NTT Security

Whitepaper

# Complexity, cost, compliance: The three Cs driving interest in Security as a Service

## Security gets harder to manage every day.

The march of mobile, IoT, and cloud-based workloads is escalating user- and device-generated data volumes, user activity and compliance requirements. Security leaders have to strike a balance between scanning the horizon for future threats while juggling a growing in-tray of right-now responsibilities.

Trying to do that with on-premise solutions is fast becoming a corporate headache – stressing budgets and drawing more and more skilled resource from an already stretched IT talent pool. CSOs and CISOs are naturally looking for alternatives.

This paper looks at the rising popularity of Security as a Service (SECaaS), and the steps that NTT Security recommends organizations should take when considering moving their security solutions to the cloud.

### It used to be easier

Today's IT is mobile, shaped by an explosion in endpoints connected across highly distributed networks. Workers bring their own devices and applications to the office and constantly move data in and out of the cloud, while the vast industrial deployment of IoT creates new threat vectors that have to be defended.

It's safe to say that the complexity around security management is growing, while the frequency and effectiveness of attacks is on the rise. Proof isn't hard to find. Consider these breaches from 2017 alone:

### Torn from the headlines

- In January, a college in the US was compelled to pay hackers $28,000 USD in bitcoin to unlock files after a ransomware attack.[1] The incident occurred over the winter break and caused widespread disruption to online financial aid, email and voicemail systems, while locking out 1,800 students and staff from their computers. This raises the need for integrating security services without on-premise hardware by providing cloud-based security for centralized security management, managed threat detection and additional visibility into IT infrastructures.
- Research from the NTT Security Global Threat Intelligence Report 2017 showed that phishing attacks were responsible for as much as 73 percent of malware being delivered to organizations.[2] Implementing and running on-premise anti-phishing solutions can be challenging and expensive. In February 2017, the US Internal Revenue Service warned of a fraud in which phishing emails masquerading as legitimate communications from tax software providers would arrive during the tax season.[3] Today, it is increasingly important to adopt more robust cloud-based anti-phishing solutions that can be quickly deployed in a timely manner, are scalable to the needs of the business and offer end-to-end capabilities such as monitoring and detection of advanced phishing attacks, and response and resolution of these incidents.

With enterprise IT teams at the receiving end of 578 security alerts a day[4] on average, CSOs and CISOs face a growing challenge in terms of how to remain focused on the bigger picture. They need time and resources to track shifts in the threat environment and develop long-term strategies to defend against attacks or minimize the impact.

*1. LA Times 2. NTT Security Global Threat Intelligence Report 2017 3. US Internal Revenue Service Press Release: Security Summit Alert: Tax Professionals Warned of New Scam to "Unlock" Their Tax Software Accounts 4. SC Magazine - Balabit CSI Report*

## The challenges of modern cybersecurity management in the cloud age

Compliance is another area making the lives of CSOs and CISOs more difficult. Private and public sector organizations alike face a growing number of expanding regulatory regimes – globally, within trading blocs like NAFTA and the EU, and often in parallel with industry-specific rules and national differences in implementation.

On the GDPR alone, Gartner predicts that more than half the companies affected by its requirements won't be fully compliant even after a year.[5]

Boards and executives are also much more conscious of security as a business and reputational issue, especially when increasing their digital footprint through cloud migration. As breaches occur at other businesses, they will want to know if their own organization is susceptible. That puts pressure on CSOs and CISOs to provide clear and persuasive (e.g. data-supported) answers in order to seed confidence.

### How complexity drags down security effectiveness

1. Declining IT productivity
2. Missed vulnerabilities
3. Inconsistent policy and governance
4. A muddied accountability picture
5. Technology investments failing to deliver full ROI
6. Potential communication gaps with senior management
7. Poor technology integration
8. More active endpoints than can be effectively tracked or managed

The highly-changeable threat landscape provides the backdrop for all of this. While some types of attack are becoming commoditized, the rise of advanced persistent threats (APTs) requires investment in advanced technologies; which typically bring complexities of their own in terms of configuration and maintenance.

