Cloud Security Services

Securing your end-to-end cloud journey.

Building digital trust in cloud solutions

The journey to cloud is accelerating as organizations recognize the competitive advantages that can be harnessed in today's digital world.

Achieving market differentiation demands agility and the exploitation of capabilities centered around big data, data analytics, machine learning and artificial intelligence (AI). This allows organizations to adopt Internet of Things (IoT) capabilities and deliver digital-based transformation programs.

These developments have fueled the need for greater processing power and storage capabilities, whilst ensuring the environment remains agile by design. Cloud meets this need. It enables enterprises to support the constant demand for innovation without the necessity of CapEx investment.

Cloud services free up organizations to focus on creating shareholder value by avoiding complex programs of work, such as building and operating secure data centers. That's not all. Cloud delivery models, such as platform-as-a-service (PaaS), offer an attractive business case by enabling pay-as-you-use models that reduce and align costs, whilst improving agility.

Securing your cloud evolution

As the journey to cloud gathers pace, there are still only a few true cloud-only organizations, other than those born in the cloud. More typically, enterprises must secure evolving hybrid environments that comprise growing and complex ecosystems of vendors. These environments are characterized by a mix of dedicated and cloud facilities, tools and procurement approaches, which are further complicated by an ever-changing threat landscape.

In this complex hybrid environment, a lack of centralized control raises concerns about end-to-end security. As a result, Capgemini believes that organizations need pragmatic cybersecurity approaches and services to support their ongoing cloud evolution in order to foster and establish digital trust in the business activities and transactions being undertaken.

On-premise / legacy
Private cloud
Public cloud
Multiple

Hybrid cloud landscape

Cloud security challenges

Few organizations have a complete grasp of their cloud security posture. The fragmentation caused by multiple cloud solutions, hybrid environments and ecosystem complexity leads to a greater attack surface for perpetrators to exploit. This heightens the risk of a security incident taking place.

In this landscape, business and technology leaders face a number of critical challenges:

• **Identity and access control**
Organizations struggle to provision and control access consistently across IaaS, PaaS and SaaS services due to the lack of centrally managed identities and access rights.

• **Monitoring and response**
Organizations need visibility and control of access to data and services, regardless of location, and they must respond rapidly to any emerging threat or vulnerability.

• **Data leakage**
How do you protect sensitive data leaking from cloud storage services and code repositories, where the cost of leakage can be huge in terms of both reputational damage, loss of intellectual property, and subsequent non-compliance penalties?

• **Governance**
Ownership of strategy and risk is not always defined, leading to a lack of control, with little agreement on how to secure ways of working.

• **Skills shortages**
Cloud skills are at a premium, while cloud security skills are even rarer.

What are chief information security officers asking?

• **Why should I trust the cloud?**
• **How can I test and monitor the security of our services and data in the cloud?**
• **How can I control who has access to my data once it leaves my data center?**
• **Can I use my existing tools?**
• **How can I access the cloud security skills needed?**
• **What happens if the cloud service is hacked?**
• **What can I get "off the shelf"?**

• **Shadow IT**
Staff bypass central IT to adopt cloud services, exposing organizations to unquantified risk. How do you manage EU GDPR compliance if you cannot identify where your personal data is stored?

Capgemini's Cloud Security Services offer you a pragmatic and cost-effective solution to these challenges. We will provide you with the complete picture of your cloud security through our portfolio of advisory, stand-alone and end-to-end Managed Security Services. We have the capability, scale and global reach required to provide you with everything you need in one place to effectively manage your security across a hybrid cloud IT estate.

Assess. Advise. Implement. Operate.

Cloud security extends beyond the technology. It embraces a broad scope of business, technology and cultural change. Our Cloud Security Services reflect this, giving you an as-a-service model and a catalog of services designed to help you at every stage of your cloud journey.

Whether you are just starting out on your migration to cloud, are re-evaluating the cloud architecture you've built, or have already reached a mature, agile DevSecOps position, Capgemini can help. We will inform, guide, support and reinforce your cloud security choices

Assess

A **Cloud Security Assessment** provides you with insight into your current or planned adoption of cloud computing.

- We measure the maturity of your overall approach to cloud security via interviews, workshop and documentation reviews.

