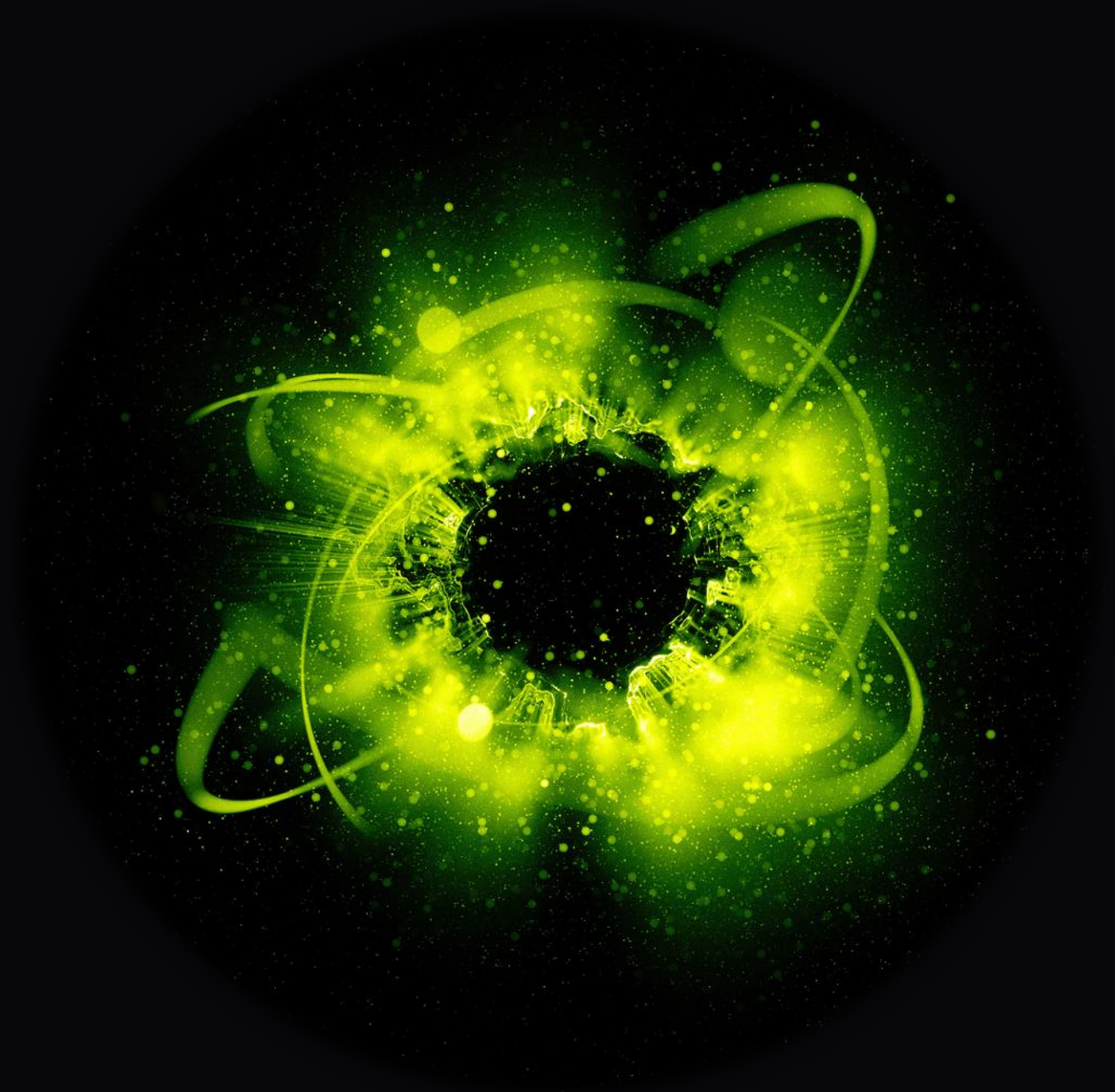
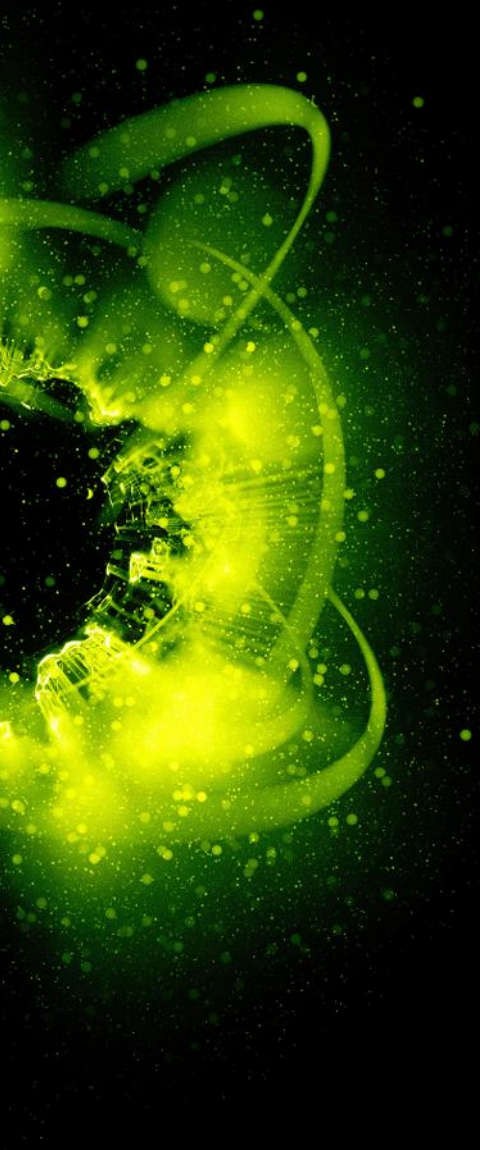
Deloitte.



