



Application Security Testing

Build digital trust to enhance brand value and accelerate innovation



Applications are your business. Better secure them

Most of what matters to your business is delivered by applications. The customer experience. Product enhancements. Operational efficiency. Employee satisfaction. The faster you can deliver new applications, the faster you can differentiate and transform your business.

But applications are also a major source of risk and vulnerability. Cybercriminals target applications because they contain customer data and sensitive information. However, because of the pressure to release quickly, the security checks needed to manage applications and systems in depth are often incomplete. This leaves organizations open to attacks.

Better application security requires better testing across the development process. But it also requires a broader view of why testing is so critical.

Securing applications is not just about avoiding the unthinkable - data breaches, penalties for compliance violations, class-action lawsuits, etc. Capgemini recognizes that securing applications is also the key to accelerating innovation and exploiting new opportunities.

That is why Capgemini's Application Security Testing service is much more than another testing option. By testing all of your Web, mobile, desktop business applications - quickly, completely, expertly, and independently - we help you build digital trust.

At a glance

Application Security Testing is a platform-based, on demand, pay-per-use service. You simply upload your application code or URL via a portal, and our expert auditors scan them and send you comprehensive results quickly, so you can see and remediate vulnerabilities. It's the easy, accurate way to meet application security targets, guide security decisions, and cost-efficiently support the business.

It's time to move application security testing off-premises

The move to network-based business models and IT infrastructure is gaining momentum. Why continue to pay for on-premises systems, facilities and specialists, when you can simply move to network-based services?

The same concept applies to application security testing. Yes, you can do it all yourself. You can recruit, hire, and pay security testing specialists. You can purchase the tools and infrastructure to do the testing. You can establish the processes and compliance procedures to meet regulatory requirements. You can manage and maintain everything internally. But why?

With Capgemini's Application Security Testing service:

- **You simply purchase a subscription** and our experts systematically test all your applications - Web-based, mobile, or business applications, proprietary or open source - prior to release.
- **You get a balanced mix of manual and automated testing** depending on the level of service you need, using best-in-class tools and processes from Capgemini and world-class partners.
- **You receive actionable results via a single, intuitive dedicated portal.** The portal gives you the ability to scan requests, review results, and view dashboards that help you understand your application security posture and build the most appropriate remediation strategy.
- **You can customize your dashboards** in terms of business priorities or technical complexity.
- **You ensure objectivity** by separating the testing process from development, and you get a whole new level of scalability and repeatability.
- **You get broader and more accurate coverage** because we combine top-tier analyst tools, continuously updated threat intelligence, and expertise based on many years of testing experience to detect vulnerabilities - all delivered by security experts based in multiple geographies.
- **You have the flexibility to test wherever you undertake development activity**, ensuring responsiveness to your time pressures and enabling faster time to market.

- **You enhance GDPR compliance** and overall application risk management and highlight potential license conflicts or unwanted obligations.
- **You have access to the vast array of Capgemini cybersecurity services** to complement the expertise of your internal teams - including consulting services as well as a wealth of managed security services (MSS) and cybersecurity monitoring options.
- **You learn to create secure code** as your developers enhance their coding skills.

In an era when security specialists are increasingly hard to find and CapEx budgets are stretched thin, our solution makes it easy and fast to implement effective application testing - whether you have just a few applications or are looking to launch a comprehensive security program across your organization.

How it works: A closer look

Capgemini's Application Security Testing Service offering is accessible through the Managed Security Services (MSS) Portal and implemented using a secure public cloud service. This underlying architecture is ready to use on-demand. We can have you up and running quickly, and our rapid turnaround time integrates well with different delivery methods, including Waterfall and Agile.

The testing process itself is delivered by Capgemini security professionals, whose expertise is reinforced by highly automated artificial intelligence (AI) knowledge engines that increase scanning effectiveness. Based on six structured steps we analyze and run simultaneously hundreds of scans within short timelines. Reports produced by our teams highlight weaknesses and how to strengthen security gates.

Six steps that dramatically improve application security



Application security: A growing challenge.

- The average cost of a data breach globally is **\$3.86M**¹
- In 2017 more than **8 billion records** were exposed in **5,207 data breaches**.²
- Data breach incidents cost companies **\$148** on average per lost or stolen record³
- **15.4%** of reported incidents are related to web application attacks.⁴
- **82%** in a global study say they are highly likely/very likely/likely to experience the loss or theft of data caused by an unsecured IoT device or application over the next three years.⁵
- In 2017, **55%** of organizations had to manage public scrutiny of a breach⁶

¹Ponemon Institute, "The Cost of a Data Breach," 2018.

²Dark Reading, 2018.

³Ponemon Institute, "The Cost of a Data Breach," 2018.

⁴Verizon 2017 Data Breach Report.

