



Zero Trust

*Build business benefits
by adopting a modern
security architecture*

Deloitte Zero Trust Services



Table of contents

3	Introduction	16	Client spotlight
7	The Deloitte Zero Trust Difference	20	Contacts
11	Putting our capabilities to work for you		

Securing the enterprise to enable digital transformation

The enterprise perimeter is dissolving as organizations become more interconnected and digitally driven.

Perimeter-based approaches to security architecture are no longer suitable to secure the modern enterprise.

As the boundaries of today's enterprise blur, new opportunities for business value emerge. So do new cyber risks and potential vulnerabilities.



How will you secure the modern enterprise?



How will you increase confidence across your business?

Where challenges and opportunities converge

Today, many organizations struggle with the value they get from their investments as they fail to address the security needs of the connected enterprise. That disparity compounds their ability to act on a wide range of disruptive changes, including:

<p>Making cyber an enabler of business outcomes, with measurable ROI E.g.: Brand reputation, digital trust, increased revenue, increased resilience, and fine avoidance</p> <p>73% of organizations are seeing positive value from cloud cyber services and updating controls and governance strategies¹</p>	<p>Widespread tech-driven disruption AI, 5G, and digital assets, growing interconnectedness</p>	<p>Accelerated cloud adoption External apps and platforms plus need for 24×7 availability</p> <p>+95% of organizations leading in cloud innovation are seeing a cost reduction across their IT organization²</p>
<p>Increased business complexity, enterprise digitalization, and IT costs</p> <p>~70% of technology leaders view technical debt as a hindrance to innovation and the No. 1 cause of productivity loss³</p>	<p>Growth of cyber threats—in number and sophistication</p> <p>91% of organizations reported at least one cyber incident or breach⁴</p>	<p>Modern workforce challenges Hybrid/remote, third-party connectivity, mobile apps, and device/software management</p> <p>81% of execs say work is increasingly performed across functional boundaries⁵</p>
	<p>Increasing third-party access More APIs/integrations, inherent supply chain risks</p>	<p>Expanding regulatory compliance needs Complex global environment, potential for fines</p> <p>Strategic business growth and innovation M&A, new product development, digital services, and competitive pressures</p>

^{1,2} [Deloitte US Future of Cloud Survey.](#)

³ [Deloitte Tech Trends 2024.](#)

⁴ [Deloitte's 2023 Global Future of Cyber Survey.](#)

⁵ [Deloitte 2023 Global Human Capital Trends Report](#)

Never trust. Always verify. Unlock end-to-end business value.

Deloitte's Zero Trust services provide a layered, disciplined approach that allows organizations to move from a legacy perimeter-based cybersecurity posture to one that eliminates implicit trust at every point.



Advise

Develop your strategic vision for a modern security architecture that enables the business



Implement

Deploy and integrate leading solutions to modernize capabilities in each of the Zero Trust core domains: *Identities, Workloads, Data, Networks, Devices*



Operate

Outcome-based managed services that streamline and operate capabilities needed to support a modern Zero Trust architecture

Our combined capabilities can help you increase the **speed of business**, reduce cost of **IT operations**, and accelerate **innovation**.

Business benefits from the Zero Trust model

Modernized infrastructure requires that organizations approach security differently. A Zero Trust approach can help protect the enterprise, close the transformation gap, and drive business agility.





