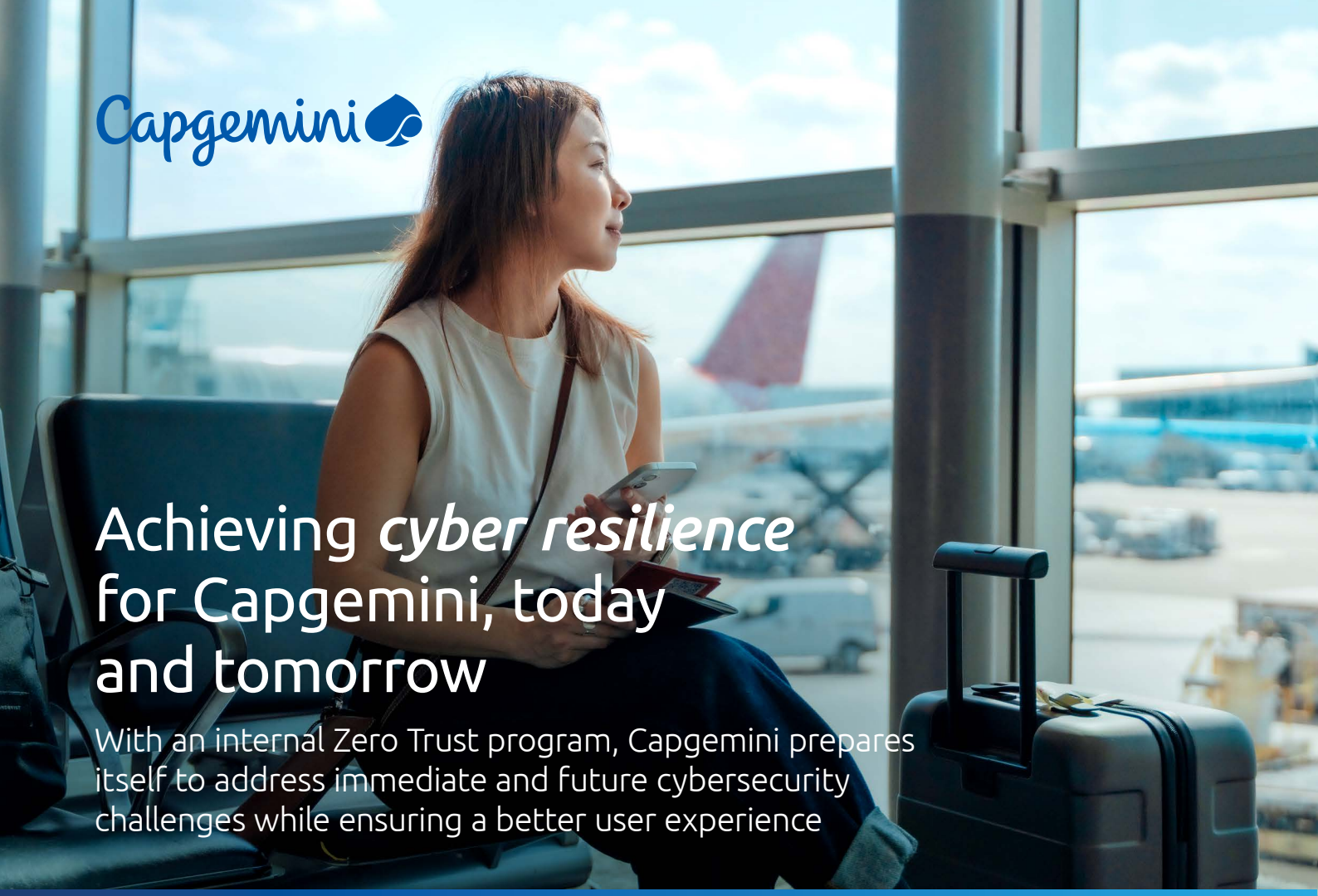

Achieving *cyber resilience* for Capgemini, today and tomorrow

With an internal Zero Trust program, Capgemini prepares itself to address immediate and future cybersecurity challenges while ensuring a better user experience

Protection designed for today's working world

Capgemini is a global leader and its 350,000 people are increasingly mobile, meaning they require secure access to their data anywhere, any time, and on their Capgemini or client supplied devices. However, with cyber threats continually increasing in severity and frequency, resulting in expanding compliance requirements, maintaining this flexible employee IT at scale is complex.

Enter Zero Trust – and its three core principles:

- **Never trust, always verify:** every connection attempt should be authenticated and authorized.
- **Assume breach:** always operate under the assumption that a breach has already occurred, and design systems to limit its impact and detect anomalies early.
- **Least privilege:** Users and applications should only be granted the minimum amount of access to perform their jobs effectively. No more, no less.

