Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Capgemini & Sogeti Cybersecurity Services

Guiding enterprises and government through digital transformation while keeping them secure

Safeguarding today's digital organization with end-to-end advisory, protection and monitoring security services across critical areas of Identity & Access Management, Applications, End-points and Infrastructure

Secure digital transformation

What's needed is a digital transformation strategy with security at its core. In this way, the digital enterprise can evolve and grow securely and confidently.

Secure digital transformation

Incidents of cybercrime are escalating rapidly. With an increase in cyber attacks of more than 120% between 2013 and 2014[1], it is no wonder that businesses and governments alike are looking for answers.

The threat is more pertinent today than ever as organizations of all size and in every geography seek to transform digitally. In adopting social, mobility, analytics, cloud and the "Internet of Things" (SMACT) technologies, CIOs recognize that this also makes their organizations bigger targets. The threat comes in many guises, including from criminal organizations, hacktivists seeking notoriety, and, in certain cases, state-sponsored attacks.

And the cost of those threats? The average yearly cost of cybercrime for each large organization participating in a recent study was US$7.6m[2]. This was a 10.4% net increase over the previous year. Major cyber attacks could potentially result in losses totaling tens or even hundreds of millions. Then there is the damage to reputation and customer confidence, as well as to business continuity, caused by cybersecurity breaches.

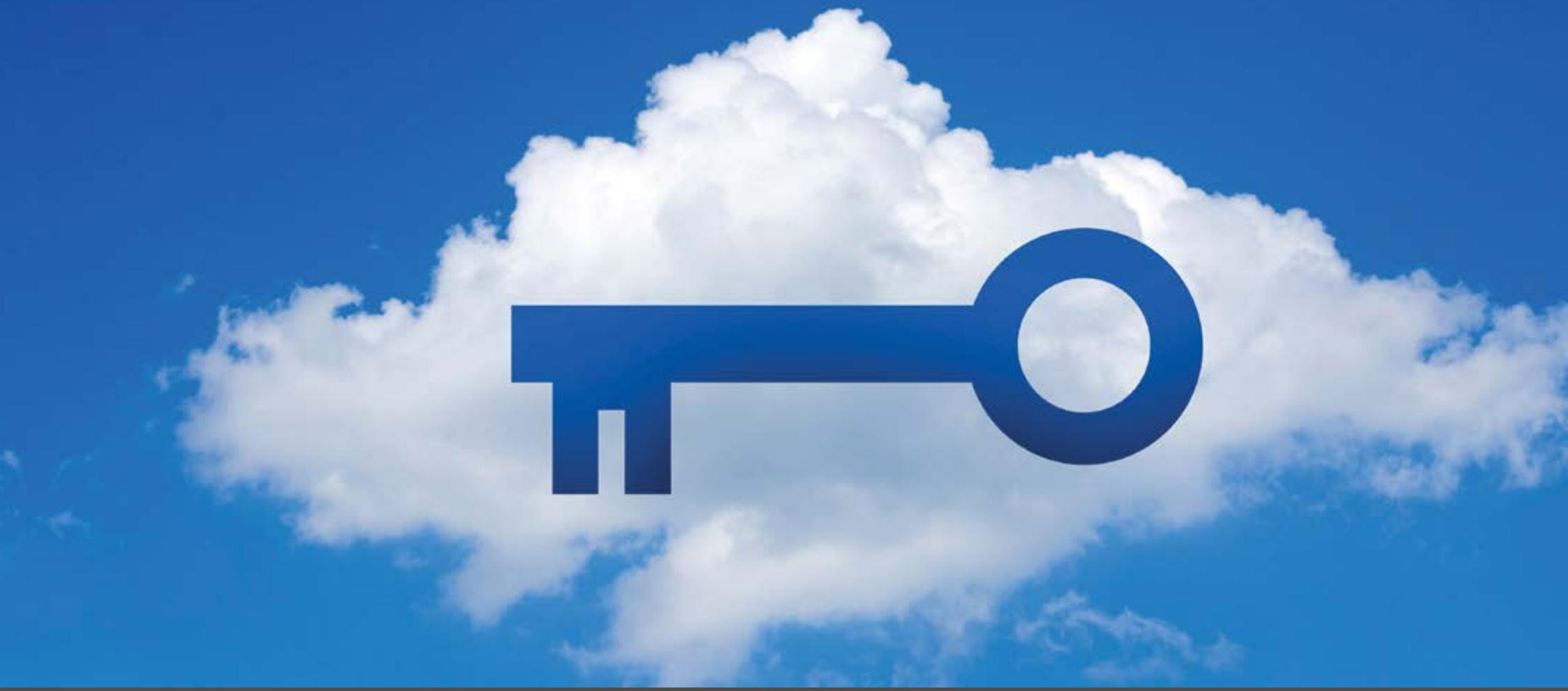
We introduced "Identity Management as a Service" with a single source of customer master data for over 5 million identities across 86 applications, with some 600,000 new registrations in just five months and 10m+ unique visits per month.