Zero Trust

A revolutionary approach to Cyber or just another buzz word?

2021



Despite the recent marketing hype, the concept of Zero Trust is not new – in fact, academics have spent the last 20 years debating the advantages and challenges of a security model that is based on the principle of never trusting and always verifying. It's only been in the last few years that the technology has started to catch up, making this once theoretical model a reality and generating lots of excitement, with vendors bringing new products to market with big claims and game-changing promises.

Through this document, we will look beyond the hype and break down what Zero Trust is, the business drivers behind it and the benefits it can bring. We will also explore approaches to Zero Trust, what the journey feels like and share some common pitfalls and challenges along the way.

Why Zero Trust?

The drivers and trends putting Zero Trust on the agenda

In recent years, Zero Trust has become somewhat of a buzz word within industry circles, with lots of attention placed on how this innovative approach to cyber security can help organisations to defend against the new generation of attackers – who are better networked, more organised and who have access to tools that only a few years ago were the preserve of nation state actors.

However, there are a broader set of business drivers and demands, which are pushing Zero Trust onto the corporate agenda and highlight the need for greater speed and adaptability in how organisations approach cyber security, as they seek to survive and thrive in an increasingly digital world.

What is driving the move to Zero Trust?

The rapid pace of digitalisation is increasing IT complexity and driving up cost

Adversaries are becoming more sophisticated and are outmatching current cyber defences

The development of digital products and services is being constrained by rigid cyber security controls

The shift to the Cloud is demanding a new approach to securing critical business data

An increasingly mobile workforce now expect to be able to work from anywhere, on any device

The demand for better and easier business collaboration requires a more agile approach to security

The cost of compliance is rising due to overlapping and rigid controls, and more strenuous requirements

The proliferation of Shadow IT is increasingly hard to contain without damaging business agility

Securely managing Mergers and Acquisitions is increasingly complex, time consuming, and costly

Increasingly complex vendor landscapes and supply chains require a more efficient approach to security

