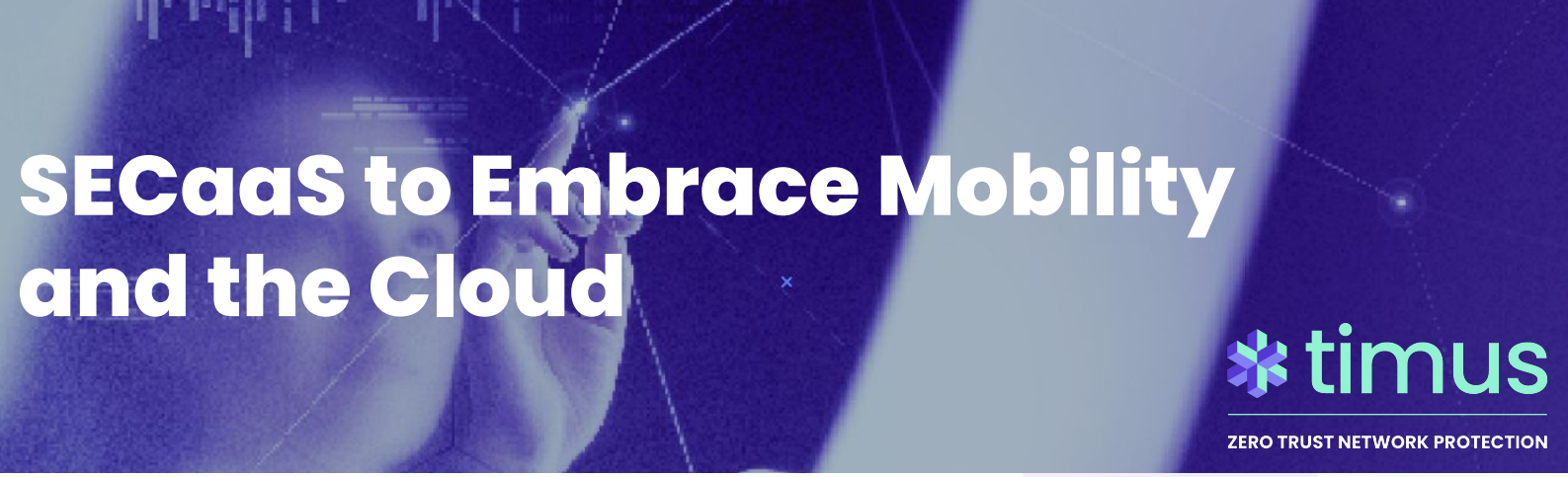


SECaaS to Embrace Mobility and the Cloud

timus
ZERO TRUST NETWORK PROTECTION

Introduction

"The enterprise data center is no longer the center of access needs for users and devices," Gartner said in a 2019 report. At the time, on-premises networking and application hosting were already becoming things of the past. As more and more applications resided outside the network, users were already starting to rely on SaaS applications and cloud services. But all these rapid changes would also lead to new security risks.

In this new environment, where cloud usage and mobile technologies advance at a dizzying pace, network architectures of the past can no longer be relied upon to meet our security needs. In other words, traditional network security methods are simply no longer effective in a cloud-based and increasingly mobile world. Today, users no longer work from the office; rather, they have become accustomed to working virtually anywhere.

The SECaaS (Security as a Service) model, in which key security functions are provided as a cloud service, is becoming increasingly popular, just like other cloudbased services in the last decade. That's because SECaaS is easily accessible, reliable and scalable.

According to one recent report, the global SECaaS market was valued at $9 billion in the first year of the pandemic but is expected to reach a staggering $23 billion over the next four years. If you're not yet familiar with SECaaS, this white paper will help you understand how it is helping businesses meet the cybersecurity challenges of the 21st century – and what you need to consider when migrating away from the outdated security architectures of the past.

In a cloud-based and mobile-first world, traditional methods of network security are no longer effective.

© Timus Networks, Inc. 2025. All Rights Reserved.

Contents

What is the SECaaS Model? 3–5

How does SECaaS Help Modern Businesses? 6

What are the Benefits of SECaaS for Cloud Services? 7

5 Things to Consider When Migrating away from On-premises Security 8–10

Conclusion 11

© Timus Networks, Inc. 2025. All Rights Reserved.

What is the SECaaS Model?

In its infancy, "Security as a Service" simply referred to antivirus software. But today, following the emergence of the SaaS (Software as a Service) model, the term has acquired a whole new meaning since it doesn't require on-premises hardware and allows users to sidestep significant costs.

