Cloud Controls Buyer's Guide

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Introduction

The world of IT is moving to the cloud for flexibility, on-demand computing resources, and speed just to name a few benefits. Market data varies but estimates of cloud usage show that in the range of 20–25% of overall compute workloads are operating in public cloud environments today, with that expected to grow to 50% over the next 5–10 years. However, most organizations haven’t moved 100% of their IT compute resources to the cloud just yet.

Organizations are starting to, and planning to, operate in a hybrid environment that includes both public cloud, private cloud, and virtualization in the coming years. For most organizations this will require security controls that can serve this complete infrastructure. According to IDC, 80% of organizations will commit to a hybrid cloud architecture this year. So organizations are faced with a decision: take one or two separate paths? Protect cloud and on-premises assets using two different solutions or single one?

Using the same product in both places can be difficult because there are different needs and unique challenges in the cloud.

Foundational Controls

Foundational controls include essential security and compliance capabilities like asset discovery, security configuration management, vulnerability assessment, and log management. These are the fundamentals that you need to get right because they provide the biggest return on investment in terms of risk reduction. No matter what security framework your organization uses, it will include some variation or combination of these foundational controls.

An example of foundational controls shown here is the Center for Internet Security’s CIS Controls, formerly known as the SANS Top 20. According to CIS, “Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent.”

CIS Control
Control 1: Inventory and Control of Hardware Assets
Control 2: Inventory and Control of Software Assets
Control 3: Continuous Vulnerability Management
Control 4: Controlled Use of Administrative Privileges
Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

These foundational controls are just as important in the cloud as they are on-premises, and can be summarized as follows:

- » Know what you have
- » Know it’s secure
- » Know when it changes

However, there are some challenges you may run into deploying these five controls across hybrid IT environments. This buyer’s guide will address those challenges and provide recommendations for things you should consider when selecting foundational controls for hybrid environments.

Challenge: Multiple Solutions

Cloud infrastructures are different from their on-premises counterparts. If your security and compliance controls were designed for on-premises environments, don’t assume they will work correctly in the cloud. Conversely, don’t assume that controls built for the cloud will work well or at all in on-premises environments. If your controls don’t support both types of environments, you may end up deploying multiple controls for multiple environments. Dealing with multiple controls for environments is costly and time-consuming in terms of deployment, administration and reporting.

Ideally, you want a unified solution that provides foundational controls across your physical, virtual, private and public cloud landscape.

Which environments does your solution support?

□ Physical datacenters

□ Virtual environments

□ Private clouds

□ Public clouds

□ All of the above

Challenge: Scale Controls Up and Down

Another challenge is the dynamic nature of elastic computing environments, where elastic assets come online and go offline to scale up and down to meet demand. In elastic environments your servers may only exist for minutes, hours, days or weeks. Your security controls will need to match that demand as cloud assets are rapidly created and destroyed, otherwise gaps in visibility and errors can occur as hosts appear and disappear.

Some questions you may want to consider for foundational controls in elastic environments:

□ Does the solution use an agent?

□ If the solution uses an agent, can it automatically install the agent?

□ Does it integrate with automation tools like Chef and Puppet?

□ Can it import asset tags from the AWS console during the onboarding process?

□ Can the solution dynamically onboard and offboard nodes, and preserve data from decommissioned nodes for reporting or compliance purposes?

Challenge: Cloud Policies and Platforms

Make sure that your foundational controls support the polices, operating systems, platforms and technologies you use across your complete infrastructure. Cloud-oriented infrastructures may require specific platform and policy support, so make sure that your foundational controls support the assets you need to protect. For example, not all solutions support Amazon Linux. In addition, pre-hardened and ready to deploy Amazon machine images and Azure images can make deployment of foundational controls easier.

Does your solution:

- □ Support the polices, operating systems, platforms and technologies you use?
- □ Support monitoring of assets in Amazon Web Services (AWS) or Microsoft Azure?
- □ Support CIS Benchmarks for the AWS Console and Amazon Linux?
- □ Offer machine images for Amazon/Azure?

Challenge: Containers

Another cloud-oriented infrastructure that's not necessarily cloud based are containers like Docker. Containers share the same underlying operating system, but have a different operating environment for applications and libraries. If your foundational controls don't understand container technology they may provide inaccurate or incomplete information.

Some questions you may want to consider for Docker containers:

- □ Can it report distribution based vulnerabilities in Docker containers (e.g. Ubuntu, Debian, RHEL, CentOS, OEL, etc.)?
- □ Can it determine if the various Docker components (i.e. Docker Daemon, Client, and Toolbox) are installed?
- □ Does it support enumeration and reporting of Docker Containers?
- □ Can it normalize Docker container logs?

Summary

In terms of an ideal foundational controls solution for hybrid cloud environments, consider a toolset that can:

- □ Apply the same robust controls across on-premises and cloud networks with unified management and reporting environment
- □ Support dynamically on-boarding and off-boarding nodes to ensure continuous coverage in elastic environments
- □ Support cloud policies and platforms in addition to the policies and platforms that you use on-premises
- □ Assess cloud-oriented technologies like Docker containers
- □ Operate in an architecture that can support physical, virtual, private and public cloud environments

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

The State of Security: **News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook

BRCCBG1k 1706