The Deloitte Zero Trust Difference

Zero Trust: What it looks like



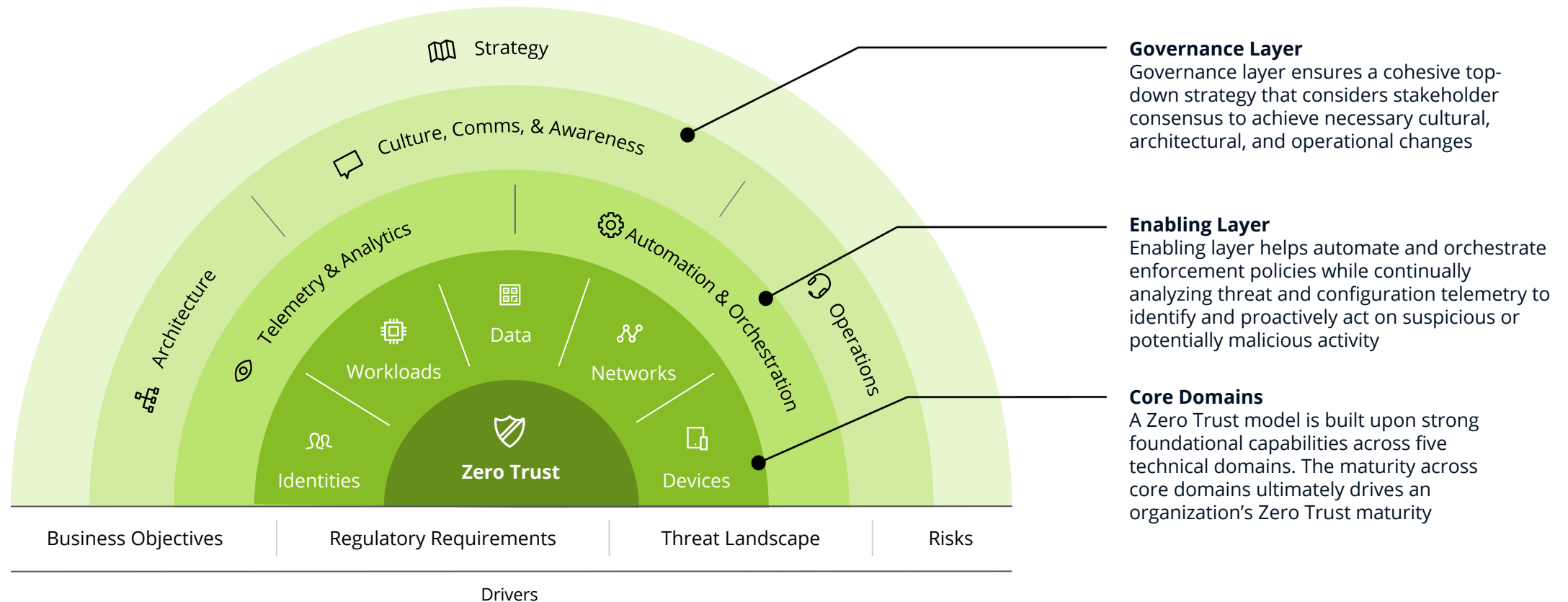
Adopt the principles of **least-privileged access** and context-aware authentication. Securely connect users and devices to enterprise applications and data over any network, at any time.

Embrace a modern **“never trust, always verify”** approach to providing and continuously validating access.











Shift to a new perspective across the enterprise—migrating from traditional and binary access control decisions (e.g., allow vs. deny) to a **risk-based posture** where each connection request is informed by contextual signals and continuously verified throughout each session. A Zero Trust architecture is the de facto approach to secure the modern enterprise.

How we help create a modern security architecture based on Zero Trust

Deloitte delivers capabilities that address end-to-end needs across three essential areas—core domains, the enabling layer, and governance.



How we help you unlock value in every layer

Governance Layer	Enabling Layer	Core Domains
 Architecture Provide a robust, mature, and flexible enterprise security architecture enabling appropriate risk appetite while allowing security by design and cutting-edge security solutions	 Telemetry and Analytics Achieve full visibility across all digital assets to deliver meaningful insights from different sources of digital infrastructure for all five core domains	 Identities Integrate centralized and consolidated identity technologies with the digital identity landscape to embrace context aware authentication
 Culture, Comms, & Awareness Facilitate active engagement of employees and embedding Zero Trust principles into the security DNA of the organization	 Automation and Orchestration Enable continuous security and compliance monitoring of digital infrastructure by deploying automated use cases across all core domains	 Workloads Enable secure cloud deployment pipelines based on security reference architecture through automated testing and application static and dynamic analysis
 Operations Enable IT operations to adapt to the changes caused by a Zero Trust model and facilitate alignment to its core principles through People, Process, and Technology improvements		 Data Ensure data-in all states (e.g., in-motion, at rest, in-change, in-use) and throughout the data lifecycle is protected, visible and under control
		 Networks Utilize public networks, identity-based access and micro-perimeter for legacy services (i.e., software-defined perimeters), rather than private networks and perimeter-base security
		 Devices Facilitate real-time assessed device trust level based on device health and conditional criteria



Putting our
capabilities to
work for *you*

Zero Trust *your way*—and with you every step of the way

Deloitte understands that no two client journeys are the same, which is why we work with you to implement Zero Trust on your own terms—with an iterative, incremental approach that allows you to...