Basic or advanced, the practical reality of security infrastructure management places strong emphasis on responding to all the alerts generated by intrusion detection, firewalls and other systems. Security teams now face a hailstorm of notifications, many of them false positives or duplicates replicated on different machines and in different environments - cloud, hybrid, on-premise and virtual. Aside from being time consuming and labor intensive, responding to these can distract analysts from seeing the red alerts that could indicate a serious breach.

It's been normal in this environment for enterprises to seek support and counsel from trusted third parties to help evaluate their security posture and improve the effectiveness of security operations. Now they are asking security providers to take on more of the burden – to manage the end-to-end security lifecycle of critical assets in multiple cloud and on-premise environments on their behalf and reduce complexity, costs, and adequately mitigate risk. This emerging model is called Security as a Service (SECaaS).

## What is SECaaS exactly?

By enabling companies to access security services through the cloud, SECaaS has the potential to make life easier for CSOs and strengthen each organization's IT defense posture.

The key technologies that would have been run on-premise are deployed and managed by a managed security service provider, allowing CSOs and CISOs to rapidly access state-of-the-art security capabilities on-demand, while keeping capex and operational costs to a minimum.

It works by combining automation with continuous monitoring by human experts. Alerts are reviewed and analyzed around the clock, triaged for risk level and appropriate management steps taken. Visibility to serious threats is increased, making it easier to take action and stop them from causing significant damage.

As it relies on the experience and intervention of seasoned security experts, SECaaS relieves CSOs of much of the need to recruit, hire and sustain extensive in-house skill sets. The infrastructure itself is constantly updated with the latest versions and patches in the background, meaning minimal disruption to operations and less reliance on end users to achieve compliance.

Technologies delivered under SECaaS include:

- Business continuity and disaster recovery (BCDR or BC/DR)
- Continuous monitoring
- Data loss prevention (DLP)
- Email security
- Encryption
- Identity and access management (IAM)
- Intrusion management
- Network security
- Security assessment
- Security information and event management (SIEM)
- Vulnerability scanning
- Web security

A full service offering could also wrap in business continuity and disaster recovery (BCDR or BC/DR), data loss prevention (DLP), email security, web security, encryption, identity and access management (IAM), security assessments and vulnerability scanning.

## Who is responsible for what?

While the list of potential services is comprehensive, any organization considering SECaaS won't be able to completely hand over compliance to a third-party provider. Data and privacy laws, plus regulations such as the GDPR will compel any SECaaS customer to take ultimate responsibility for protecting sensitive information.

Vital security functions can be performed by the security provider, but the customer remains responsible for the correct configuration and implementation of SECaaS. All controls and policies migrated to a SECaaS provider would also need to be consistently reviewed and kept up to date. Any company considering a move to SECaaS should ask providers if they can provide guidance and assistance in these areas as part of the service offering.

