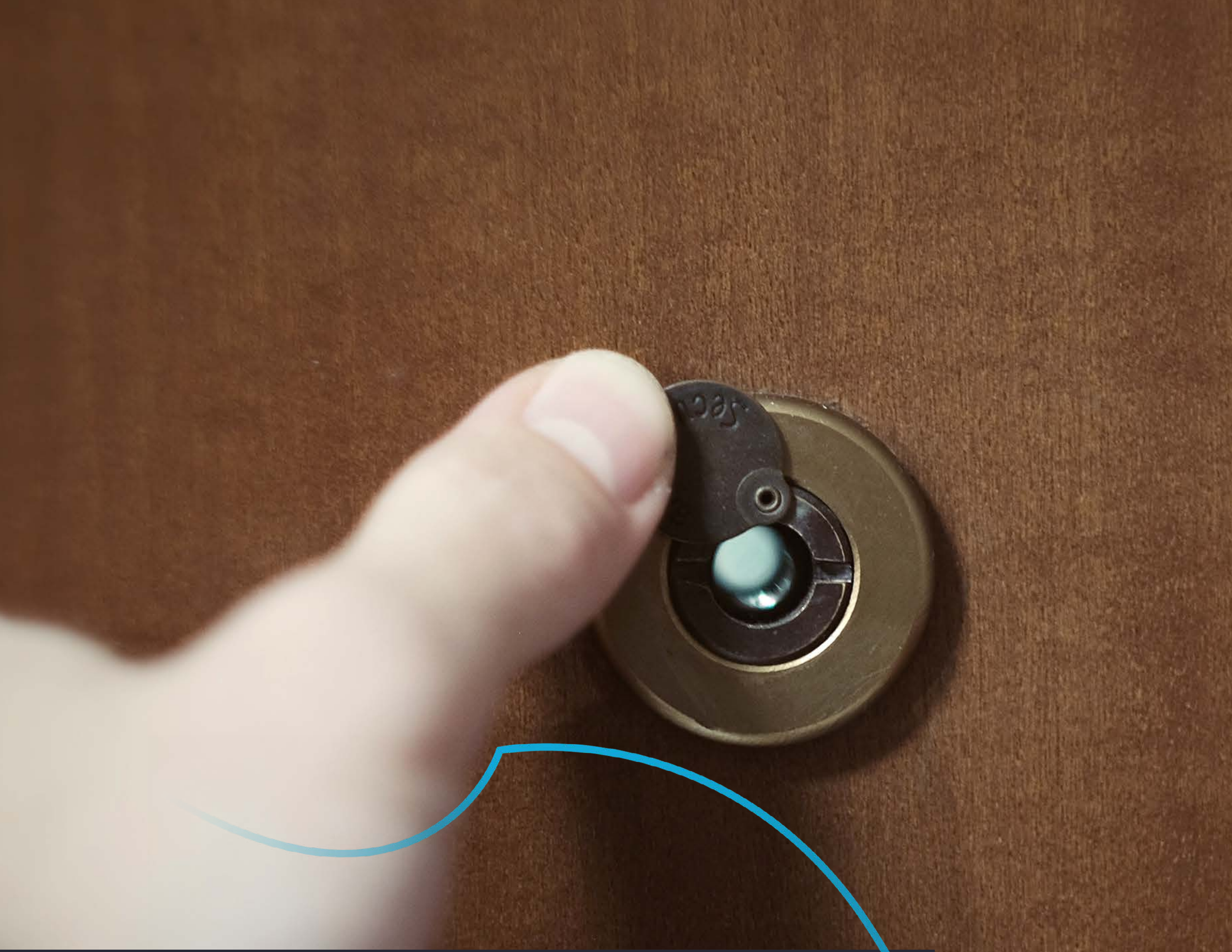


Accelerate your journey to zero trust with zero trust orchestration

How to orchestrate secure, reduced friction user journeys within a Zero Trust Framework

Capgemini

Ping Identity

INTRODUCTION

Cloud computing and interconnectivity have changed IT security forever. In the old days, when all your servers lived in your own data centre and everyone connected directly within your corporate network, or via VPN, you could rely on your corporate firewall as a fixed perimeter security control. Today, your employees, partners and customers—as well as connected devices from the Internet of Things—could be logging in from any location, via any network, to services hosted anywhere.

