyond ransomware and crypto mining rigs, other runtime threats may exploit zero day vulnerabilities, inject malicious code into memory, or download malware from nefarious servers at runtime. Here too, a cloud workload protection solution will detect and eliminate these methods which other security controls cannot.

5 IBM Security Cost of a Data Breach Report 2022

CHAPTER 06

Parting Thoughts

A cloud defense in depth strategy sets organizations up for success by weaving together the various strengths of each layer in the security stack. Choosing between security and the business agility which the cloud enables is a false choice. It is possible to innovate quickly and securely. With cloud workload protection as the security backstop, organizations of all sizes have the runtime security they need to accelerate their continuous software development, confident in the knowledge that if anything goes wrong, real-time detection and response will keep the business running.

Singularity™ Cloud

If you would like to learn more about how SentinelOne can help protect your cloud workloads - wherever they run, AWS, Azure, Google Cloud, or private data center - we invite you to visit our website. There you will find customer case studies, demo videos, and more about what makes our Singularity Cloud product portfolio unique. And when you are ready, our team of cloud security specialists is ready to connect with your cloud security experts.

LEARN MORE

Find even more cloud content by scanning this QR code.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity Platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

sentinelone.com

S1_eBook_035_Cloud_Defense_In_Depth_04062023

© SentinelOne 2023