Leverage your existing investments alongside new tools and processes to address potential capability gaps

Prioritize Zero Trust activities based on business impact and potential risk reduction

Minimize the potential for operational disruption

Demonstrate value before scaling to other parts of the enterprise

Access Deloitte's industry-leading cyber services at every step—across every layer and in every area of your business—through our advise-implement-operate offerings and industry-specific insights

A closer look at our key capabilities supporting Zero Trust

Advise

- ✓ Explore **use cases, technologies**, and possibilities through interactive labs and workshops, including our Zero Trust Experience Center
- ✓ Develop your **strategic vision** for a modern security architecture that enables the business
- ✓ Create a **detailed roadmap** for turning your vision into a reality
- ✓ Build the **business case** and create a detailed roadmap for Zero Trust adoption
- ✓ Continuously **evaluate and prioritize Zero Trust activities** to align them with evolving business needs and objectives
- ✓ Define requirements and **assess vendor technologies** for their alignment

Implement

- ✓ **Design and execute proof of value (PoV)** exercises within a client's environment
- ✓ **Facilitate vendor bake-offs** and technology testing
- ✓ **Leverage proprietary accelerators** to help rapidly unlock value through methodical technology implementation
- ✓ **Deploy and integrate leading solutions** to modernize capabilities in each of the Zero Trust core domains: Identities, Workloads, Data, Networks, and Devices
- ✓ **Integrate cyber solutions** with other enterprise apps and third-party solutions
- ✓ **Develop automation and orchestration use cases and capabilities** to enable a shift to a more proactive security posture
- ✓ **Enhance operational workflows** associated with Zero Trust technology modernization
- ✓ **Design user education and awareness materials** to socialize the potential end user impact and facilitate adoption of modern technologies

Operate

- ✓ **Provide outcomes-based managed services** that streamline and operate enhanced capabilities needed to support a modern Zero Trust architecture, including Cyber Operate services:
 - Digital Identity by Deloitte
 - Managed Secure Access Service Edge (M-SASE) by Deloitte
 - Managed Extended Detection and Response (MXDR) by Deloitte
- ✓ **Conduct periodic cyber risk assessments** and related services such as Cyber Incident Readiness, Response, and Recovery (CIR3) services, as needed
- ✓ **Provide 24x7 security operations center (SOC) services** through Deloitte's Global Cyber Intelligence Centers (delivered through Deloitte's Detect & Respond services)

Why Deloitte for Zero Trust and a modern security architecture?

To help you drive outcomes that matter, Deloitte provides a global network of professionals who bring a powerful business lens, domain-level expertise, multidisciplinary capabilities, leading edge tools, and strong vendor relationships.

Multidisciplinary capabilities

- Enabled by the Deloitte network's multidisciplinary model
- Covers needs across business consulting, tax, accounting, audit, assurance, risk advisory, technology, and financial advisory
- Can apply additional lenses for assessing potential regulatory risk and implications for implementing Zero Trust solutions

Powerful business lens

- Focused on your business needs and objectives, with industry-specific expertise and IP
- Services tailored for your specific business challenges
- Proven ability to unlock business value (e.g., operational efficiencies, faster innovation, greater business resilience, regulatory fine avoidance, risk reduction)
- Deep domain-level expertise in all areas of the enterprise

Leading tools

- Proprietary assets and resources to accelerate your Zero Trust journey
- Interactive lab experiences for building and refining your cyber strategy
- Exclusive maturity assessment models, benchmarking tools, reference architectures, and playbooks
- Industry-specific preconfigured solutions and tailored approaches
- User awareness and change management programs

Extensive global network

- Professionals in analytics, risk legal/regulatory, digital transformation, technology consulting, and other disciplines
- 25K cyber practitioners working on cyber projects worldwide
- 30+ years of providing cybersecurity services, with 10 years managed service delivery
- 3 Cybersphere Centers for 24x7x365 operational support and solution delivery globally, plus in-region satellite centers

Strong ecosystem alliances

- Close relationships with leading technology vendors
- Vendor alliances beyond security—including ERP, HR, and cloud service providers
- Ability to address complex needs for cyber, business solutions, and tech innovation
- Focused on an architecture leveraging the solutions your business uses and needs

The potential value you can expect for your business

Create a solid foundation for Zero Trust that allows you to remove implicit trust and confidently verify access—all while unlocking broader business benefits and creating a bigger impact for your organization.