Keeping your business safe in these complex hybrid, multi-cloud, hyper-connected and highly-collaborative landscapes is far more challenging. Organisations are increasingly recognising that the only way to stay secure in this world while providing a frictionless user experience is through a Zero Trust security approach, which replaces reliance on legacy network security controls with an approach where every access request is assessed on a rich contextual basis. This Zero Trust Architecture becomes the new perimeter.

Zero Trust is no longer just a buzzword—it's now mandated or recommended by governments and industry bodies around the world. However, we see that a successful adoption of Zero Trust principles such as those defined in NIST-SP 800-207 requires the orchestration of multiple elements that combine to provide policy-based controls that work across user journeys and channels. These user journeys often involve both legacy and modern systems and services that need to work together seamlessly—and managing these interactions introduces new problems.

This paper explores best practices for orchestrating these interoperating elements as part of a comprehensive Zero Trust framework, addressing the following key questions:

- What are the market challenges that are driving organisations to implement Zero Trust?
- What is a Zero Trust Orchestration layer, and why is it required?
- Where does an Orchestration layer deliver the greatest benefits?
- How are Capgemini and Ping Identity helping organisations adopt Zero Trust Orchestration?

MARKET CHALLENGES DRIVING ZERO TRUST

We now live in a world where employees expect to be able to work from anywhere and log into corporate and partner systems via any device on any available network connection. The challenge for organisations is to open up more streamlined, user-friendly access for employees in this modern environment, while maintaining appropriate levels of security to protect against increasingly sophisticated cyber threats.

Meanwhile, customers (and regulators) are increasingly concerned about data privacy and the risk of identity theft, fraud and scams. Customer-facing systems which have traditionally been designed to maximise user convenience in a siloed way must now find ways to bolster security and protect customer data, while simultaneously improving the user experience.

	Security risks	User experience risks
Customer-facing applications **For example:** • Online retail websites • Online and mobile banking apps • Customer portals	• Customers are exposed to account takeovers and identity theft • Fraud and scams lead to financial losses and reputational damage • Data breaches result in data privacy violations and regulatory penalties	• Complex registration process discourage new customers from signing up • Difficulty logging in increases risk of shopping cart abandonment • Personal data used in authentication raises privacy concerns
Employee-facing applications **For example:** • HR portals • File systems • Line-of-business apps	• Ransomware attacks pose an existential threat to business operations • Risk of intrusion and data theft by hackers and fraudsters • Potential abuse of resources by employees • Overly permissioned users disrupt systems, either by accident or by intent.	• Mutliple logins and lack of SSO result in employees locking themselves out of their applications, impacting productivity • Frequently re-entering user IDs, passwords and OTPs creates friction

Table 1: Drivers for Zero Trust

Balancing the competing demands of security and user experience for customers and employees has become increasingly challenging due to the levels of connectivity and flexibility required by modern user journeys. A routine user journey—such as a customer ordering a product or an employee creating a purchase requisition—now often involves interactions between dozens of services, from legacy systems hosted in the company's data centre to microservices and third-party SaaS applications running across multiple clouds. A key driver for a Zero Trust approach is that it can provide a solution to this demand for both security and user experience in today's open environments, by taking into account the broader risk and context of the specific access at any point in time.

WHY DO WE NEED ZERO TRUST ORCHESTRATION?

As described above, a Zero Trust approach is becoming the only viable solution for effectively providing access in these extended IT ecosystems. However, implementing and managing a comprehensive Zero Trust framework can be complex.

The fundamental principle of the Zero Trust model is based on the assumption of a breach and entails a meticulous examination of each request as if it were originating from an entirely untrusted source, such as the unrestricted internet. Regardless of the origin or the resource being accessed, the Zero Trust approach mandates a "never trust, always verify" methodology.