- A technical assessment evaluates your existing cloud-based solutions (AWS, Azure or Google Cloud Platform) against the relevant Center for Internet Security (CIS) benchmark(s).
- Maturity assessments cover the broad spectrum of cloud security, from compliance and governance through to DevSecOps and container security.

Advise

Our **Cloud Security Advisory** services are based on more than a decade of helping clients adopt cloud security.

- We help you develop the foundations on which to operate in the cloud, with services such as AWS Landing Zones or Azure Scaffolds, roadmaps of capabilities for securing cloud workloads and DevSecOps transformations – from culture to tooling.
- We advise on the design and construction of cloud security architectures to safeguard data and service across the cloud spectrum, and on all elements of cloud security.
- We mitigate the impact of a massive gap in cloud security skills, enabling knowledge transfer and the upskilling of in-house teams to help you move ahead with your cloud adoption and improve existing implementations.

Implement

Our **Cloud Protection Services** offer a range of solutions for identity and access management, data protection, application security and infrastructure security.

- Our teams can work either 'with' you to enable knowledge sharing, or 'for' you to implement secure cloud services.
- We draw on our experience of building services across IaaS, PaaS and SaaS, and securing interactions across hybrid environments globally.
- Our partnerships with leading technology vendors enable us to bring best practices from their implementations, as well as from our own.

Operate

To ensure the security of your cloud-based operations, our **Cloud Security Monitoring** solution makes security monitoring a key foundation of your cloud architecture.

Flexibility by design enables us to cater for feeds from diverse providers and related systems, e.g. AWS Cloud Trail, CASBs and Azure Security Center, etc
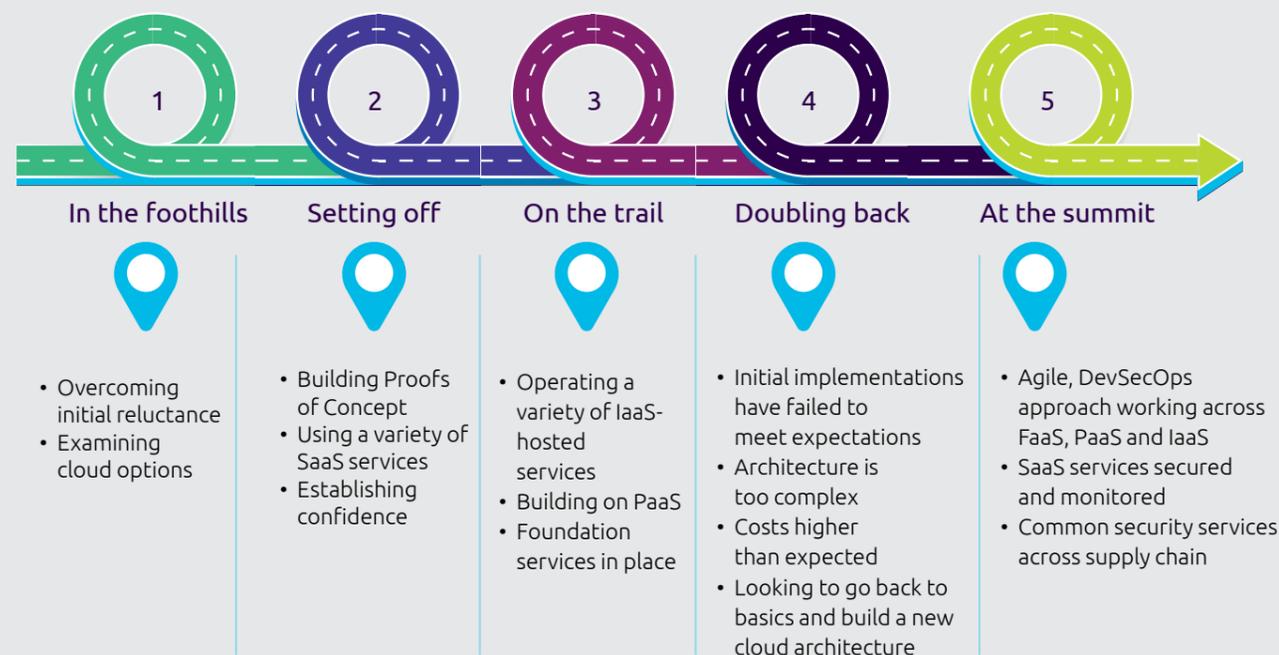
- You can adopt either fully centralized or distributed approaches to monitoring, while the service will take account of cloud-native security monitoring capabilities, such as AWS GuardDuty.
- An advanced sense analytics engine baselines normal behavior, detects anomalies, uncovers advanced threats and removes false positives.
- You'll have visibility of identified incidents and status updates via our Managed Security Services Portal.
- Increase your productivity and effectiveness. Machine learning detects anomalies, coupled with human analysis to investigate and suggest resolution activities