*5. Press Release: Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation*

## Other considerations: Choosing the right model

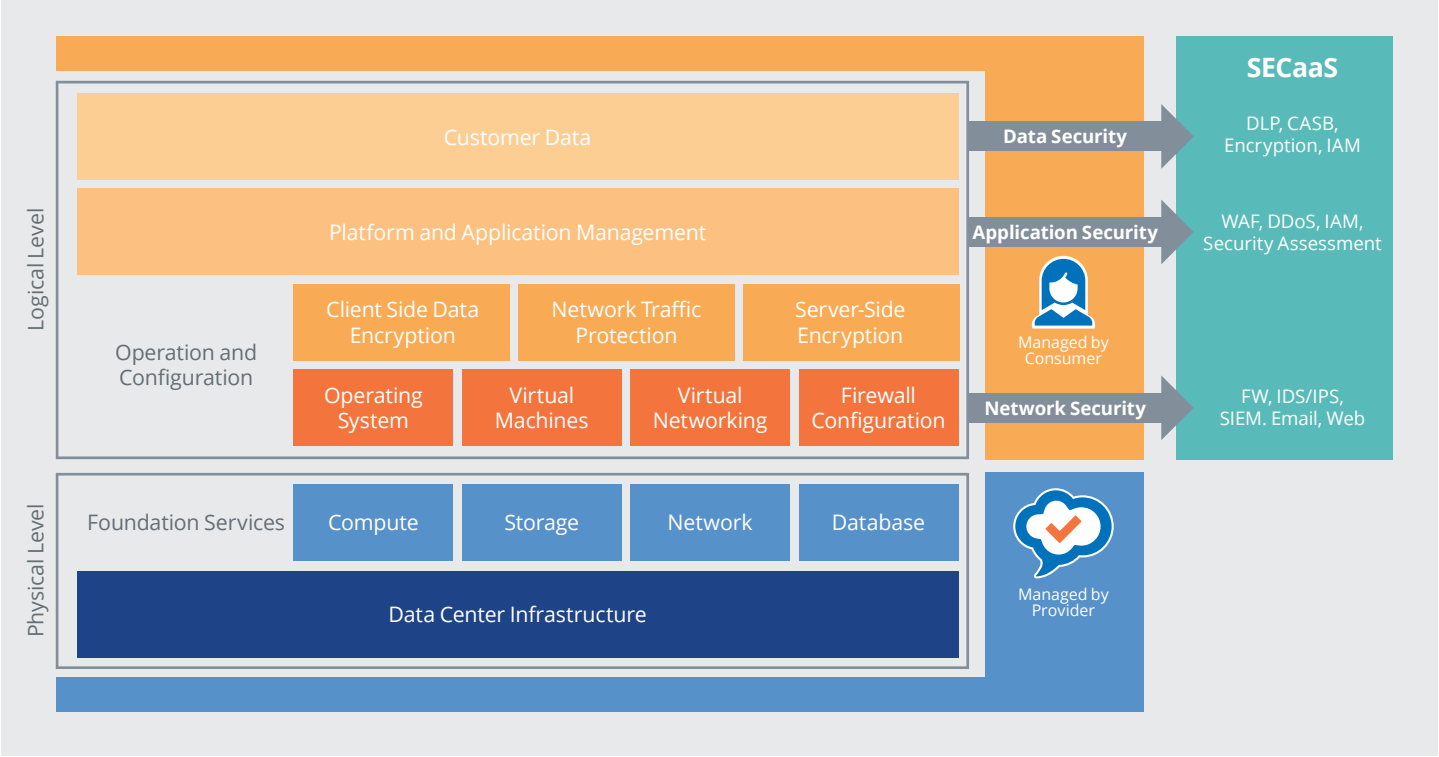
As organizations adopt cloud capabilities they also adopt a mix of security responsibilities, risks and issues. It is important to understand the dependencies and responsibilities between the three main cloud computing models, IaaS, PaaS and SaaS, and how they relate to SECaaS.

- **IaaS** provides the consumer or client organization's infrastructure resources with extensive flexibility and control; however, this puts the onus on the consumer to secure applications, runtime, middleware, and infrastructure. Examples under this model could include Amazon EC2 and Microsoft Azure IaaS.
- **PaaS** provides a platform from which web applications can be developed and deployed by the consumer. Responsibilities can be split between both parties. SECaaS solutions include more application-based controls such as application scanning and secure web gateways (SWGs).
- **SaaS** on the other hand provides a consumable service with built-in functionality and the highest level of integrated security – for which the provider bears the greater responsibility. As a trade-off however, the consumer must hand over flexibility and control. Examples under this model could include O365 or Salesforce.

The service model has a direct impact on the level of responsibility assumed by the organization. More flexibility and control necessitates complementary security services provided by SECaaS.

