Symantec™
A Division of Broadcom

Hey You, Get off of My Cloud

7 Tips to Securing Your Cloud Environments

The Benefits of Cloud Migration

The spread of cloud technologies is changing every facet of modern IT, including reshaping the way we develop and use 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.

Cloud adoption also introduces new security challenges. Looking beyond the IT-related benefits and similarly embracing the customer-centric mindset is also critical for the security professionals to succeed in this new world.

ORGANIZATIONS EMBRACING THE CLOUD ARE UNLOCKING BUSINESS ACCELERATION:

- Improved customer experience
- Empowered digital employees
- Long-term cost savings
- Better, faster delivery of services to customers

The Security Challenges of Cloud Migration

Cloud adoption shifts the traditional network boundaries, challenging our approaches about how to secure virtual environments, often combining more than one cloud and on-premises locations.

If this weren't enough, these hybrid environments need to be accessed by an increasing number of mobile and remote people using multiple managed and unmanaged devices.

As complex as these challenges are, IT teams are often sacrificing security to deliver faster and better services.

To help you address these challenges and design a modern security roadmap, here are seven tips to secure your organization's assets, wherever they are hosted, while maintaining the level of flexibility, agility, and user experience your business requires.

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 cloud vendors or is it vendor-specific?

Additionally, what happens when you scale? IDC predicts that the amount of data created over the next three years will be more than the data created over the past 30 years, and that of all the data that is stored, almost 40% percent of this data will reside in the hyperscale/cloud datacenters.[1] Many cloud projects use solutions which can scale-out and scale-in to support large and dynamic loads in your environment. **How can your selected security vendor handle such growth?**

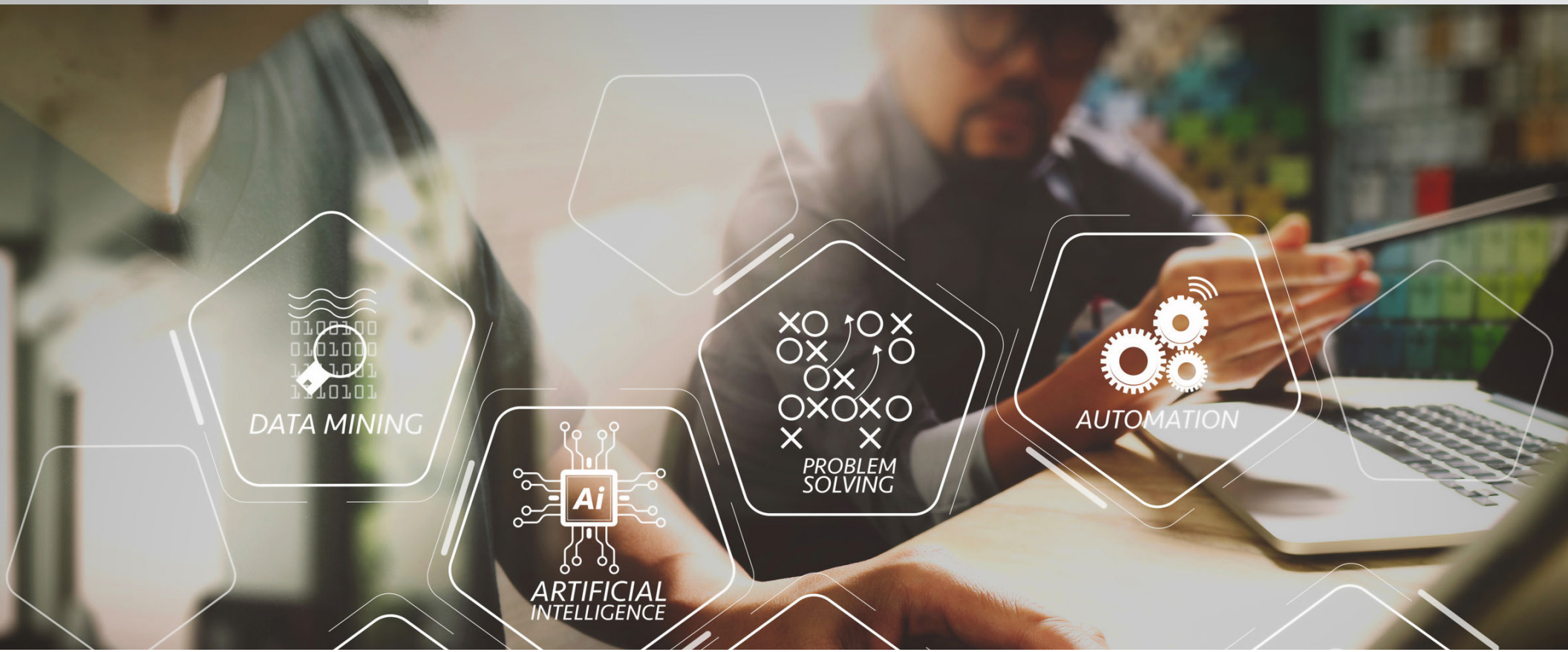
2. Don’t think what you did yesterday is going to work tomorrow

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 existing solutions and approaches will crumble and will need to be redesigned from scratch.