Each request must provide sufficient evidence of its legitimacy as originating from an authorized user or application. Every access request undergoes comprehensive authentication, authorization, and encryption before and during the session. Additionally, the level of verification deemed "sufficient" may vary dynamically based on context, necessitating additional security measures and/or access privileges to be modified.

Establishing the context for Zero Trust verification requires the organisation to gather information from a number of different sources which are potentially interpreted by mutiple policy engines (or "signals"). As Zero Trust implementations become more sophisticated and the number and type of signals increase, a Zero Trust Orchestration layer becomes vital to integrate the information from all these signals, make dynamic decisions on whether the access request aligns with security policies, and trigger an appropriate response from the security tooling that enforces access control across the technology stack. It is this ability to take signals, make smart access control decisions based on those signals and then orchestrate the enforcement of policy throughout the technology stack that forms the core of the technology implementation element of a Zero Trust programme.

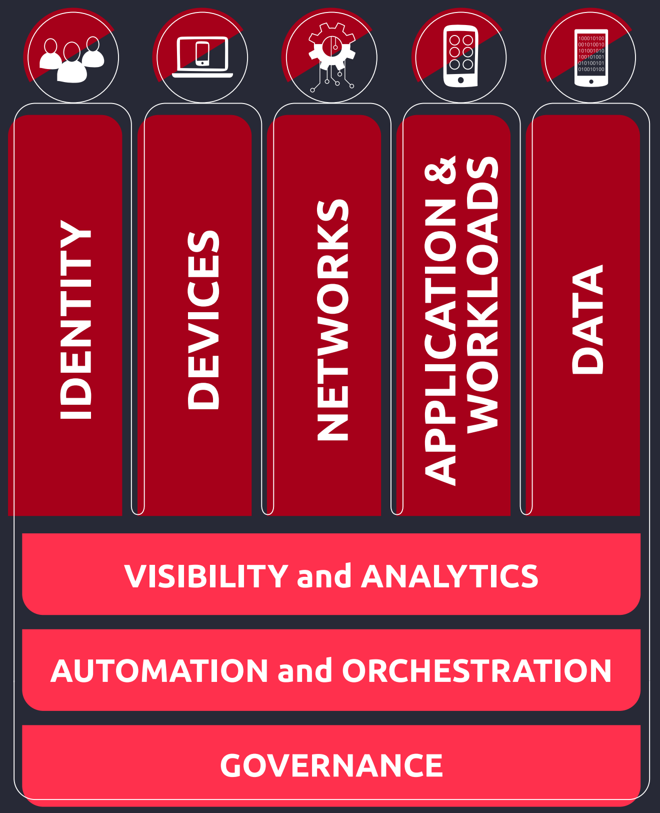


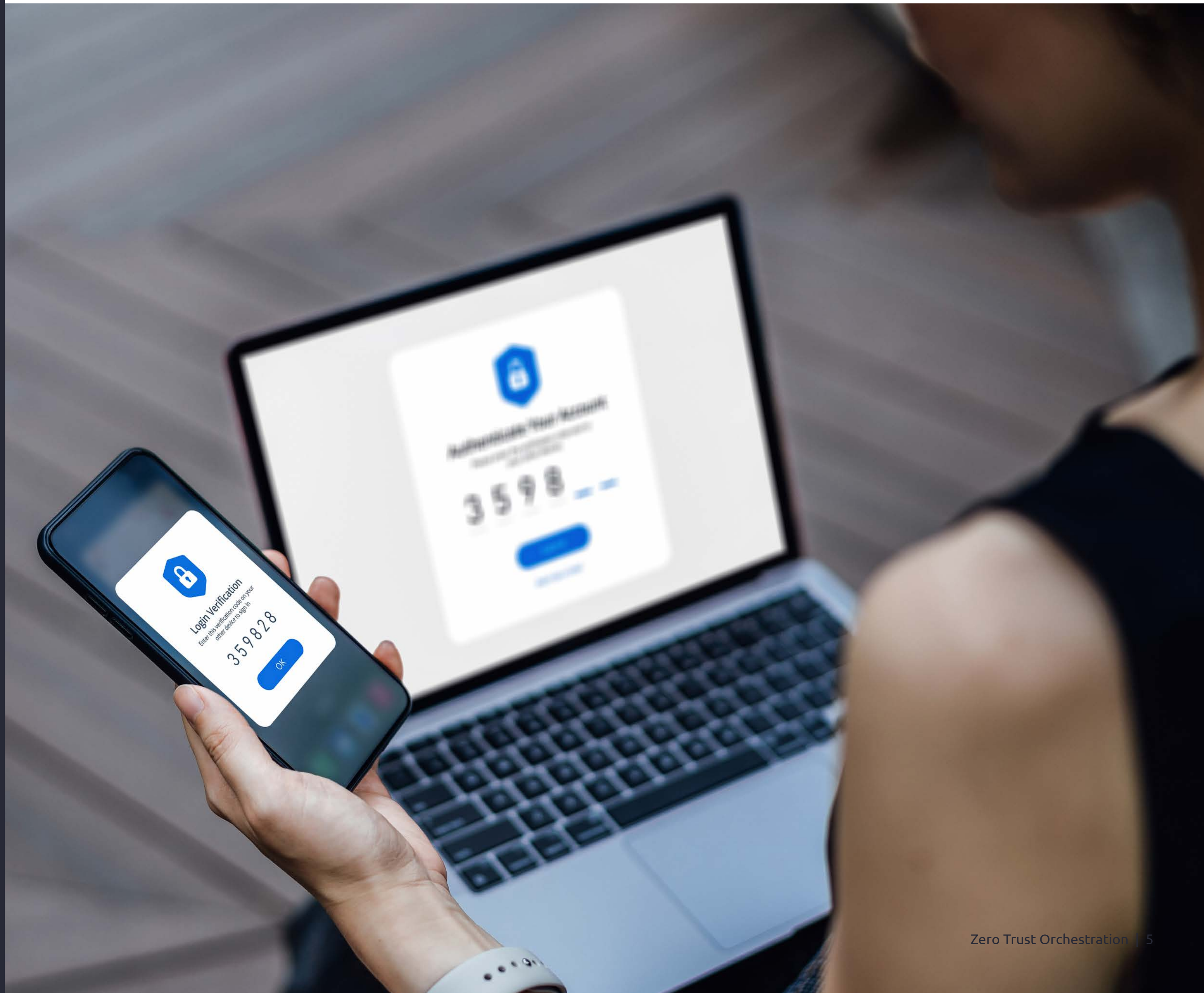
Figure 2: Zero Trust Maturity Model Pillars, CISA Zero Trust Maturity Model, Version 2.0, April 2023. CISA define Automation and Orchestration as a foundational cross-cutting capability for Zero Trust Architectures