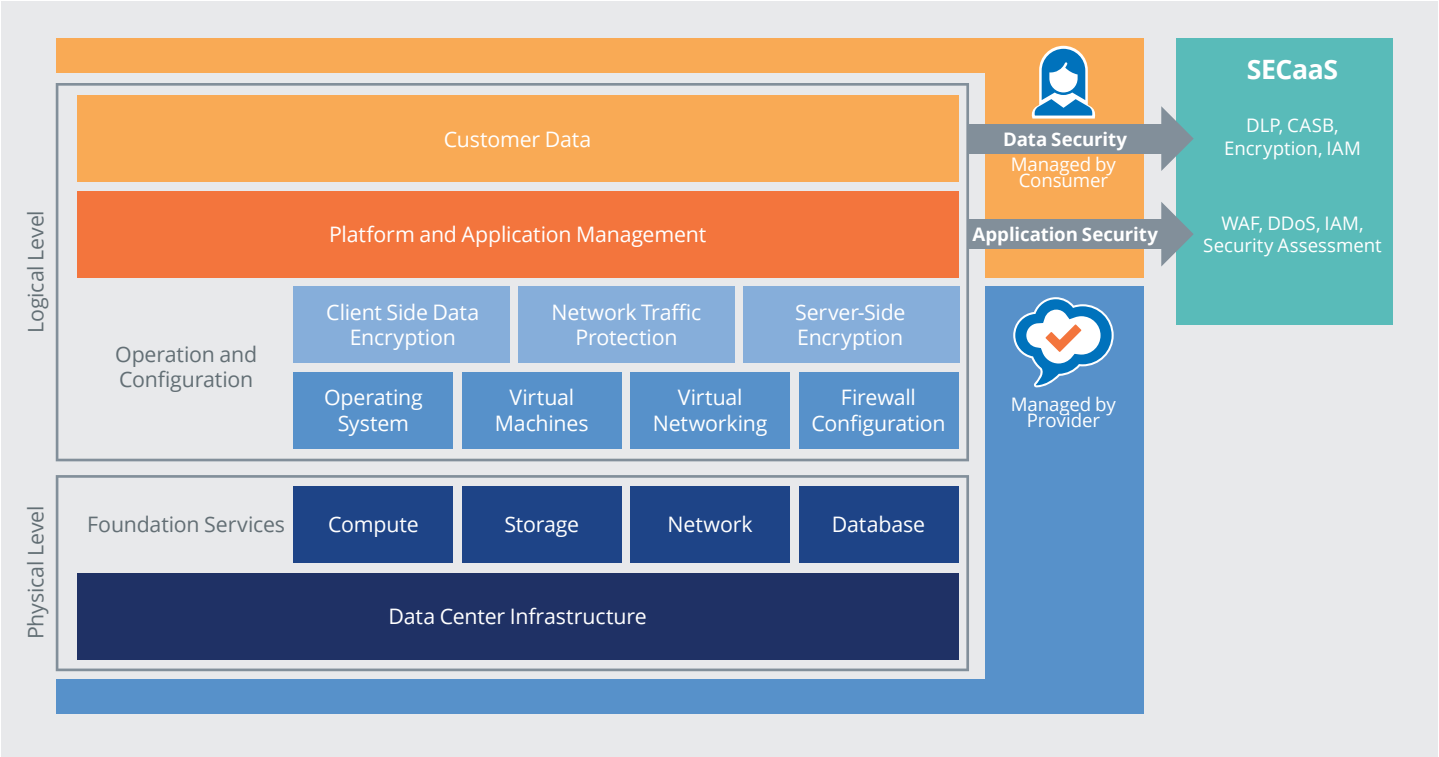
For example, organizations that adopt an infrastructure services model are arguably in a better position to leverage the full benefits promised by SECaaS. The diagram below shows the types of SECaaS offerings that can be mapped to infrastructure responsibility areas.