Wikipedia's entry on SECaaS describes it as "a business model in which a service provider integrates their security services into a corporate infrastructure on a subscription basis more cost-effectively than most individuals or corporations can provide on their own, when the total cost of ownership is considered." In other words, it's a convenient means of outsourcing security-related services to a highly qualified third party. Unlike the traditional on-premises service model, the service provider delivers these solutions via the cloud.

SECaaS allows internal IT and security teams to focus on core business needs

The cloud-based SECaaS model lets organizations outsource crucial security tasks such as security monitoring, threat detection and remediation to dedicated teams of external security experts using advanced solutions allowing internal IT and security teams to focus on core business needs.

Like workforce shortages in other areas, the persistent lack of cybersecurity skills remains a problem for many businesses. But by outsourcing critical security functions to a third party, security experts can monitor your networks around the clock while enjoying an advantage that can save you both time and money.

Essentially, SECaaS is a cloud-based method for outsourcing cybersecurity by which customers subscribe to security services. It is an increasingly popular option for many companies since it is easier to scale as businesses grow. It also allows businesses to avoid the expense of creating complex, on-premises security architectures.

The Cloud Security Alliance (CSA) is an organization dedicated to defining secure cloud computing and raising awareness about novel cybersecurity threats. In so doing, the CSA has defined the following categories of SECaaS tools:

© Timus Networks, Inc. 2025. All Rights Reserved.

Network Security
consists of security services that allocate network access and distribute, monitor and protect network services.

Security Assessments
are third-party audits of cloud services based on industry standards.

Email Security
controls incoming and outgoing email, thus protecting organizations from phishing, malicious attachments and spam. It also provides business continuity options.

Identity and Access Management (IAM)
provides identity administration, governance and access controls. It also includes authentication, identity assurance, access intelligence and privileged user management.

Encryption
is the process of hiding data using cryptographic and numerical passwords. It often involves the conversion of plain text into ciphertext

Intrusion Management
is the process of using pattern recognition to detect statistical anomalies, prevent and detect intrusion, and manage intrusion incidents.

Data Loss Prevention (DLP)
is the monitoring, protection and verification of data security at rest, in motion, and in use.

Security Incident and Event Management (SIEM)
systems accept log and event information, correlation and incident data, and provide real-time analysis and correlation.

Business Continuity and Disaster Recovery (BCDR)
is the implementation of measures designed to provide operational resilience during a service interruption.

Web Security
offers real-time protection of public application services, typically delivered by proxying web traffic through a cloud service provider.

The SECaaS model allows businesses to outsource their security needs to a provider that operates within the cloud. The provider can manage security services, such as authentication, intrusion detection, antivirus and malware management, etc. Service management is generally performed off-site with the provider's hardware and cybersecurity equipment.

The company typically pays a fee to keep its business operations up and running without investing in software or staff. For online businesses without a physical location, SECaaS provides the necessary protection while being less expensive than hiring dedicated threat detection experts.

© Timus Networks, Inc. 2025. All Rights Reserved.

Although the range of services varies from vendor to vendor, you can expect most of the following to be covered by a SECaaS model:



Device Security

Working with customers to develop security policies and configurations for company-owned and personal devices used for business.



Application Security

Standardizing authentication policies across all SaaS applications, allowing for measures such as multi-factor authentication and single sign-on.



Compliance

Working with clients to develop processes that fully comply with industry-relevant regulatory frameworks.



Monitoring

Detecting – and, if necessary, blocking – suspicious network traffic.

SECaaS provides the necessary protection and is cheaper than hiring dedicated threat-detection experts

© Timus Networks, Inc. 2025. All Rights Reserved.

How does SECaaS Help Modern Businesses?

IBM's Cost of a Data Breach Report 2021 notes that the average cost of a data breach increased by nearly 10% year-on-year, the largest single annual cost increase within the last seven years. It also asserted that remote working and digital transformation due to the COVID-19 pandemic had dramatically raised costs associated with data breaches. The report estimated that the average cost was $1.07 million higher in breaches where remote work was a causal factor. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely.

Considering the average cost of a data breach, SECaaS represents a sound investment for most businesses. But it isn't just about the cost since most businesses also face the following risks:

- Theft of intellectual propert
- Loss of competitive advantag
- Damage to brand reputatio
- Loss of customer
- Regulatory fines

Network security is no longer a case of simply installing one or two firewalls at the edge of your network and enforcing a strict security policy. As cybercriminals become more sophisticated, cybersecurity is becoming more involved for businesses.

Organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches

Security as a Service can protect companies whose data is located on laptops, mobile phones, tablets, local servers, edge servers and cloud servers. Each of these devices and platforms must be secured. SECaaS can protect all of them from an ever-growing number of threats, such as malware, ransomware, phishing, viruses, Denial of Service (DoS), Distributed Denial-of-Service (DDoS), brute force attacks, etc. It is rapidly becoming the method of choice for both small and large enterprises, and this is due to its many advantages, which include lower costs, greater reliability, and enhanced threat monitoring.

Today's CIOs are being called upon to shift their focus from basic infrastructure projects to strategic initiatives that drive business value, such as moving security to the cloud, increasing business agility, and generating larger returns on investment. This approach frees up company resources, allowing CIOs and CISOs to think more strategically and

© Timus Networks, Inc. 2025. All Rights Reserved.

What are the Benefits of SECaaS for Cloud Services?

Current cloud technologies assume that the cloud provider secures the cloud. SECaaS, on the other hand, allows the users of one cloud to benefit from security measures provided through other clouds. SECaaS provides security as a service that users can subscribe to. That means cloud users are no longer limited to the security solutions offered by their particular cloud provider. Such an approach yields numerous benefits, which contribute to making it:

More Economical
It eliminates the cost of purchasing and managing multiple network security devices.

Better
It continuously inspects internet traffic and correlates threat data in real-time, providing better security.

Faster
Connecting directly to the security service edge provides the shortest path to your internet destination, resulting in a faster user experience.

Equitable
It closes corporate vulnerability gaps by non-network users and those who connect directly to cloud apps and the internet. If you can't secure every connection, you're leaving your entire network vulnerable to attack.

Talented
Most SECaaS vendors are well established Cybersecurity companies with teams of experts who understand the latest trends and adhere to current cybersecurity best practices. Most SMEs can't afford such expertise.

Responsive
Moving your security infrastructure to the cloud makes your organization more agile, allowing you to quickly adapt to evolving threats and changing stakeholder needs.

Rapid
Experts manage deployment, configuration, tuning and training, so your solution is up and running quickly.

Simple
As a cloud service, it offers the functions of a traditional internet gateway while also reducing the cost and complexity of network security.

Visible
It provides a clear picture of your IT infrastructure, allowing you to assess your security posture and understand your environmental risks.

Consistent
All connections are constantly audited and secured regardless of user, the app accessed, or the employed encryption.

Centralized
An integrated cloud solution gives you a centralized view across all services, such as firewall, sandbox, secure web gateway, bandwidth control, etc.

Scalable
Cloud security is infinitely scalable. Even when encrypted, it easily handles spikes and inspects all traffic without affecting overall performance.

Up to date
The SECaaS provider will take care of all activities by the employer. They can provide the latest patchwork for day-one protection against newly discovered vulnerabilities and viruses.

24/7
SECaaS providers have multiple teams on standby to tackle any problem or threat. They typically offer 24/7 uptime, thus ensuring round-the-clock protection.

Efficient
Because many SECaaS functions are automated, internal IT resources can be allocated to more critical tasks.

© Timus Networks, Inc. 2025. All Rights Reserved.

5 Things to Consider When Migrating away from On-premises Security

Today, many businesses operate entirely on the cloud or in a hybrid cloud environment. Organizations are increasingly looking to secure cloud migration to move applications, data and entire IT infrastructures to remote server facilities. According to the Cloud Computing Study 2022, 69% of organizations have accelerated their migration to the cloud in the last 12 months. The percentage of companies that maintain most or all of their IT infrastructure in the cloud is expected to jump from 41% today to 63% within a year and a half.

During and after migration, SECaaS vendors will be on hand to deal with any potential security threat, including data breaches, phishing scams, and distributed denial-of service attacks. SECaaS vendors combat these threats by using the cloud to integrate their services with your existing infrastructure. 69% of organizations have accelerated their migration to the cloud in the last 12 months

- If you think you're ready to move to the
- SECaaS model, there are five key points
- to consider. These are:

69% of organizations have accelerated their migration to the cloud in the last 12 months

1. Know how to assess the provider

When reviewing a vendor, inquire about their processes for protecting data throughout the entire lifecycle. Also, try to choose a vendor with experience in your particular sector. Having a familiar provider with how your business runs will make the transition to SECaaS that much easier.