The advantages of digital transformation[3], however, are so significant that progress cannot be halted despite these threats. Instead, what's needed is a digital transformation strategy with security at its core. Unacceptable risks must be identified and quantified. The organization's risk appetite should be defined and reflected in the design and implementation of security controls.

In this way, the digital enterprise can evolve and grow securely and confidently.

1 Factiva, 'Major News and Business Publications' database; Thomson Financial, Investext database; databases of various security agencies
2 2014 Global Report on the Cost of Cyber Crime: Ponemon Institute, October 2014
3 The Digital Advantage: How digital leaders outperform their peers in every industry, Capgemini/MIT

SMACT



SMACT

The adoption of SMACT technologies introduces new risks to sensitive data and other assets.

We provide security analytics, Security Information and Event Management (SIEM) services and forensic analysis services to both public and private sector clients.

Government and enterprises are operating and engaging with customers in new ways. New channels, such as social and mobile, big data and analytics, cloud-based services, and digitization of enterprise business and industrial processes demand a new approach to protecting critical assets. That's because the adoption of SMACT technologies introduces new risks to sensitive data and other assets.

How are new channels and ways of working affecting security?

- **S**ocial media: users trust social media and this creates an efficient route for cyber attacks. Data leakage is a major concern, with sensitive (or inaccurate) information either deliberately or inadvertently shared and then rapidly disseminated. There is also the risk of damage to brand reputation and image if social channels aren't managed adequately.
- **M**obile: securing corporate data and enforcing policies and compliance on mobile devices may require different device management, encryption and user authentication mechanisms to other corporate platforms. These could include different, and very specific, management of mobile devices and applications, as well as user identities. This can be particularly complex where Bring/Choose Your Own Device policies enable a range of platforms and operating systems to be used. Can you guard your organization against data leakage and attacks via legitimate mobile devices accessing corporate information from public networks? And what about assuring mobile users' identities and securing mobile apps? These complex requirements all demand specific policies, tools and supervision.
- Big data and **A**nalytics: the ability to unlock many kinds of corporate intelligence to support better decision-making, including additional security intelligence, demands new large data stores. These are managed in innovative ways for fast data processing and the secure integration of data science tooling. Safeguarding data in these data lakes is not always straightforward. Personal data, as always, requires careful handling to comply with national and international regulations. This is especially the case when huge quantities of this data are stored together.

- Cloud: security becomes more complex on the journey evolving your organization from traditional IT infrastructure to a more agile and virtualized private cloud computing environment. Companies typically begin by virtualizing infrastructure to consolidate investments and reduce costs. Many then virtualize business-critical applications. They pursue a strategy of leveraging automation and higher degrees of management to extend virtualization beyond the computing platform to the rest of the infrastructure, including storage and networking. These efforts reduce operational costs and improve service quality, but it requires a careful security analysis. Yet it seems that many organizations haven't adapted their security architecture to the new virtualized software-defined data center model. For example, they haven't changed their traditional approach of using physical security infrastructures to secure virtual data centers and networks.
  Further concerns arise with public cloud solutions. Here the traditional enterprise perimeter changes and it is critical to check the level of security services that public cloud service providers offer. Your IAM needs to be enhanced to safeguard identity and manage access – particularly by privileged users – to cloud services. Legislation also becomes an issue unless you can dictate the region in which your data is stored. Are you comfortable with the national legislation governing your cloud provider?

