White Paper

Symantec
A Division of Broadcom

Five Tips to Make Your Cloud Security Roadmap Flexible, Agile, and User-Friendly

Overview

Digital transformation and the spread of cloud technologies are changing every facet of modern IT, including reshaping the way we develop applications, set up infrastructure, and define security measures.

Organizations embracing the cloud are enjoying a range of business gains with mobile apps and workloads, increased adaptability, long-term cost savings—and equally important—the ability to offer customers better services delivered faster. Looking beyond the IT-related benefits and embracing the customer-centric mindset is critical for IT and security professionals to succeed in this new world.

Cloud adoption shifts the traditional network boundaries, challenging our security approaches about how to secure virtual environments, often combining more than one cloud and on-premises locations. If this weren't enough, these environments need to be accessed by an increasing number of mobile and remote employees and contractors using multiple managed and unmanaged devices.

As complex as these challenges are, IT teams are required to deliver faster and better services to their internal customers—the business units, engineers, operation teams, and eventually the organization's customers. When designing your security roadmap, listed are five tips to secure your organization's assets, wherever they are hosted, while maintaining the level of flexibility, agility, and user experience your business and customers require.

Tip 1: Favor solutions that solve for today, but scale for tomorrow

When working toward securing new cloud environments, evaluate solutions and vendors that not only deliver the required outcome today but can also help you provide better quality and speed of services in upcoming projects. For example, check how a specific solution can support multi-cloud deployments. Does it support all major public cloud vendors or is it vendor-specific? What happens when you scale x10? What about x1000? Many cloud projects use solutions (especially ones which are built around modern server-less stacks) which can scale-out and scale-in to support dynamic loads in your environment. How will your selected vendor handle such loads?

Tip 2: Don't think what you've done until now is going to work in the future

Can your existing vendors deliver cloud-native solutions, or will they end up adapting their legacy solutions to the cloud era? When objectively evaluated, many of the existing approaches and solutions will crumble and need to be redesigned from scratch. The phrase "we've always done it this way" won't fly in the process of digital transformation and cloud adoption.

One clear example is legacy firewall and VPN solutions. Many traditional vendors have provided a virtual version of their legacy appliance solutions that fits cloud environments. However, when evaluating these solutions with a cloud mindset, it is very clear that these solutions don't scale. While your cloud application can scale to 10x the load in a matter of seconds or minutes, your traditional firewall cannot! Instead, you will have to deploy 10x "virtual" appliances in your environment, configure each of them to pull the right access policy, and hope nothing was missed in this cumbersome process. Look for cloud-native solutions that can dynamically and flexibly scale-out and in with your environment workloads. Often such solutions are offered "as-a-service."

Tip 3: Look for automation and integration abilities in your security solutions

The security industry has been accustomed to solutions that are boxed, do not communicate with each other, and require complex and expensive integration processes. That part of the security setup has been coined Security Automation and Orchestration (SOAR). Unfortunately, this dynamic opposes the nature of the cloud where the state of mind is "if it can be automated, it will be." Your security solutions should be no different. Look for solutions that are well-documented and have well-maintained APIs, and ones that can seamlessly integrate with other tools via standard approaches such as webhooks.

One such example is provisioning access to production workloads automatically, based on support tickets and their owners as created in your support-ticketing solution. Providing this kind of immediate service to your users is what the cloud is all about.

Network security is another good example of the mind-shift process. Shifting from the traditional approach of a perimeter secured via IP-based access rules (the castle-and-moat approach) to a software-defined-perimeter model that applies a Zero Trust approach to access. To implement Zero Trust Network Access (ZTNA), you must determine the level of network access based on a combination of identity, device, and application context instead of an IP:Port-based approach. Applying this model, each user starts from a Zero Trust point—where the user gains network access to a specific set of organizational resources only once authenticated.