One clear example is the legacy firewall and VPN solutions. Many traditional vendors have provided a virtual version of their legacy appliances that fits into cloud environments.

When evaluating these solutions with a cloud mindset, it is clear that these solutions don’t scale. Whereas your cloud application can scale to 10x the load within minutes or less, the traditional firewall cannot.

Our suggestion is to **look for cloud-native solutions that can dynamically and flexibly scale-out and in** with your environment workloads.



3. Look for solutions with automation and integration abilities

The security industry has been accustomed to point solutions that focus on a specific threat vector, do not communicate with each other, and require complex and expensive integration processes. Unfortunately, this approach opposes the nature of the cloud where the state of mind is "if is can be automated, it will be." Your security solutions should be no different.

We suggest that you look for solutions which are well-documented and have well-maintained APIs, and ones that can seamlessly integrate with other tools via standard approaches.

One such example is provisioning access to production workloads automatically, based on integration with DevOps toolchain or support tickets. **This kind of immediate service is what the cloud is all about.**

4. Take the opportunity to adopt new models for old problems

Innovation happens across all major aspects of security, leveraging cloud environments and securing them. Existing IAM platforms integrate with these newer perimeter tools to perform the continuous verification and validation of users and devices so that least privileged access can be enforced.

Detection solutions are a great example of adopting a new model and approach. Modern EDR vendors are moving away from the old signature-based model, and using Machine Learning-based behavioral detection, which run in the cloud, share information, and provide better, faster security across all customers.

Network security is another good example of the mind-shift process, as traditional IP-based access rules are replaced with a software-defined perimeter model that applies a Zero Trust approach to access.

5. Know the difference between network and business perimeter

Cloud adoption and migration are routinely used as if they were synonymous, but they can be very different. The security challenges of moving your applications from on-premise data centers into cloud environments (IaaS /PaaS) is very different than those presented by adopting cloud applications (SaaS). In the first case, the cloud apps are running within your network perimeter, but in the second they are running in your business perimeter.

We suggest that you look for a platform that secures both the network and business perimeters, and freely shares access and activity data across these distinct cloud application environments, and can combine it with on-premise data to provide to your User and Entity Behavioral Analysis (UEBA) tools.

Only with a complete picture can the UEBA provide accurate real-time decisioning that is required for Zero Trust continuous verification.

6. Recognize the expanded attack surface introduced by the cloud

As your IT environment has expanded outside your four walls to incorporate public cloud resources and software-as-a-service (SaaS) applications, the traditional way of approaching administration and operations has also quickly fallen apart—mainly because it fails to protect new attack surfaces like management consoles and APIs. How are you protecting the keys to these kingdoms?

We suggest that you look for solutions that protect these cloud accounts and interfaces that provide privileged and administrative access to these environments.

In many cases, these accounts are not even being used by people—they may be DevOps tools, applications or configuration files empowered by hard-coded administrative credentials. **All of which can be hacked and compromised where security is inadequate or non-existent.**

7. Think hybrid, for a (very) long time

The combination of on-premise and cloud-based data centers is a reality for most organizations today, and will be for the foreseeable future. Cloud-only and cloud-first strategies are excellent for new IT projects, but legacy apps and systems will continue to run internally for many years to come.

Evaluate solutions which can give you real support in a hybrid environment.

What about your access and access management solutions? Can your existing RBAC models, the ones you took years to build, grant the right level of access to all your assets, across on-premises and multi-cloud environments?