Securing your customer experience

Giving customers a great experience, whilst ensuring high levels of confidence in terms of identity and access management, can be a crucial competitive differentiator. Integrating your customer experience across channels using SMACT technology and processes requires the development and introduction of new web code and mobile apps. Lifecycles designed to speed up time to service run a higher risk of code inadvertently containing vulnerabilities that can be exploited by hackers. These security vulnerabilities need to be weeded out via a proper Secure Software Development Lifecycle.

It is critical to check the level of security services that public cloud service providers offer.

- The Internet of Things: today there is also a movement towards interconnecting enterprise business management systems with the Internet of Things. ERP and HR applications are increasingly being interconnected with operational systems, such as industrial control systems (ICSs) including sensors and embedded systems. This adds a new layer of complexity that results in numerous potential vulnerabilities. It also vastly enlarges the attack perimeter attainable by hackers. Cyber attacks may now result in severe consequences in terms of the impact not just on data but also on industrial infrastructures, and possibly even on people's safety.
  In this context, the need to identify the vulnerabilities within business-critical industrial control systems and prevent cyber attacks is paramount. The multiple different end-point devices within an organization's ICS demand heightened governance, protection and supervision mechanisms.

Our security solutions are tailored to the leading business management applications (ERP, CRM, etc.), web and mobile applications. We continually develop our services to ensure that we can help clients secure the cloud-based SaaS they want to use.

Advise, Protect & Monitor

Advise, Protect & Monitor

Maintain the level of security you need to operate effectively as your business continues on its digital journey.

We recommended and connected a variety of mobile devices to a range of high-security services to support a central government department's need for secure mobile case workers handling departmental assets and sensitive personal data.

We know that transforming your business to make the most of new ways of working is a strategic imperative. Doing so securely is a powerful enabler for your strategic objectives. But where do you begin? And how do you maintain the level of security you need to operate effectively as your business continues on its digital journey?

At Capgemini-Sogeti our 3,000 cybersecurity professionals are 100% focused on protecting the business of customers like you. We have built an end-to-end cybersecurity services portfolio covering IT and industrial systems, and IoT products. We advise and control. We protect. We monitor.

- Advise and control: make sure your cybersecurity strategy is fit for purpose and in line with both your appetite for risk and your budget. From cybersecurity maturity and health assessments, to roadmaps, risk assessments and information asset inventories, including security controls such as pentests and audits, our consulting services are designed to help you make the right choices about what to prioritize and where to invest;
- Protect: our cybersecurity protection services design and build the defenses you need to safeguard your data, IT systems, industrial systems and enterprise, throughout your applications, end-points, data-centers and Identity & Access Management;
- Monitor: gain situational awareness of how your security controls are operating and the threats you face with our security supervision services. You will detect and react efficiently to cyber attacks.

Transform securely. Understand and manage the risks on your digital journey as you exploit the power of the internet while guarding against cyber attacks.

Why Capgemini & Sogeti?

Why Capgemini & Sogeti?

We view cybersecurity in the context of your business transformation goals, treating security as a business enabler rather than a problem. It's what sets us apart.

We guide you through your digital transformation while keeping you secure. How? By combining our understanding and proven experience of cybersecurity with deep expertise in IT infrastructure and applications integration. This includes unique capabilities for business-critical systems, such as industrial control systems (ICS), SCADA and embedded systems.

We believe one of the best ways to counter cyber attacks is to think like the attackers. This way of approaching your cybersecurity provides a valuable perspective that helps you harden your defenses and streamline your security investments.