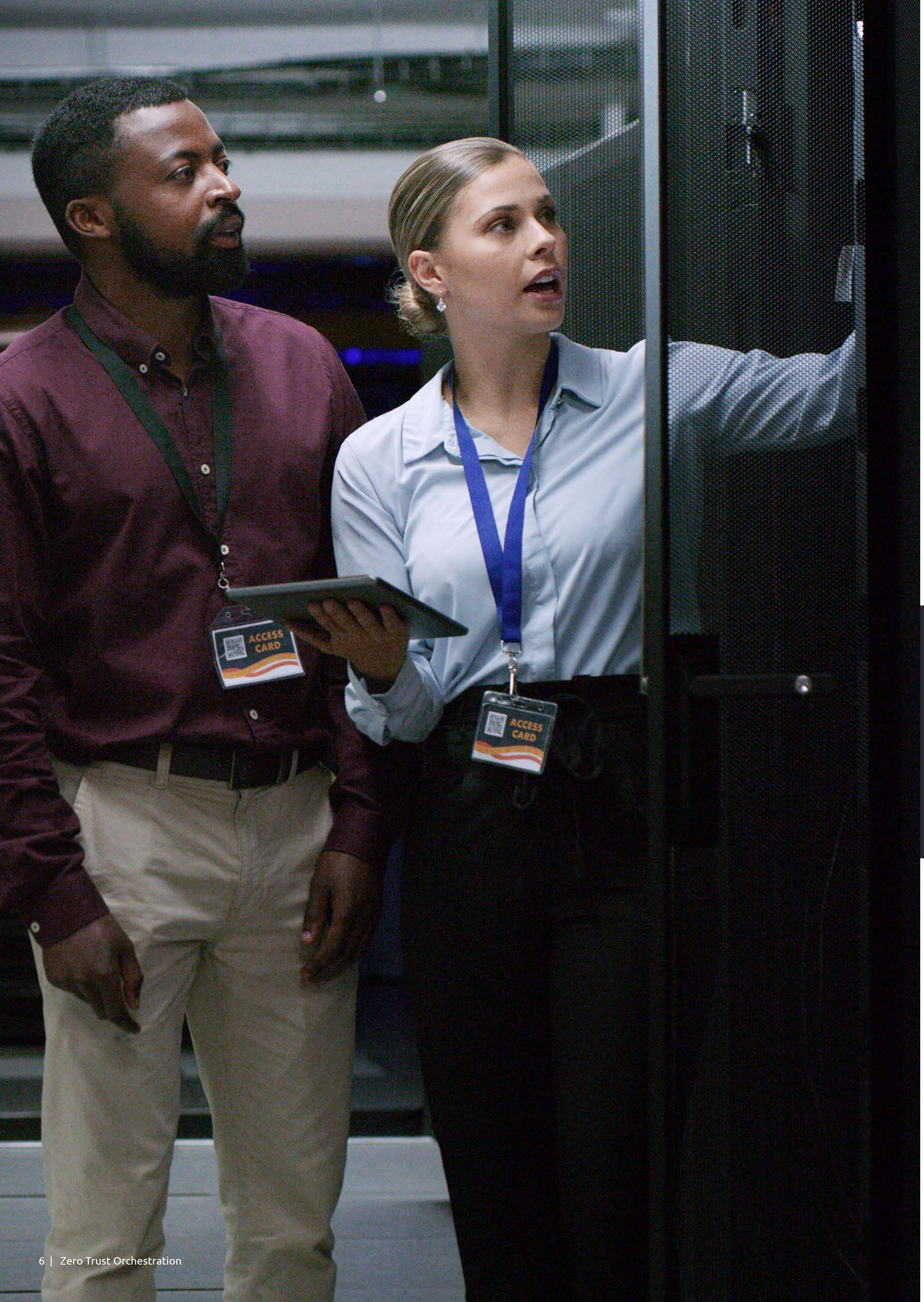
THE ROLE OF ZERO TRUST ORCHESTRATION

A Zero Trust Orchestration service within a Zero Trust Architecture provides a policy and integration layer capable of connecting identity elements from many systems, providing a single point of control.

An Orchestration service can capture signals from your underlying applications and infrastructure and pass them to a central policy engine that drives smart, real-time decision-making during complex user journeys. And best-practice Orchestration solutions, such as PingOne DaVinci, empower you to map out these user journeys as seamless flows, while defining the authentication and authorisation requirements for each resource based on appropriate risk metrics.

A Zero Trust Orchestration service makes it possible to implement Zero Trust principles quickly, effectively, and cost-efficiently—so you can design, deploy and evolve your user journeys seamlessly in response to emerging business needs.





