5 tips to make your **cloud security roadmap** flexible, agile and user-friendly

luminate

www.luminate.io

5 tips to make your cloud security roadmap flexible, agile and user-friendly

It is pretty obvious that 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 such as leveraging mobile apps and workloads, increased adaptability, and long-term cost savings and equally importantly - the ability to offer customers better services delivered faster. Seeing beyond their 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. As if this is not enough, these environments need to be accessed by an increasing number of mobile and remote employees and contractors using multiple managed and un-managed 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 end-users and customers.

This whitepaper will provide you with 5 tips on how to design a security roadmap that secures your organization's assets wherever they are hosted while maintaining the level of flexibility, agility and user experience your business and customers require.

Organizations embracing the cloud are enjoying a range of business gains:

Leveraging mobile apps and workloads

Increased adaptability

Long-term cost savings

The ability to offer customers better services delivered faster

luminate

1. Favor solutions that solve for today, but scale for tomorrow

When working towards 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?

While your cloud application can scale to x10 the load in a matter of seconds or minutes, your traditional firewall cannot!

2. Don’t think that 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 will need to be redsigned 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 the 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 x10 the load in a matter of seconds or minutes, your traditional firewall cannot! Instead, you will have to deploy x10 ‘virtual’ appliances in your environment, configure each of them to pull the right access policy, and hope nothing was missed in this cumbersome process.

Our suggestion is to 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”.

3. Look for automation and integration abilities in your security solutions

So far, 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 as Security Automation And Orchestration or 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.

We suggest that you look for solutions which are well-documented and have well-maintained APIs, 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 about!

Security Automation and Orchestration (SOAR) simply defined:
A coordination of automated security tasks 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 cybersecurity professional.

Security Orchestration - the connecting and integrating of various security applications and processes together.

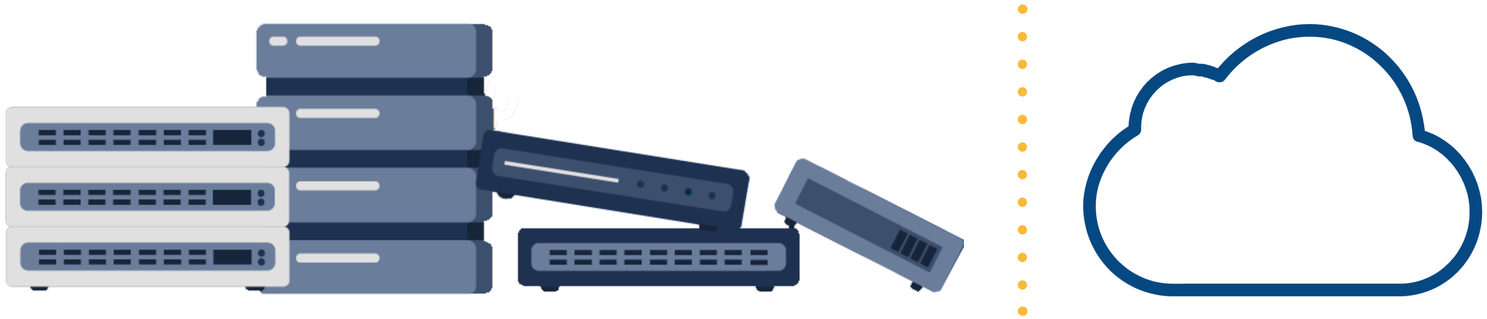
4. Take the opportunity to adopt new models and approaches for old problems

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 detections is the 'new norm' for detection solutions. All 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 that is not available 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'.

Network security is another good example of the mind-shift process. Shifting from the traditional approach of a perimeter that is secured via IP based access rules (the castle and moat approach) to a software-defined-perimeter model that creates a Zero Trust approach. The SDP and Zero Trust models determine the level of network access based on a combination of identity, device and application context instead of an IP:Port based approach. Leveraging 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.



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

The combination of on-premises and cloud-based datacenters 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 it 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?

Most probably the answer to both questions is 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.

In conclusion.

Following the suggestions outlined in this whitepaper will eventually allow you to provide a flexible and agile service, one you can quickly and easily adapt to the constantly changing needs of your business. A service which will provide better security across your company's assets, whether they are hosted in the cloud or on-premises, and eventually provide a better experience to your internal and external users and customers.

To learn more, visit our website at www.luminate.io or contact us for a short and insightful demo

CONTACT US

Luminate Secure Access Cloud™

Luminate enables security and IT teams to create Zero Trust Application Access architecture without traditional VPN appliances. Its Secure Access Cloud™ securely connects any user (be they employees, contractors, business partners or customers) from any device, anywhere in the world to corporate on-premises and cloud-hosted applications while all other corporate resources are cloaked. No 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, therefore, can be deployed in less than five minutes, without forcing a disruptive change in the organization's existing architecture, user permissions and applications. Luminate's Secure Access Cloud™ provides full governance and real-time enforcement of users' actions in each corporate application.

Vendor validation checklist

- ☐ Evaluate the vendor's multi-cloud support, technological scale (more load) and economical scale (price).
- ☐ Favor vendors who are cloud agnostic, 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, etc.).
- ☐ 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 on-premises level of service as good (or better) as their service for cloud environment and leverage your existing investments.