⁵2018 Study - Global Megatrends in Cybersecurity, Ponemon Institute

⁶Cisco 2018 Security Capabilities Benchmark Study

Tests all code, including open source

Our highly scalable solution is suitable for every type of application: mobile, web-based, desktop, and business applications, including mission-critical applications. We test both proprietary and open source applications. Given the recent proliferation of open source code, this capability is increasingly critical. In fact, recent reports suggest that open source software now makes up more than 35% of the average commercial application.⁷

As open source software is redistributed outside its license terms, many companies are unaware that they are compromising intellectual property, or of potential critical security vulnerabilities embedded in the code. Our automated service helps to uncover these risks, remediate as appropriate and enforce compliance with open source licenses throughout the application lifecycle.

Thorough, accurate scanning with exceptional flexibility

The Application Security Testing service is powered by our industrialized approach, and the expertise of our security experts.

The testing service is available from anywhere and the flexibility of the platform allows easy scale-up and scale-down of scanning activities depending on your growth rate, specific requirements and quality standards.

Your portal: easy-to-interpret, actionable insights

The portal provides an integrated, secured and personalized view of your applications and how they are exposed to security threats. For development teams, it's easy to upload code, see results, and use a variety of dashboards to find and remediate vulnerabilities. A full range of portal features are ready to use, including:

- Role-based access controls that determine who can do what
 - Secure Sockets Layer (SSL) user authentication based on certificates to identify the user to the server
 - Multi-factor authentication
- A standardized approach to managing requests for application testing, such as static scan request, remediation scans, dynamic testing, and open source software analysis
- Standardized false-positive removal
- Standardized dashboards to highlight potential risks to the business
- Customizable reports to highlight security posture, trends, remediation status and priorities



A broad range of business benefits

Capgemini's Application Security Testing service delivers unique business value on multiple fronts, including:

Continuous protection keeps your focus on business value

Today's application development cycles are short, with frequent updates. Application Security Testing enables you to audit applications regularly across the board, so you can focus on the business value of the applications rather than security concerns.

Reduces the attack surface for fast, accurate remediation

Our audits enable application breaches to be precisely located, weaknesses to be effectively targeted, and potential attacks to be thwarted. By monitoring your applications continuously, identifying threats and protecting against malicious acts, the Application Security Testing service limits the opportunities for hackers to attack.

Avoids wasting time so you can release software faster

The earlier security tests are carried out, the more effectively you can correct vulnerabilities. By automating testing on all your applications, and by testing when the project is about to go live, we strengthen the application's security while expediting its release.

Accelerates GDPR compliance

The General Data Protection Regulation (GDPR) strengthens security controls, and the Application Security Testing service enables your business to place security at the heart of your application layers.

⁷Source: Pittenger, Mike. "The state of open source in commercial apps: You're using more than you think." TechBeacon

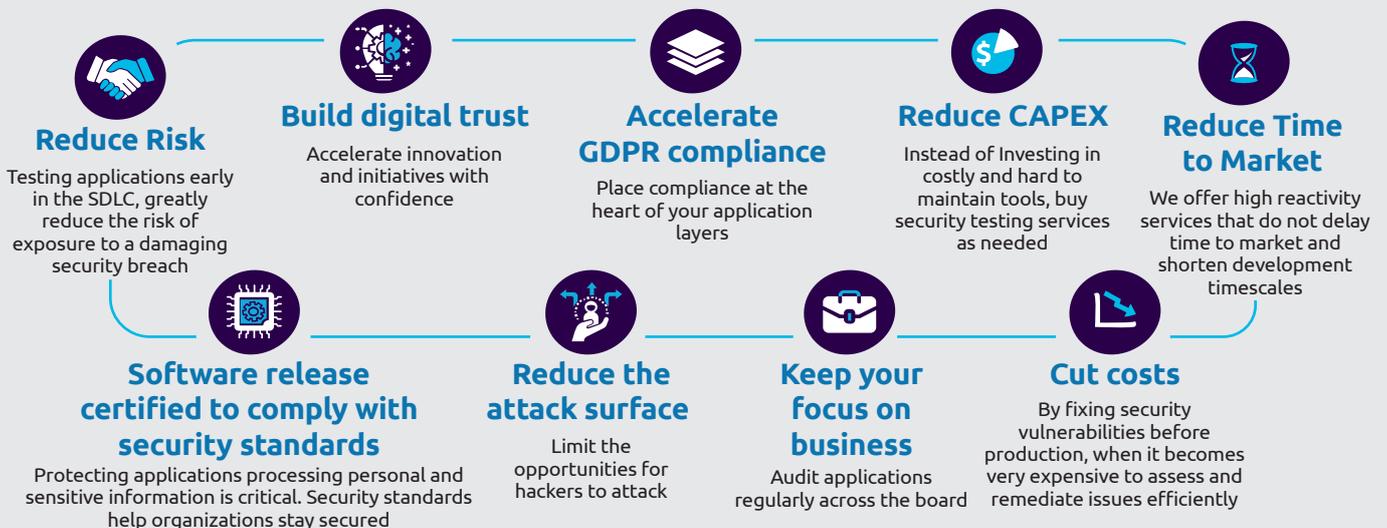
Builds digital trust

All companies fear the consequences of the press and social media channels revealing that they have been victim of a

cyberattack. On the other hand, protecting your applications across the development lifecycle create digital trust, which allows you to accelerate innovation and business initiatives with confidence.