ZERO TRUST ORCHESTRATION USE CASES

We now see Zero Trust Orchestration as a fundamental component within any Zero Trust Architecture. Some use cases where Zero Trust Orchestration is particularly beneficial include:

Providing adaptive trust in complex heterogeneous environments

Zero Trust Orchestration can help you gather risk signals from right across your network, including various risk and policy engines, and wider security tooling to feed them into a central Orchestration policy engine that can deny, approve, log or request additional authentication for access requests at all relevant stages in your user journeys. Moreover, a Zero Trust Orchestration service can then enable automated risk mitigations beyond Access Management such as firewall and device patching, or removal of access rights through IGA integration, proactively preventing incidents and saving time for your security team. Industry-leading solutions such as PingOne DaVinci allow organisations to streamline and simplify this process by including integration connectors to security tools like CrowdStrike, OPSWAT, Splunk, InTune, JAMF, PingOne Protect and hundreds more, all out of the box.

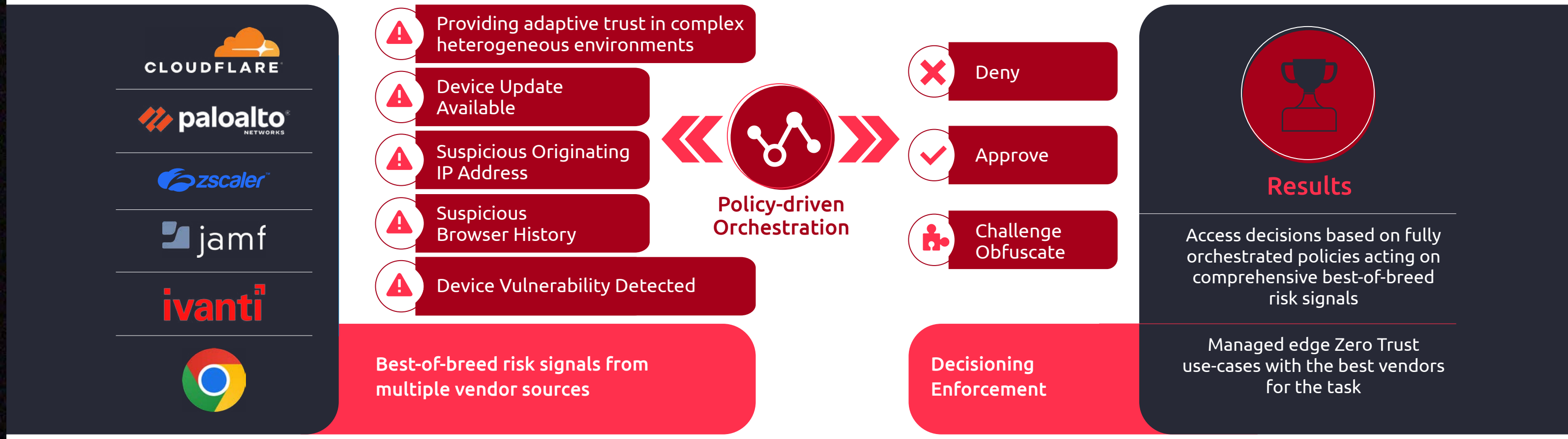

CLOUDFLARE
paloalto
zscaler
jamf
ivanti
Providing adaptive trust in complex heterogeneous environments
Device Update Available
Suspicious Originating IP Address
Suspicious Browser History
Device Vulnerability Detected
Best-of-breed risk signals from multiple vendor sources
Policy-driven Orchestration
Deny
Approve
Challenge Obfuscate
Decisioning Enforcement
Results
Access decisions based on fully orchestrated policies acting on comprehensive best-of-breed risk signals
Managed edge Zero Trust use-cases with the best vendors for the task

Figure 3: Feed best-of-breed risk signals into your orchestration policy engine to ensure appropriate decisioning, enforcement, and remediation.

Rapid development and integration

Best-practice Zero Trust Orchestration services make it easy to develop and deploy new user journeys by seamlessly integrating new services and components into authentication and authorisation flows. With a low-code, drag-and-drop interface, you can quickly extend your Zero Trust landscape to secure additional systems and resources, and easily introduce new identity, security and risk services to gain even richer context to inform your authentication and authorisation policies.