Client: Capgemini

Industry: Information Technology

Region: Global

Client challenge: Increasing cybersecurity challenges, the sheer scale of its global operation and a desire to modernize infrastructure convinced Capgemini to redefine its cyber strategy.

Solution: Zero Trust provides the right balance of protection and productivity, empowering Capgemini's employees to continue working seamlessly while safeguarding their work and the information exchanged with clients, partners, and colleagues.

Benefits:

- Enhanced cyber resilience across all layers of the organization
- Enabled secure and seamless work
- Aligned with global cybersecurity standards while preparing for the future

From Capgemini's perspective, it practices what it preaches: the concept of providing borderless security across the entire enterprise is at the heart of its Zero Trust strategy. It not only embodies this across the Group but also enables clients to benefit from the same approach.

So, how did it come to be?

The Zero Trust program

In response to the Group's expanding cybersecurity needs, Capgemini's IT and cybersecurity teams created and implemented the Zero Trust program to deliver a number of critical enhancements.

This began with an upgrade to the existing IT infrastructure, to support greater robustness and agility. In addition, security was increased to protect even more effectively against evolving threats. As a part of this process, Capgemini also simplified its network architecture.

Throughout this project, the team maintained a constant focus on ensuring a better user experience. This required rigorously managing third-party access and supporting all devices used by company employees worldwide.

Zero Trust wasn't just about securing IT systems – instead, it transformed how Capgemini's entire organization operates, connects, and protects information. This was made possible through:

- **Consistent identity data management** through a single identity stream for seamless, accurate identity verification.
- **Passwordless access control** for an enhanced user experience, mitigating the threat of credential theft and making secure access effortless and fast.
- **Full visibility and security** achieved by monitoring every application, workload and device, giving Capgemini a comprehensive view of its IT ecosystem.
- **Enhanced, standardized client connectivity.**
- **Micro-segmentation** to isolate and protect system-to-system communications, minimizing potential vulnerabilities.

Finally, the IT and cybersecurity teams introduced context-based access policies that analyzed identity and behavior to assess user risk in real time. This approach also included steps to ensure that every device meets Capgemini's high security standards. Finally, the new access policies took into account workload sensitivity so that adaptations could be made based on data sensitivity.

Partnership and the future

The IT and cybersecurity teams worked closely with Capgemini's partners to deploy best-in-class solutions, providing secure application and internet access while managing identity and authentication with advanced risk assessment. This also ensures cutting-edge endpoint protection and streamlines device management for Capgemini's globally distributed teams. Additionally, Capgemini now fully supports micro-segmentation.

This program stands as one of the most ambitious and complex internal cybersecurity and operational IT transformations in Capgemini's history.

"By successfully implementing Zero Trust at this scale within our own organization, we've built unmatched expertise—enabling us to lead and accelerate similar transformations for our clients with even greater confidence and hands-on experience. We are actively partnering with numerous clients to fast-track their own Zero Trust journeys." Sudhir Reddy, Capgemini Group CIO confirms.

This project strengthened cyber resilience across all layers of the organization while enabling secure and seamless working for a mobile global workforce. Moreover, it helped Capgemini adopt a future-ready cybersecurity posture that aligned with global standards.

With Zero Trust now embedded into its core infrastructure and culture, Capgemini is better equipped to navigate the cybersecurity challenges of today and those on the horizon. The learnings, frameworks, and architecture developed through this initiative will continue to inform and elevate future engagements and deployments.

> A firewall with a hole is no longer a defence—it's an invitation. At Capgemini, our adoption of Zero Trust Architecture has transformed how we secure our digital landscape. By eliminating implicit trust and verifying every access, we've not only strengthened our cybersecurity posture but also enhanced user experience, operational agility, and scalability. This is how we lead in a world where resilience is non-negotiable.

Sudhir Reddy,
Capgemini Group CIO

> Trust is no longer by default — it's a decision. Zero Trust architecture makes that decision intelligent, dynamic, and secure in a world without borders where digital confidence is a key business enabler. At Capgemini, we ensure secure access across hybrid environments without compromising agility, while minimizing attack surfaces and lateral movement risks. In today's threat landscape, under relentless regulatory pressure, Zero Trust is not just our strategy – it's the backbone of our cyber resilience.

Marjorie Bordes
Group CISO, Capgemini

Capgemini

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Get the future you want | www.capgemini.com

For more details contact:

cybersecurity.in@capgemini.com