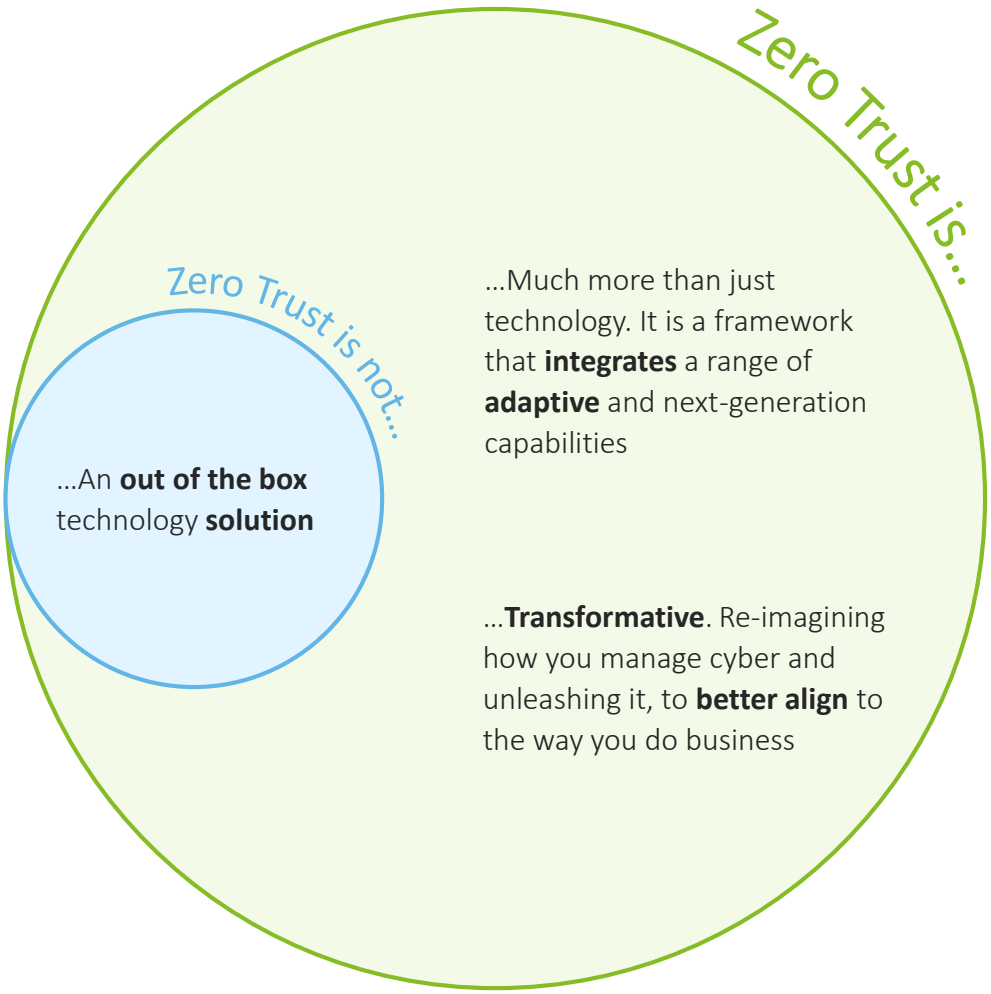
Understanding your drivers to embarking on a Zero Trust journey will help shape the path you take

Introducing Zero Trust

What does it really mean?

Zero Trust is a framework for looking at Cyber Security in a new way. Based on the fundamental principle of "never trust, always verify", Zero Trust moves away from the traditional perimeter-based concept of managing security, to one where trust is established between individual resources and consumers, as and when needed. Trust is determined based on a combination of internal and external factors and is constantly revalidated.