Our cybersecurity transformation suite of methodologies and services gives you proven practices, world-class consulting and technology, and leading edge managed security services. These are built on the four pillars of cybersecurity defense: Users, Applications, End-points and Infrastructure security, as illustrated left.

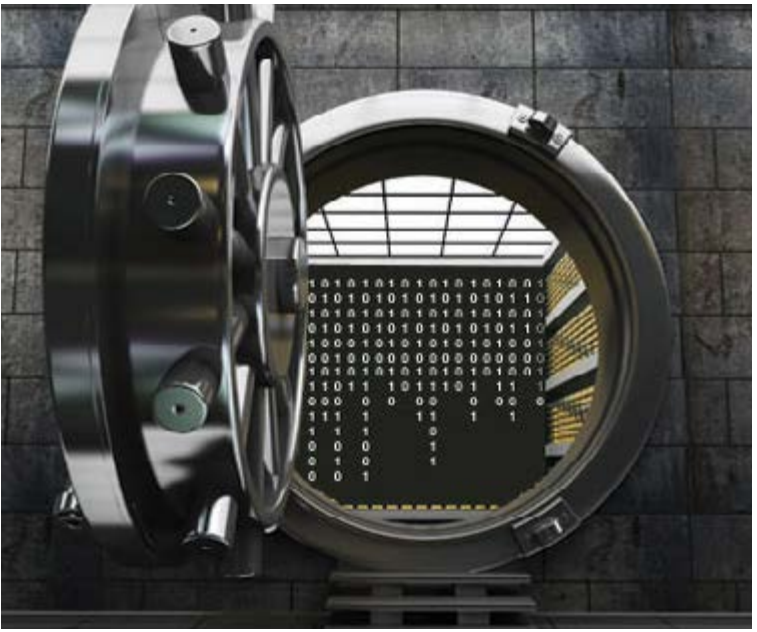
They are offered as time & materials (T&M) support, fixed-price projects, consulting services, managed or hosted security services. We're also investing to keep us in the forefront of the industry's rapid movement towards Security-as-a-Service. This approach saves our clients capex investment, while increasing flexibility and reliability.

We are supplier-agnostic. This sees us working with a large ecosystem of technology partners and specialist providers from which we form alliances as required to meet our clients' individual needs. We might, for example, work with a niche player who has a product that is of importance to a specific client.

With our 24/7 Global Security Operations Centers acting as the "eyes and ears" monitoring your enterprise, we will equip you to address even the most advanced threats.

In safe hands

In safe hands



Our clients trust us to help them secure their digital worlds against cyber attack:

- Government: we created a portal framework providing secure support for all web applications for a key central government department. This incorporated sophisticated security controls to assure significant volumes of sensitive citizen transactions, with internet access security services interfacing with external authentication regimes.
- Healthcare: we supported a hospital by implementing secure operating systems, user authentication mechanisms, communications channels, and hosted infrastructures, to ensure compliance with privacy regulation and protection of patient data.
- Transport and utilities: we provide risk analysis for complete systems, such as rail transportation systems and smart grids.
- Customer contact center: we designed and implemented security controls for a large organization's contact center that accesses multiple IT systems with sensitive data. We then undertook full assurance testing of the solution to confirm that the required security levels had been achieved.
- Financial services: we operate Security Operations Centers (SOCs) for a number of financial services organizations. These detect attempted attacks on critical assets and monitor overall network security.
- Industry: we helped an international industry leader build its cybersecurity and information protection strategy and transformation program. This spanned group infrastructure security, data protection in R&D activities, SAP-based IAM model, and industrial systems security.

About Capgemini and Sogeti

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security. Sogeti brings together more than 23,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 3,000 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT, industrial systems, and the Internet of Things (IoT) products & systems. We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, eight security operations centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

Learn more about us at
www.capgemini.com/cybersecurity or www.sogeti.com/cybersecurity

For more details contact:

Franck Greverie
Cybersecurity CEO
franck.greverie@capgemini.com

MCOS_GI_AP_20170216