**Figure 1** : Shared security model – Infrastructure as a service (IaaS):



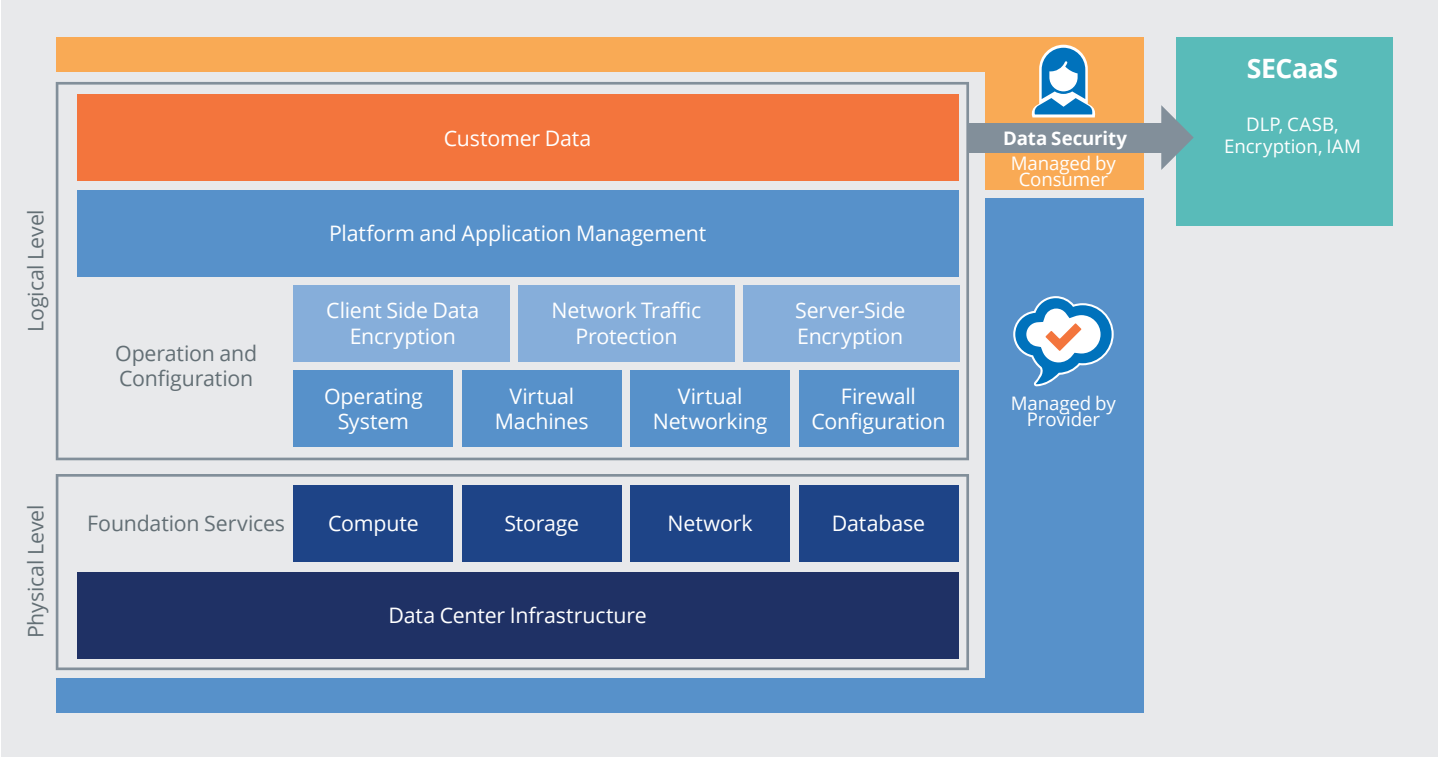

In contrast, SaaS or abstracted service models are less reliant on SECaaS offerings to secure areas of consumer responsibility, due to the provider already integrating many security functions as part of the service. However, these integrated security functions can often prove inadequate for mitigating advanced persistent threats (APTs), especially those already inside the consumer's network, due to their focus on prevention rather than detection and response.