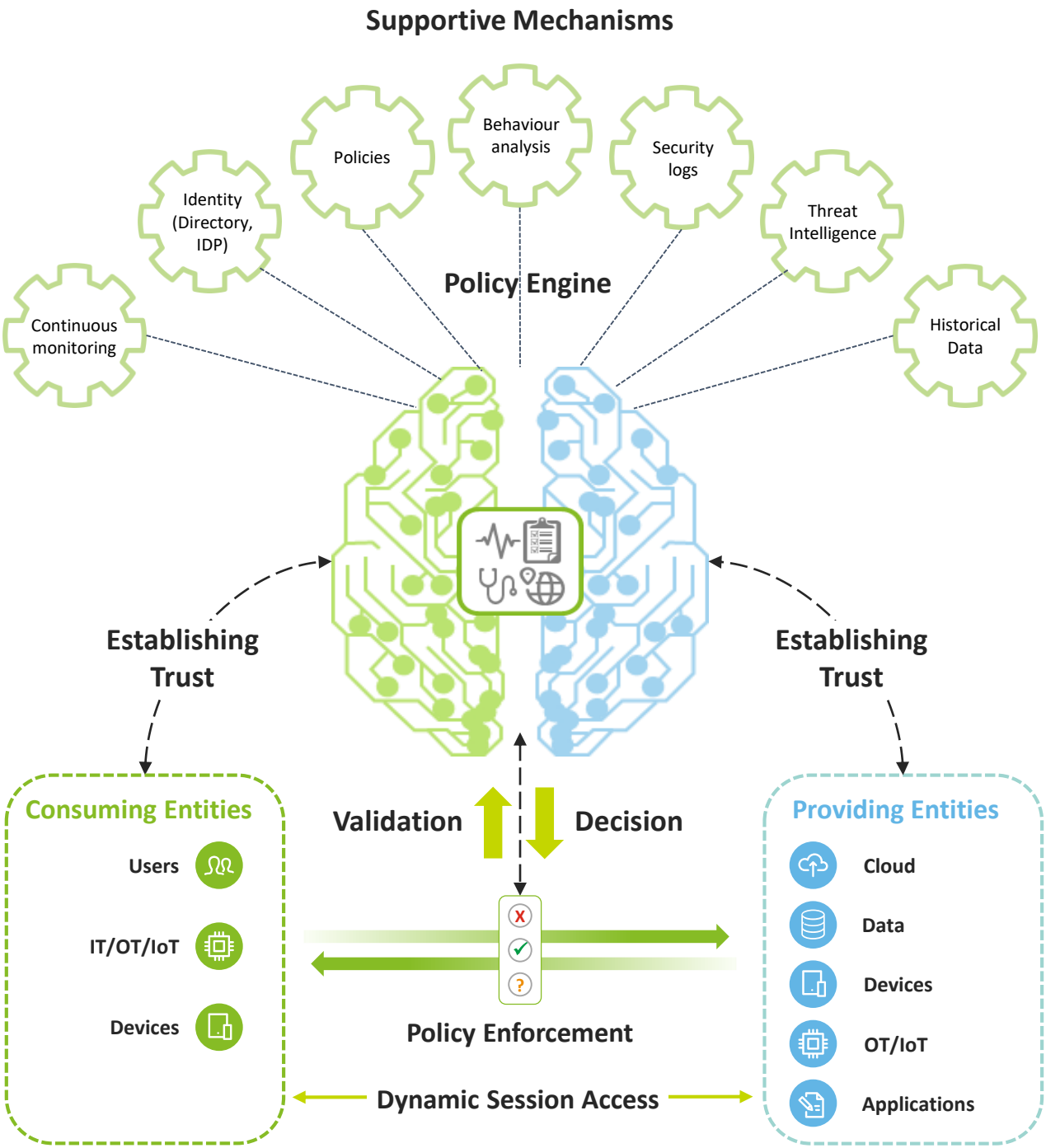
Zero Trust releases the shackles from IT, enabling businesses to strip away cumbersome and expensive security controls, and build a more dynamic, efficient and customer-orientated technology platform.



Zero Trust is a new way of thinking about security based on the principles of "never trust, always verify" – aligning the way you do security to the way you do business

Key Concepts

How does it work?



All communications, regardless of location, are treated from the same starting point of having no inherent trust. Trust is established by a dynamic policy, informed by a range of signals – from behavioural analytics to threat intelligence - and is constantly revalidated

Benefits of Zero Trust

Should we believe the hype?