Adopt a modern security architecture for today's evolving landscape of threats and opportunities

Move away from less effective and costly legacy solutions that depreciate over time and require significant capital expenditure (CAPEX) to maintain

Embed Zero Trust principles across your business, helping increase the speed of business and growth of stakeholder confidence

Accelerate innovation and adoption of new technologies, including AI, IoT, and cloud solutions

Streamline access- and security-related processes as part of M&A activities

Meet regulatory requirements with greater confidence, preventing heightened scrutiny and financial penalties

Protect the confidentiality, integrity, and availability of business-critical systems and other resources, to support greater business resilience

Incorporate security practices and solutions that enable the remote workforce and support the future of work

An abstract graphic in the top-left corner of the slide, consisting of several concentric, semi-transparent circles in shades of blue and teal, creating a layered, circular pattern.

Client spotlight

Client story

Bringing Zero Trust to life for a life sciences leader

The issue

A large global biopharmaceutical organization faced layers of risk across its regions—including lack of visibility and security controls in emerging regions. While the company had embraced a “cloud first” vision for its business, it continued to struggle with antiquated systems and processes—including outdated network and security standards, as well as aging on-premises infrastructure.

Other factors—such as backhauled network traffic, an abundance of appliances and hardware across sites, and an inability to isolate and segment environments—made it difficult to manage costs, stop malware propagation, and stand ready for future cyber threats.

The solution

Company leaders chose Deloitte to design a reference architecture and develop segmentation capabilities across networks, applications, and sites in its high-risk regions. To help the company reduce risk and achieve key business outcomes, Deloitte led security and engineering functions across a number of areas. Deloitte collaborated with the company to:

- **Design** a reference architecture that emphasized Zero Trust, depicting the company’s current, interim, and future state
- **Identify** high-risk applications, sites, and countries
- **Align** multiple groups and initiatives—such as Network Services, Identity Management, Enterprise Apps, and Cloud Engineering—to produce a cohesive reference architecture
- **Prioritize** segmentation initiatives across network, application, and identity capabilities
- **Develop** a method to isolate networks in emerging markets, in case of malware propagation, government instability, or business divestiture

As part of the Zero Trust initiative, Deloitte leveraged the SABSA (Sherwood Applied Business Security Architecture) framework for establishing its design approach. Deloitte also inventoried and prioritized global services and dependencies, to help guide migration from on-premises systems to the cloud.

The impact



A modern security architecture based on Zero Trust principles



Greater insights and visibility into risks and progress, supported by an executive dashboard



Enhanced enterprise readiness for malware and other cyber threats



Reduced risk across the company, especially in emerging markets



A strong foundation to support the organization’s “cloud first” strategy for the future

Zero Trust, infinite value

Deloitte's global scale, trusted leadership, and depth of cyber services is unmatched.

Our Zero Trust services bring those strengths together—with Deloitte's industry-specific experience, leading technology alliances, and specialized teams all focused on helping you modernize your organization's security architecture.

The greater value? Capabilities that allow you to increase the speed and agility of your business, and operate with greater efficiency and resilience.

25k

Cyber practitioners
working on cyber
projects worldwide

150+

Countries

30+

Years of experience
in cybersecurity



Deloitte named
a global leader in...

Ranked #1 in Market Share for Security Consulting Services based on revenue for 12th consecutive year by Gartner¹

Deloitte is a Leader in the 2024 IDC MarketScape for Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services Vendor Assessment²

Deloitte is named a Leader in the Cybersecurity Risk Management Services 2023 Vendor Assessment by IDC³

1. [Market Share Analysis: Security Consulting Services, Worldwide, 2022. Published on 14 July 2023. – ID G00785548.](#)

2. [Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment. By Cathy Huang. Published January 2024 – ID#US50463423.](#)

3. [IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment. by Philip D. Harris. October 2023. IDC #US49435222](#)

Move to *modern*.
Build business *benefits*.

Deloitte Zero Trust Services



Marius von Spreti

Partner
Cyber Risk Advisory, EMEA
mvonspreti@deloitte.de
+49 89 290 365 999



Andrew Rafla

Principal
Cyber Risk Advisory, US
arafla@deloitte.com
+1.201.499.0580



Shweta Pandey

Partner
Cyber Risk Advisory, APAC
spandey@deloitte.com.au
+61 432 510 203

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 457,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2024. For information, contact Deloitte Global.