Why Managed Security-as-a-Service is the Next Big Thing

By Rishikesh Kamat
Vice President - Products and Services

Not long ago, enterprise security was all about securing the perimeter, encrypting data and installing the firewalls. Nonetheless, if you are living by the same rules in today's business environment, you are headed for a security disaster.

Flexibility and business agility offered by increased use of digital technologies (cloud, big data, mobile, IoT and artificial intelligence) has come with a caveat—increased security complexities. Growing interconnected systems, mobile devices and open platforms has increased data touch points both within and outside the firewall. With data assets spending a lot of time in transit, the risk of vulnerability to virus, ransomware, identity theft and unauthorized exposure to data has increased manifold.

No wonder, the frequency, magnitude, sophistication and cost of security incidents are rising every year. Several big names have been the victims of cyberattacks, which resulted not only in huge financial losses but also loss of reputation. As per the projections of a US research company Cybersecurity Ventures, cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

MARKS THE SPOT IN THE EVOLVING THREAT LANDSCAPE

As enterprises continue to add new applications, devices and workloads across functions and geographies in the multi-cloud world, the risk too will continue to mount from all directions. In this ever-evolving threat landscape, how can enterprises ensure security, while staying competitive and agile? Those enterprises thinking that taking preventive measures and steps against security breaches and threats is good enough, have completely missed the point. The need of the hour is proactive not preventive security.

That said, in-house IT teams usually lack the skills as well as budgets to meet increasing security demands. More and more enterprises are thus looking at outsourcing security and get their security demands fulfilled without having to come up with their own infrastructure or invest in developing, maintaining, and creating these resources. Leveraging the power of cloud to provide security and compliance services, Security-as-a-Service (SeCaaS) is emerging as a viable option for staying ahead of the cyber security curve. Pay-as-you go option coupled with speed, agility and ability to scale up and down are the key benefits that have led to the popularity of SeCaaS model. Many experts believe that security outsourcing will become a necessity in the future.

While taking the decision to adopt SeCaaS is easy (and a smart one), choosing the right provider for maximum benefits is a more difficult decision that requires careful evaluation. Consider these criteria before getting started on your SeCaaS journey:

BUSINESS UNDERSTANDING AND INTEGRATION WITH SYSTEMS

Analysing the partner's understanding of your business is a good place to start. It is essential for the SeCaaS provider to have a clear view into your organization's compliance requirements, department-level challenges and even culture. This is crucial as the partner should be able to suggest solutions that best fit your business. Also, extremely important is to make sure that the solution you select works well with business systems already in use and in-house existing security solutions. It is always a great idea to work with a provider that has many services in the cloud (such as IaaS, PaaS, DRaaS) as it allows for bundled pricing and better interoperability.

Ability to scale with your enterprise: It's important to understand that the threat vectors will continue to increase as your enterprise grows and adopts new technologies and expands its digital footprints. Look out how much experience the partner has in dealing with complex security environments, such as multi-cloud and hybrid IT. Also, the ability to keep pace with changing threats is a crucial check point. A provider with a global reach can completely fit the bill as it will ensure that the provider is on top of the evolving threat scenario. Further, the provider should be able to offer you flexibility to change and expand your services as your security infrastructure grows.

Spectrum of Service: One of the key points to look for is the range of services offered by a provider. An enterprise environment has a mix of legacy systems and advanced cloud-based systems. For effective security, it is important to make sure that the provider is equipped to handle a comprehensive array of environments. The provider should be able to adopt a holistic view towards security by taking into account all the aspects right from risk management, auditing, disaster recovery, compliance to even training.

EXPERTISE

Security is a broad subject and it is practically impossible for an enterprise to have an expert on each aspect. Access to trained security talent and experts across various aspects, including network and infrastructure protection, DC workloads and endpoint protection and application and data protection, at an affordable price point is one of the biggest pluses of SeCaaS model. Look for a provider who has its own Security Operation Centre ((SOC) with a highly skilled team that manages the operations on a 24x7 basis. This ensures that your security and compliance requirements are met round-the-clock and SeCaaS provider serves as an extension of your in-house security team.

Shared model: Look for a provider that offers a shared services option, for instance a shared SOC. Multi-tenant hybrid approach enables an enterprise to have a few dedicated resources with the flexibility for additional scalability. A shared model is a win-win as it allows access to wider security, 24x7 support and access to skilled security professionals at a much lower price point.

Best-in-breed security products: The provider's platform should integrate best-in-breed security products and technologies from a wide range of security service providers. A strong technology partner ecosystem ensures that you can make decisions that best support your infrastructure and security requirements.

FLEXIBILITY ACROSS ENVIRONMENTS

Check if a SeCaas provider has extensive experience across all environments and delivery models, including public, private and hybrid clouds. This flexibility will help you benefit from the provider's experience in creating a multi-strategy that will enable you to meet your current and future security needs.

Enterprise security is something that today's businesses can't afford to ignore or go wrong with. Choosing the right SeCaas provider is tough (especially with the plethora of options available) but a business-critical decision. Closely analysing your security challenges and requirements and matching them with the SeCaaS provider's capabilities can help you choose the right fit for your business.