There is a lot of excitement around Zero Trust with big claims made by vendors about the benefits that it can bring – but should we believe the hype? While it is certainly not a silver bullet, Zero Trust can unlock a range of opportunities for organisations by better aligning security to how they do business, reducing risk, improving agility and driving down operating costs – however these benefits are hard won and require support and commitment from across the organisation to truly be realised.

The benefits of Zero Trust

Enabling the modern workplace
Supporting the 'new normal' and enabling employee productivity, by reducing friction and providing secure and flexible access

Supporting digital products and services
Using Zero Trust principles to securely develop digital products and services and enable the transition to Industry 4.0 – creating a head start against competitors

Reducing and managing risk
Enhancing the ability to detect and respond to threats in real time and reducing the blast zone of attacks by restricting lateral movement

Sustainably reducing cost
Reducing security costs by minimising IT complexity through automating, simplifying and standardising the way we do cyber

Enhancing business agility
Enabling faster and secure innovation, greater business agility, and easier and more efficient integration with partners and third parties

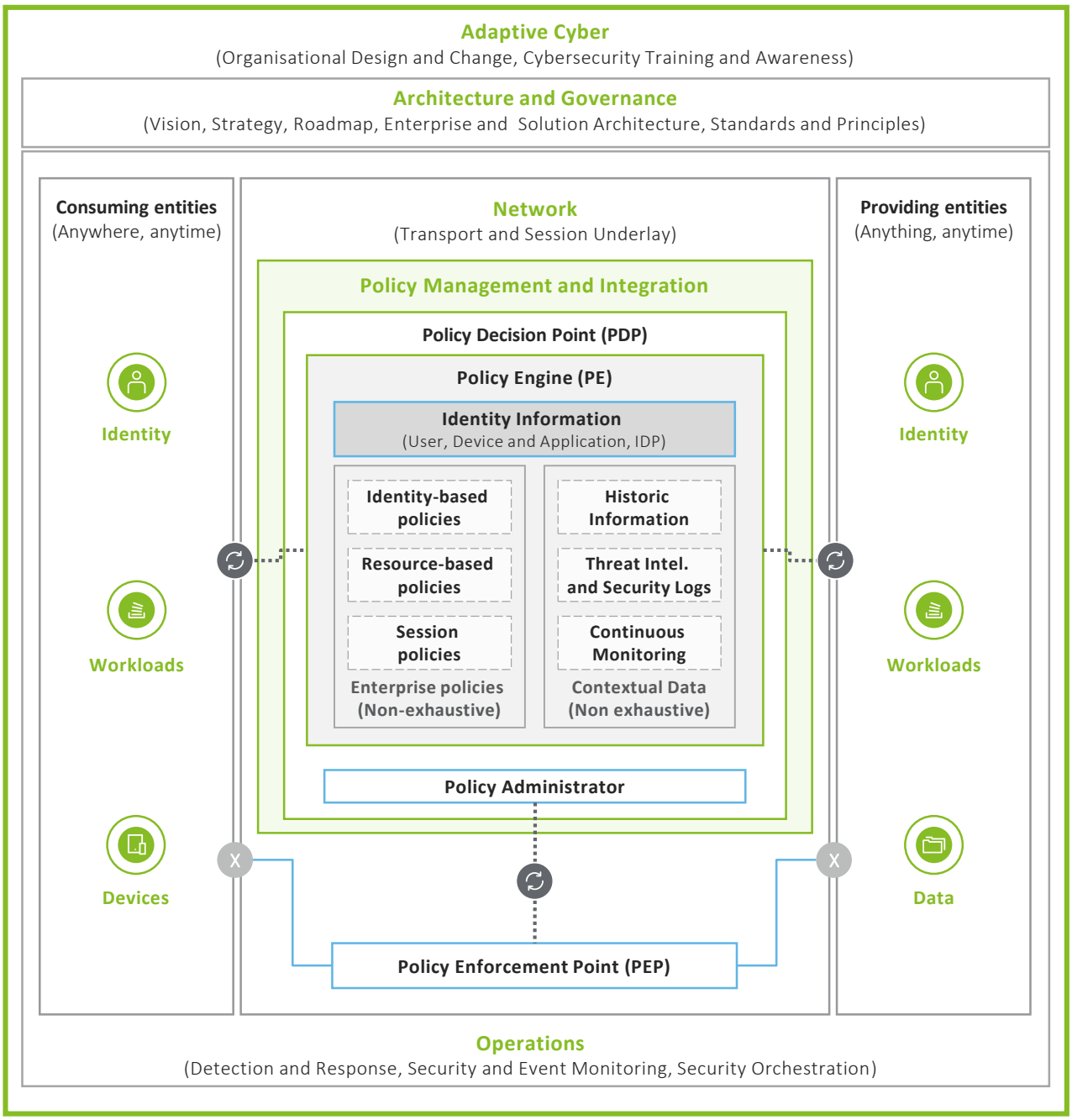
While Zero Trust can help unlock a range of benefits, to truly realise its potential you need to approach it methodically, with a clear line of sight to how Zero Trust will deliver these benefits for your organisation