User journey optimisation

Zero Trust Orchestration not only creates a unified point of control for your Zero Trust architecture—it also provides centralised visibility across your user journeys. It enables you to introduce alternative flows and perform A/B testing to determine optimal risk thresholds. This gives the insight needed to add or reduce friction at appropriate stages in each user journey to ensure policy compliance and maintain security while also delivering a better user experience.

ZERO TRUST ORCHESTRATION SOLUTIONS – PINGONE DAVINCI

Having implemented PingOne DaVinci with multiple clients, Capgemini sees PingOne DaVinci as a best-practice solution for Zero Trust Orchestration in Identity. A particular strong point of PingOne DaVinci is that it has allowed us to build identity flows using its highly visual, drag-and-drop interface, without needing to write a single line of code. This simplifies and accelerates the process of creating, updating, testing and deploying user journeys that optimise security while minimising friction for end-users.

Furthermore, PingOne DaVinci is completely vendor-agnostic and integrates easily with third-party services. This makes it particularly suitable for organisations that want to build a Zero Trust Orchestration layer on top of their existing legacy identity systems and silos—reducing Zero Trust implementation times—as well as for greenfield identity management projects that aim to take a best-of-breed approach.

TAKING ZERO TRUST FROM THEORY TO PRACTICE

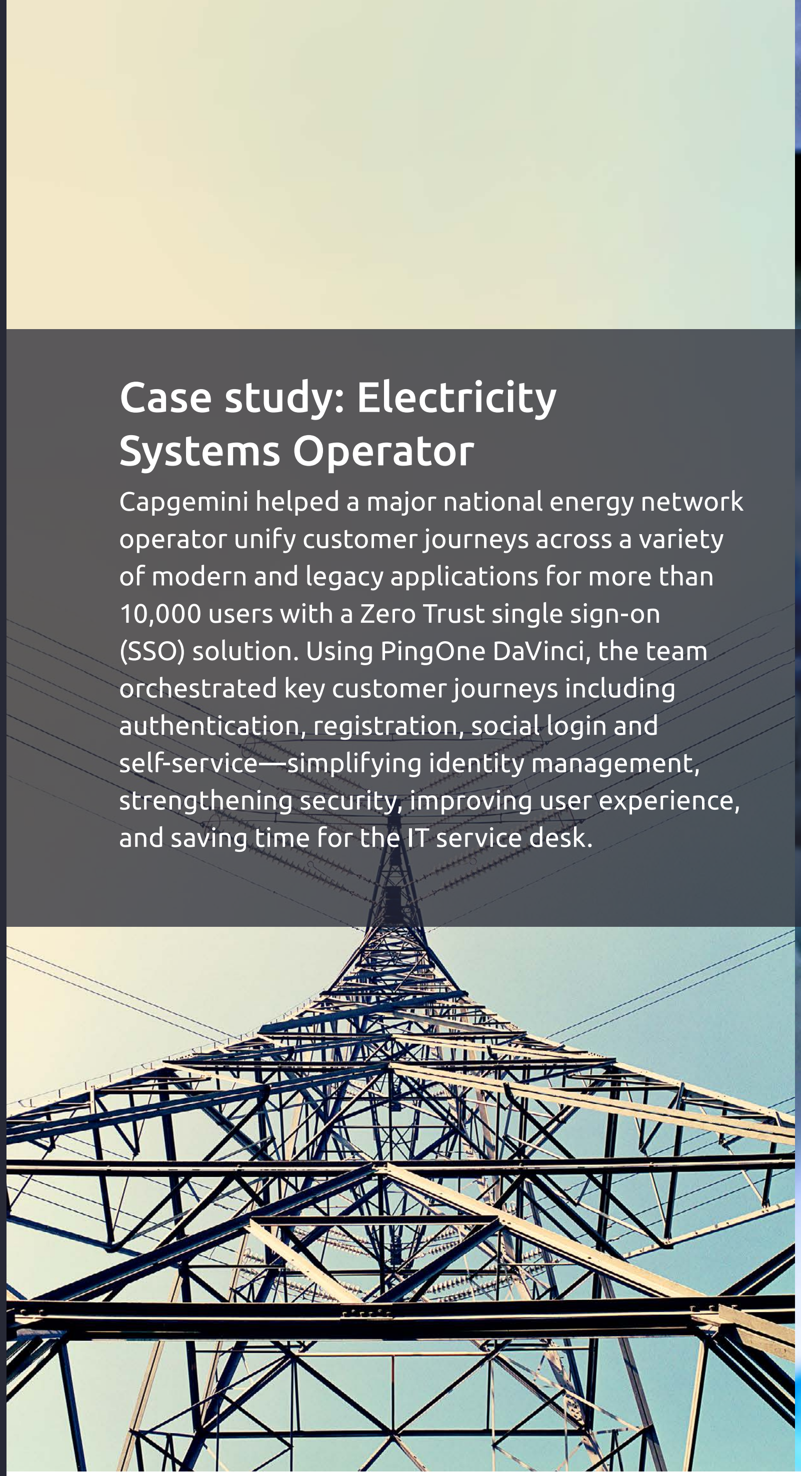
To make the shift to a Zero Trust Architecture, it helps if you can call on the experts. Capgemini has one of the largest Identity and Access Management (IAM) practices in the world, with over 1,000 consultants who have delivered more than 200 major IAM projects in the last five years alone.