 On demand	 Highly scalable	 Extremely flexible
<p>Get up and running quickly and cost-efficiently</p> <ul style="list-style-type: none"> • Launch your application security initiative in < 1 day • < 1-week turnaround on application security results • No hardware or software investments • No in-house security experts to hire, train and retain 	<p>Scale to test all applications in your organization</p> <ul style="list-style-type: none"> • Web, mobile, business applications tested • Open source software analysis • Dynamic and static testing with standardized false-positive removal 	<p>Test any application from anywhere</p> <ul style="list-style-type: none"> • Secure in-house, open source and third-party code • Test applications in the cloud or on premises, on demand

Business benefits of strong application security testing



Real results from real clients

Major French international bank

- Mobile App Security Testing solution combining security automated testing and manual testing improved testing coverage scope by **68%**
- **100%** of OWASP Top 10 critical vulnerabilities uncovered by deep assessment of the 3 key layers which make up all Mobile Apps
- Strongly contributed to boost bank's ambition to be a leader able to provide **innovative digital solutions** to improve knowledge of customer investments

Key European Energy Provider

- Cut application security testing time from **7 days to under 48 hours**
- More than halved the cost of application security testing: **57%** reduction
- Increasing scope of testing without dropping the "go live" pace vital to the customer's **business reputation**

Central Tax Management Authority

- Application Security Testing was the right solution to uncover various levels of risks in Apps holding personally identifiable data.

Remediation tips have reduced the average threat fixing duration by **75%**

- Detailed guidelines regarding Application Security Testing facilitated Client's understanding of Security Risks and how to best optimize testing budget to be fully secure before going live
- Fast track implementation and deployment of testing methodologies **improved software quality and customer's confidence**

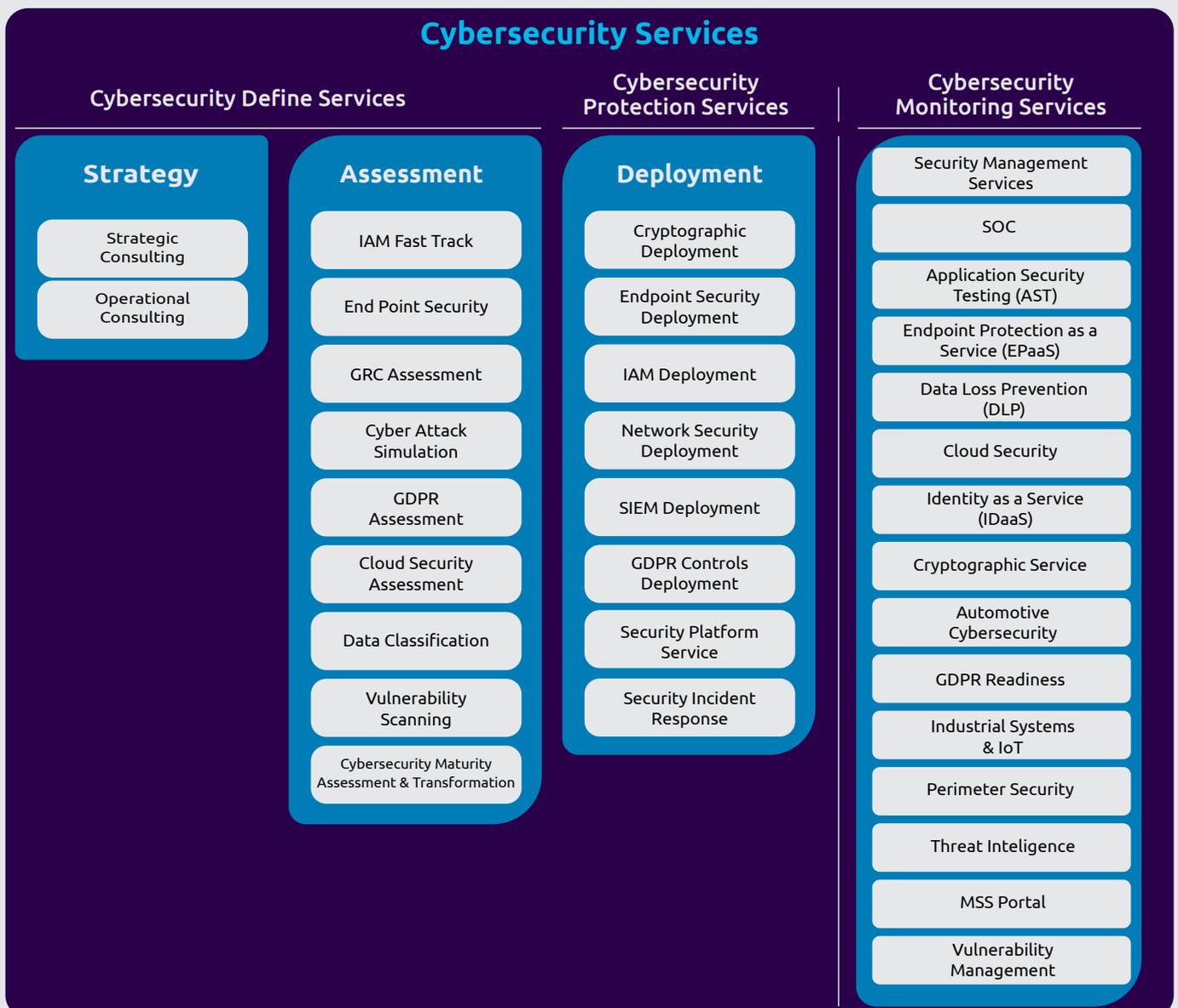
An integral part of our comprehensive cybersecurity capabilities