**Figure 2** : Shared security model – Platform as a service (PaaS)




Although abstracted or containerized services may have integrated technologies like WAF or DDoS protection, the consumer may still need to configure and monitor these services to gain the highest levels of control and mitigation.

**Figure 3** : Shared security model – Software as a service (SaaS)



## Choosing the right SECaaS service provider

Organizations looking at outsourcing security management via a SECaaS or managed security service provider (MSSP) share similar objectives: lowering costs, automating processes, easing compliance, and gaining access to the latest advanced services and technology. The choice however often boils down to which key capabilities you are happy to do without.

Choosing an MSSP, for example, who can't deliver services under a SECaaS model, might provide the benefit of handing over time-consuming tasks, but at the expense of additional hardware investments to support the managed service.

Working with an end-to-end specialized security provider who can assess your existing infrastructure with expert consultants and strategically plan, design and deliver the right managed services on-premise, is arguably the best way to reap the full benefits of SECaaS.

You can take advantage of scalable on-demand services, make use of advanced enterprise security such as managed detection and response services (advanced analytics, applied threat intelligence, rapid incident response etc.) without capital investment, and still pass the burden of comprehensive security monitoring and management to the provider.

### Other key questions you should ask when assessing a SECaaS provider:

1. To what extent does the provider's automation capability speed up response time and accurately triage notifications by risk level?
2. How soon can the provider respond if a problem is detected?
3. How frequently is the provider's technology updated to address the evolving nature of attacks and take advantage of the latest innovations?
4. Does the provider monitor 24/7 and what security assurances do they provide?
5. What level of experience, technology expertise, and seniority is on offer within the provider's consultant team?
6. Does the provider offer you a centralized management interface for managing multiple SECaaS solutions?

This last question is crucial. It is very common for organizations to find themselves with a mixture of legacy and new technology, adding complexity in terms of management and complicating how actionable security and risk information is visualized.

While the SECaaS provider is responsible for the management and operation of hardware and software that is used to deliver the service, customers need a web-interface console to view their managed security environment, and perform any compliance-related control tasks that need to be managed in-house.

## Conclusion

As NTT Security's 2017 Global Threat Intelligence Report has shown, security combines technology, processes, and people working together. Simply throwing more technology at a security problem without taking into account processes, and the type and level of resourcing required to manage it all, may do more harm than good. Also, with threats evolving so quickly, most organizations can't possibly add new security technologies at a pace which can keep up with evolving threats – let alone maintain it to full effectiveness.

It wasn't so long ago that security was a number one barrier to cloud adoption. But the benefits of the SaaS model have fuelled rapid adoption and forced innovations that weren't there just a few years ago. Leading cloud providers have now embedded security into their infrastructure, and arguably created environments that are not only as secure as traditional on-premise, but potentially even better.

As regulations and governance expectations focus more and more on the need for adequate security, SECaaS offers a tantalizing opportunity to improve security and compliance while simplifying operations and controlling costs.

## A SECaaS use case

A CISO is concerned about the rate at which the business is adopting SaaS applications without a method or policy in place to assess the suitability of each application's security.

Many SaaS applications are being used by the business without having undergone sufficient risk assessment. As a result, the company does not have sufficient visibility into the applications and the data shared within them.

Despite this, the CISO is reluctant to block access to cloud services. The company has noticed a significant increase in productivity since departments have been able to choose the tools that best fit their needs.

An upcoming GDPR audit however has focused minds. The CISO is concerned that the company does not have sufficient resources to gather all the information required before the deadline.

The CISO decides to deploy Cloud Access Security Brokers (CASBs) to address these concerns. CASBs are security policy enforcement points, placed between cloud service consumers and cloud service providers to apply enterprise security policies as cloud-based resources are accessed.

As a solution, CASB provides:

- Visibility into cloud usage
- Risk assessment of SaaS providers
- Compliance reporting
- Data loss prevention
- The ability to set granular policies per SaaS solution, while giving the CISO swift access to CASB tools via the cloud.

## About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.