How we operate

- **Our Cloud Security Services are delivered from our global network of ISO27001-certified security operations centers (SOCs) and can be accessed either via our wider Capgemini Cloud Platform (CCP), or as standalone services.**
- **The CCP is our industry-leading cloud management platform and includes several service block options relating to security.**
- **Customers are supported by a single team of cloud security experts dedicated to managing their alerts in line with their risk profiles.**

Figure 2: Help at Every Stage of Your Cloud Journey

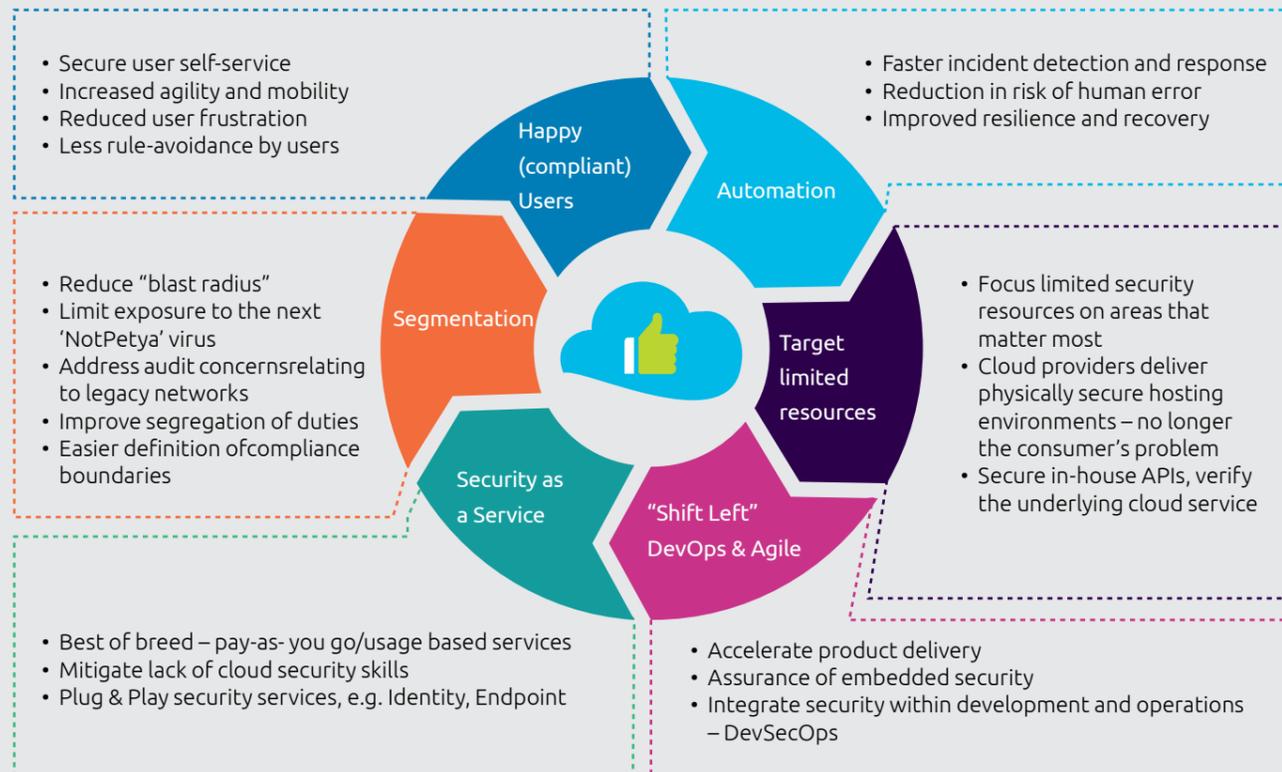| In the foothills	Setting off	On the trail	Doubling back	At the summit
• Overcoming initial reluctance • Examining cloud options	• Building Proofs of Concept • Using a variety of SaaS services • Establishing confidence	• Operating a variety of IaaS-hosted services • Building on PaaS • Foundation services in place	• Initial implementations have failed to meet expectations • Architecture is too complex • Costs higher than expected • Looking to go back to basics and build a new cloud architecture	• Agile, DevSecOps approach working across FaaS, PaaS and IaaS • SaaS services secured and monitored • Common security services across supply chain