The Application Security Testing service is a core element of our overarching, end-to-end offerings in cybersecurity. We can deliver Advisory Services addressing the full range of cybersecurity strategy, assessment, and deployment needs, as well as Managed Security Services covering

your applications, networks, endpoints, data, end users, infrastructure, clouds, perimeters, and more, all with a range of service levels.

Capgemini is the one service provider who can bring everything together for your enterprise: end-to-end cybersecurity solutions from multiple vendors, coupled with a comprehensive portfolio of consulting and managed service offerings - globally or locally, in virtually every industry and market segment.

We can serve as your single trusted advisor for integrating and orchestrating your cybersecurity solutions globally, and we have many years of experience covering security requirements in virtually every industry and market segment, at a scale that will match your needs today and tomorrow.



For details about any of the services above visit www.capgemini.com/cybersecurity

Compelling advantages

Our ability to deliver comprehensive cybersecurity capabilities results in multiple advantages that truly set us apart. These include:

End-to-end and ecosystem expertise

In an era of disjointed security solutions and increasingly diverse attack vectors, Capgemini is the one service provider who can bring everything together: Application Security Testing, end-to-end cybersecurity solutions from multiple vendors, and a comprehensive portfolio of consulting and managed service offerings - globally or locally, in virtually every industry and market segment.

A business-focused, collaborative approach

We start by understanding your specific requirements from a business perspective. Through discussions with your key stakeholders, we tailor a strategy and an approach that aligns with your business objectives, then we recommend services tailored to your specific needs.

IoT and industrial security skills

Armed with sector-specific threat intelligence, Capgemini Enterprise Operational IoT experts can assess the security posture of your industrial systems and IoT devices, including maturity analysis of industrial information systems, risk analysis of critical systems, and creation of a roadmap to improve the organization's defenses, while delivering quick wins in reducing risk.

Cloud security specialization

Capgemini has broad and deep expertise in cloud security, enabling you to adopt a range of dedicated and hybrid cloud models safely and cost-efficiently. Capgemini can help you assess your current cloud security maturity level; map your current posture against security services offered in clouds; implement security practices and tools to protect infrastructure, applications, platforms and data in the cloud; provide recommendations to address security compliance gaps; manage security incidents; and more.

Global scale

We are everywhere your development teams, networks, devices and users are, worldwide. With a global web of SOCs and research labs, over 4000 security professionals, and presence in over 200 countries, we can deliver the advice, skills and managed services you need, your way, anywhere in the world.

Industry recognition

Capgemini is recognized as a leading cybersecurity and managed security services provider by leading analyst firms in their respective reports.

Top talent

Our 4000+ skilled cybersecurity experts hold industry standard certifications such as CISSP, CISM, CISA, CCSP, including ITIL, CEH, CCIE and other technology certifications.

Satisfied clients

We carefully measure and monitor client satisfaction, and the vast majority of our clients are "highly satisfied" with the services they receive.

Simplicity

The complexity of cybersecurity can be overwhelming. We extract complexity at every turn, so you can focus on your business goals and strategic initiatives. We're here to make your life simpler while we make your enterprise safer.

Contact Capgemini. Let us show you a smarter way to test.

Take the next step toward proactive protection of your applications and your enterprise. Contact Capgemini today and learn more about our uniquely effective Application Security Testing service.



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

This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.
Copyright © 2019 Capgemini. All rights reserved.

For further information please contact:

infra.global@capgemini.com