Tip 4: Take the opportunity to adopt new models and approaches for old problems

Innovation happens across all major aspects of security, leveraging cloud environments and securing them. Detection solutions are a great example of adopting a new model and approach. Moving away from the old signature-based model, Machine Learning (ML)-based behavioral detection is the new norm for detection solutions. All Endpoint Detection and Response (EDR) vendors, for example, are claiming to be ML-based, with most algorithms running in the cloud. This approach provides huge benefits, such as sharing indicators across environments, leveraging compute power unavailable to any single customer on-premises, as well as responding faster to threats (remember the monthly definition updates?). This is actually a great example of better, faster.

Tip 5: Think hybrid, for a (very) long time

The combination of on-premises and cloud-based data centers and environments is a reality for most organizations today and in the foreseeable future. Evaluate which solutions can give you real support in a hybrid environment. Will your on-premises SIEM be able to collect all logs from all cloud services you're using? Will it scale? What about your access and access management solutions? Can your beautiful RBAC models, the ones that took 15 years of hard work to build, grant the right level of access to all your assets, across on-premises and cloud (and multi-cloud) environments?

The answer to both questions is probably no. Thinking about the hybrid approach when evaluating different solutions will help you build a better service, which you can deliver faster to your users.

Security Automation and Orchestration (SOAR) simply defined:

A coordination of automated security across connected security applications and processes.

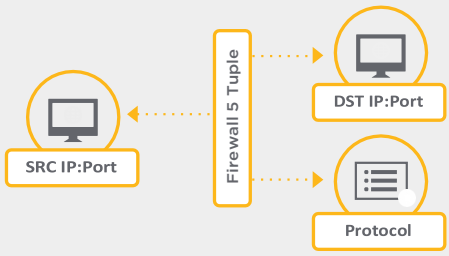
Security Automation

The automatic handling of a task in a machine-based security application that would otherwise be done manually by a cyber-security professional.

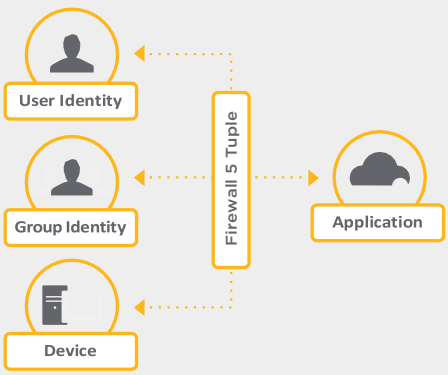
Security Orchestration

The connecting and integrating of various security applications and processes together.

IP:Port-Based Approach



Zero Trust Model



Vendor Validation Checklist

- Evaluate the vendor's multi-cloud support, technological scale (more load), and economical scale (price).
- Favor vendors who are cloud-agnostic, and support elasticity with clear pricing when the environment grows.
- Favor SaaS vendors for reduced operation and maintenance costs, immediate scale, and ability to handle peaks in loads.
- Consider integrating multiple solutions across a given environment for automating repeatable tasks as much as possible.
- Favor vendors who offer integration points (such as APIs, Webhooks, and so on).
- Evaluate emerging technologies and trends and discuss them with your vendors.
- Evaluate new entrants or new products for new technologies.
- Evaluate how the vendor operates in a hybrid environment.
- Favor vendors who can provide an on-premises level of service as good (or better) as their service for cloud environments and leverage your existing investments.

Symantec® Secure Access Cloud™

Symantec enables security and IT teams to create Zero Trust Application Access architecture without traditional VPN appliances. Symantec Secure Access Cloud™ securely connects any user from any device, anywhere in the world to corporate on-premises and cloud-hosted applications while all other corporate resources are cloaked. No direct network access is ever granted to prevent any lateral movements to other network resources while eliminating the risk of network-based attacks. The platform is agentless and can be deployed in less than five minutes, without forcing a disruptive change in the organization's existing architecture, user permissions, and applications. Symantec Secure Access Cloud™ provides full governance and real-time enforcement of users' actions in each corporate application.

Symantec
A Division of Broadcom

For more product information: broadcom.com

SYM-Roadmap-Five-Tips-WP100 November 10, 2021