Based on its long-established Ping Identity track record and number of certified staff, Capgemini is also a Ping Delivery Approved Elite Partner. And Capgemini has recently transformed its own internal IT security model to embrace Zero Trust principles, using Ping Identity extensively within the Zero Trust Identity tower and for Identity Orchestration.

Capgemini is now providing Identity and Zero Trust services to our clients, built around four key pillars:

- Assess: measure the maturity of your organisation’s approach to implementing Zero Trust in alignment with the industry-standard maturity model developed by CISA.
- Advise: advise on all elements of Zero Trust, from governance, operating models, and principles through to architecture and design – Zero Trust is not simply a matter of technology.
- Implement: work with you to implement secure Zero Trust environments, governance, and operational services.
- Operate: manage Zero Trust technologies from secure locations across the globe, providing full security monitoring and response 24x7.

Together with Ping Identity, Capgemini can work with you to help start or accelerate your Zero Trust journey – using our knowledge of all areas of Zero Trust including Zero Trust Orchestration to make this a reality.



Case study: Electricity Systems Operator

Capgemini helped a major national energy network operator unify customer journeys across a variety of modern and legacy applications for more than 10,000 users with a Zero Trust single sign-on (SSO) solution. Using PingOne DaVinci, the team orchestrated key customer journeys including authentication, registration, social login and self-service—simplifying identity management, strengthening security, improving user experience, and saving time for the IT service desk.

Case study: Pharmaceutical Company

Capgemini enabled a large multinational pharmaceutical company to modernise its digital landscape by creating a Zero Trust security framework for more than 20,000 employees across more than 150 global locations. The solution significantly improves the user experience and simplifies the technical infrastructure, as well as optimising capital and operational expenditure and streamlining the integration of new mergers and acquisitions.

NEXT STEPS

To learn more about how Capgemini and Ping Identity can help your organisation embrace Zero Trust Orchestration to provide your customers and employees with reduced friction user experiences, without compromising on security, reach out to us today.

AUTHORS

Rob Otto
Field CTO/Principal Solutions Architect
Ping Identity
Robotto@pingidentity.com

Andrew Critchley
Global Head of IAM Capability
Capgemini
Andrew.critchley@capgemini.com

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, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com

For further information please contact:
cybersecurity.in@capgemini.com

About Ping Identity

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. We let enterprises combine our best-in-claass identity solutions with third-party services they already use to remove passwords, prevent fraud, support Zero Trust, or anything in between. This can be accomplished through a simple drag-and-drop canvas. That's why more than half of the Fortune 100 choose Ping Identity to protect digital interactions for their users while making experiences frictionless.

Learn more at www.pingidentity.com.

Global Infra_11042024