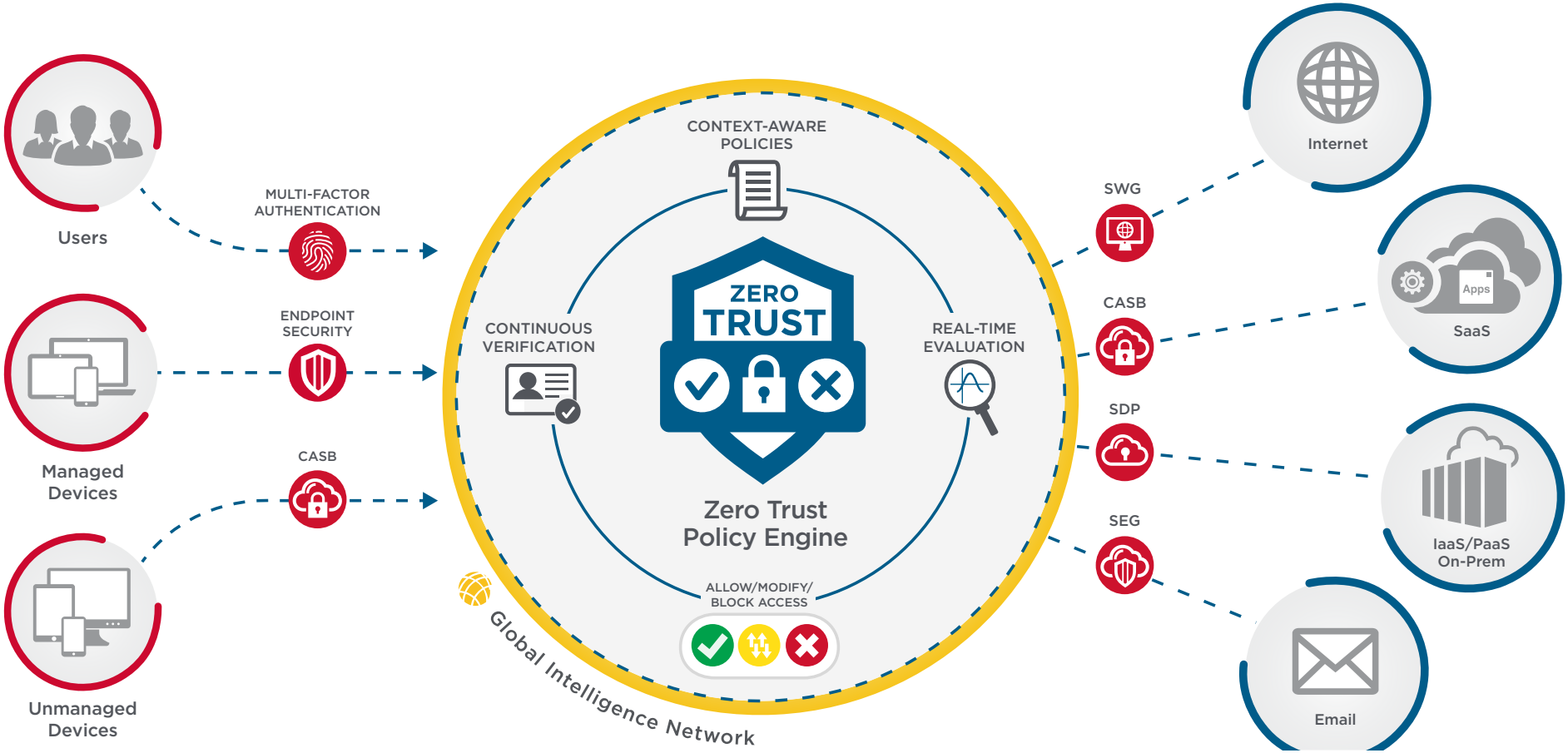
The answer to both questions is probably NO. But does this mean you need to replace everything? Again, probably NO. We suggest you look for a solution that can build a better service for tomorrow, but can also leverage your existing investments (at least for now).

Vendor validation checklist

As you look to build out your security solutions for the future, here is our suggested vendor validation checklist:

- Evaluate the vendor's multi-cloud support, technological scale (more load) and economic scale (price).
- Favor vendors who are cloud-agnostic, support elasticity with clear pricing when the environment grows.
- Identify 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.
- Embrace vendors who offer integration points, and even better, platforms that are already integrated.
- Evaluate emerging technologies, trends, and attack surfaces and discuss them with your vendors.
- Favor vendors who can provide the same level of service for both on-premises and cloud environments, and can leverage your existing investments.

Symantec Zero Trust Security



Comprehensive protection across your hybrid environment

Why Symantec

Get complete visibility and control for your hybrid infrastructure. Reduce the total cost of your risk. Empower your security team and deliver a friction-free experience.

MOST COMPLETE

Integrated Cyber Defense Platform

Symantec offers the **Most Complete** Zero Trust Platform in the market

MOST VALUE

Total Cost of Ownership

Symantec's unique Portfolio License Agreement & Integrated Zero Trust Platform **Lowers Overall Costs**

MOST RECOGNIZED

Best-in-class Technologies

Symantec has been named a **Leader in More Categories** than any other vendor in the market

See what's possible when you harness the power of a Modern Zero Trust Platform

LEARN MORE TODAY.
SYMANTEC.BROADCOM.COM/ZERO-TRUST

Symantec™
A Division of Broadcom

For product information please visit our website at: broadcom.com

BC-0600EN September 2020