Better cloud security outcomes

Trust Capgemini to secure your digital transformation with our end-to-end Cloud Security Services portfolio of

Managed Security Services. We will enable and embed security throughout your journey to cloud – at your own pace.

Our global network of security operations centers ensures you can rapidly ramp up your cloud security as it's needed, delivering secure global cloud scalability. This includes enabling a global cloud-based platform on which to secure the Internet of Things and worldwide ecosystems.

Figure 3: What Good Cloud Security Looks Like

• Secure user self-service
• Increased agility and mobility
• Reduced user frustration
• Less rule-avoidance by users

• Faster incident detection and response
• Reduction in risk of human error
• Improved resilience and recovery

• Reduce "blast radius"
• Limit exposure to the next 'NotPetya' virus
• Address audit concernsrelating to legacy networks
• Improve segregation of duties
• Easier definition ofcompliance boundaries

• Focus limited security resources on areas that matter most
• Cloud providers deliver physically secure hosting environments – no longer the consumer's problem
• Secure in-house APIs, verify the underlying cloud service

• Best of breed – pay-as- you go/usage based services
• Mitigate lack of cloud security skills
• Plug & Play security services, e.g. Identity, Endpoint

• Accelerate product delivery
• Assurance of embedded security
• Integrate security within development and operations – DevSecOps

Our agnosticism means you can seamlessly integrate security across diverse technologies and cloud platforms, including AWS, Azure and Google. Consumption-based pricing reduces the cost of cloud ownership and our as-a-service delivery model allows you to choose only what you need, when you need it.

With Cloud Security Services from Capgemini, you'll have all the support and services you need to launch new services and create new revenue streams in an agile and safe way – with embedded digital trust at its core.

☑ **Your security; your way**

☑ **Global scalability and security footprint**

☑ **Cost reduction**

☑ **Secure digital transformation**

☑ **Seamless technology integration**

☑ **Digital trust in new services**

☑ **Rapid delivery**

Why Capgemini for your cloud security services

At Capgemini, we provide a comprehensive portfolio of security services to address the challenges presented by cloud adoption. This includes a complete end-to-end global Managed Security Services offering for hybrid cloud estates, regardless of location – on-premise, public, private, and multi-cloud.

With our philosophy to 'think like an attacker', we protect our clients through a combination of threat intelligence, robust architectures and a highly industrialized and automated service delivery model. Our approach exploits unified and standardized cloud security processes to speed up delivery from our world-wide network of 24/7 global security operations centers.

Our clients benefit from highly scalable cloud security that can be customized to their needs, ensuring an efficient response to the evolving threat landscape. Our integrated approach means that we can secure and operate legacy/ on-premises or cloud (any cloud) environment.

Evolving, cost effective and compliant

Cost effective, pay-per-use pricing will enable you to better manage your cloud security spend. Further, our partnerships with leading industry players ensure we are able to secure services and best of breed tools at a lower cost of ownership. These long-standing partnerships with the major cloud providers and cloud-native security providers enable us integrate capabilities effectively to provide insight and support for all aspects of your cloud security.

Capgemini continually evolves the portfolio of security services by staying on top of cloud industry developments and workloads (e.g. container, serverless, etc.). We test and incorporate the latest security features in our solutions, and we keep our clients compliant with data protection and security regulations, such as PCI DSS, HIPAA and GDPR as required.

Get in touch

Find out how Capgemini brings together a mix of business, wider IT integration and cloud security skills and experience to address the ever-changing security challenges presented by cloud adoption as we support our clients' pursuit of agility and competitive advantage.

About Capgemini and Sogeti

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE., listed on the Paris Stock Exchange.

For more information please visit

www.sogeti.com

For further information please contact:

infra.global@capgemini.com