2. Clearly define and assign responsibility

SECaaS allows organizations to perform the "handling" of security functions, but not the "responsibility" that should go with it. Therefore, a shared responsibility model is critical to ensuring the success of your SECaaS engagement. Get a clear idea of who has access to your data and what data they have access to. Know where audit logs, user credentials and other important data are stored and precisely how they can be accessed. Your contract should clearly state how data ownership is determined, what the data-protection obligations are, and how those obligations will be enforced.

© Timus Networks, Inc. 2025. All Rights Reserved.

3. Know what to outsource

Security service providers can offer a broad and expanding range of capabilities, recognizing that some functions are better left in-house. What's happening on your network could be an attack, or it may simply be normal traffic – and the service provider may not be in the best position to know the difference, especially in a crunch. Similarly, security functions like SIEM can be difficult for a third party who lacks a perfect understanding of what's normal – and what isn't – for your network and endpoints.

4. Have a strategy for managing risk

Outsourcing security to a third party comes with a certain amount of risk, regardless of your precautions to minimize it. So, when assessing the value provided by SECaaS, you must first fully understand the risks associated with using the model – and decide how you want to manage them. Common strategies include accepting the risk, mitigating it through physical, administrative or technical control, avoiding practices that contribute to risk, and transferring risk to a third party, like an insurer.

5. Be prepared for a learning curve

Organizations that take the SECaaS route can be blindsided by changes if they're not prepared. Having security delivered as a service constitutes a major architectural change, which can affect, among other things, your other existing IT controls and practices. So brace yourself for the challenge!

Organizations that take the SECaaS route can be blindsided by changes if they’re not prepared

© Timus Networks, Inc. 2025. All Rights Reserved.

Now that you know the main factors to bear in mind, here are five more things to consider when choosing a service provider:



Availability

Cyber attacks can happen at any time. Security providers need to be available to alert you to possible threats and mitigate any potential damage. That's why it's also important to know how responsive a vendor will be if and when you contact them.



Response time

If an attack occurs, the vendor must have a fast response time to neutralize the threat quickly. A SECaaS provider must ensure that everyone who should be informed is immediately made aware of the intrusion so that the right countermeasures can be speedily taken.



Compatibility with your existing systems

Make sure that whatever security provider you choose can support most of the SaaS and on-premises applications that you already have in place. Working with a single security provider is much more economical and safer than working with a patch job.



Variable pricing

Variable pricing is one of the strengths of SECaaS solutions, as it ensures that you only pay for the services you need. For example, users pay for endpoint security software based on the number of endpoints they want to protect. Pricing should include the ability to mix and match services, so you're not locked into using a single vendor. For example, the costs for a SECaaS vendor's security software used by your IT department should be separate from those for managed services provided by the vendor.

© Timus Networks, Inc. 2025. All Rights Reserved.

Conclusion

In this emerging world, business is dynamic, users are mobile, and the protection of networks has become all-important. The power of mobility, cloud applications, social media, and digital platforms is challenging the traditional enterprise network security notions. You need next-generation IT security that will deliver the economies of scale, enhanced security and flexibility you require to achieve your objectives.

The Security as a Service (SECaaS) model, or the notion of outsourcing security, is hardly new. Companies have been moving towards it for years. Today, most businesses receive at least some of their IT infrastructure "as a service," meaning they use third-party services to provide and manage their software applications. But the SECaaS model began getting more attention in 2020 when most companies shifted their workforces from their offices to their homes.

The use of SaaS solutions increased dramatically during the pandemic period, and it's clear that this trend will continue. With the increasing complexity of enterprise security requirements, cloud security represents one of the best ways to ensure business resilience. Therefore, it is not surprising that the SECaaS concept has recently come to the fore.

SECaaS began getting more attention after most companies adopted remote-work models

© Timus Networks, Inc. 2025. All Rights Reserved.

IT departments have struggled to protect their data as they expand access to devices, solutions, and information to ensure business continuity during global emergencies. Undoubtedly, IT departments at millions of companies have done heroic work, and today they're looking to consolidate earnings and optimize security. Forward-thinking professionals are meeting new challenges by upgrading security architecture, taking fresh approaches to notions of governance, and evaluating existing vendors. All these steps will enable their companies to take advantage of the current SaaS environment and mitigate risks in the most effective ways possible.

Whether you're looking to save money, boost efficiency, or protect your infrastructure from novel security threats, services like SECaaS can provide enormous value to your organization by strengthening your defenses and improving your bottom line.

timus

timusnetworks.com

About Timus

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.