Zero Trust functional architecture

Taking a look under the bonnet

Deloitte's Zero Trust functional architecture is aligned to NIST's Zero Trust Architecture standards (SP 800-207) and is designed to provide an end-to-end view of the key components and how they interact in a Zero Trust environment.

Zero Trust functional architecture



Deloitte's Zero Trust functional architecture helps provide a target state for the end-to-end Zero Trust vision

Unlocking Zero Trust's potential

Building a successful Zero Trust programme and delivering business outcomes

The adoption of Zero Trust should be viewed as an organisation-wide journey, that is as much about repositioning how we approach and manage cyber risk across the organisation as it is about evolving technology capabilities. At Deloitte, we use a framework which encompasses nine foundational domains which help to shape the Zero Trust journey and deliver desired business outcomes

Architecture and Governance Enterprise architecture and contextual and dynamic security policies for the adoption of Zero Trust	**From**: static, complex and reactive security architecture	**To:** contextually-aware, simpler and dynamic enterprise security architecture
Network Private networks retired and use of public networks and micro-perimeter based legacy services*	**From**: private network with enterprise-wide perimeter	**To:** use of public networks with resource/services perimeter
Identity Consolidated identity technologies and processes to enable adaptive access	**From**: disparate identity stores and pre-defined static access	**To:** consolidated identity stores (e.g., Identity providers and Trust-based access)
Operations Predictive and preventative security tooling and automated processes	**From**: reactive, pre-defined metric measurement and manual response	**To:** predictive, monitoring and automated response
Devices Real-time assessed device trust level based on device health and additional criteria	**From**: pre-defined or accepted device trust level	**To:** dynamically assessed device trust based on multiple criteria
Workloads Context-aware access using defined trust levels to applications, secured with micro-perimeters	**From**: static predetermined access and an inherited trust model	**To:** dynamic access based on health and other criteria
Data Trust levels based on enterprise-wide classification of data	**From**: varied data type and sensitivity classification	**To:** enterprise-wide classification of data-based value and sensitivity
Policy Management and Integration Centralised security policy management and dynamic enforcement for resources	**From**: siloed security policy management and static controls	**To:** centralised security policy management and dynamic policy enforcement
Adaptive Cyber Dynamic security organisation closely aligned to business priorities and continuously adapting to the internal/external environments	**From**: static cyber organisation, disconnected from the business, without clear ownership of cyber risk	**To:** shared accountability for cyber and continuous collaboration amongst teams to deliver business goals

Zero Trust programmes involve much more than just technology and require the integration of a broad set of capabilities to realise its full potential

* Click here to read Deloitte's point of view on the evolution of 'Enterprise Network Security Architecture'

The journey to Zero Trust

What does it feel like?

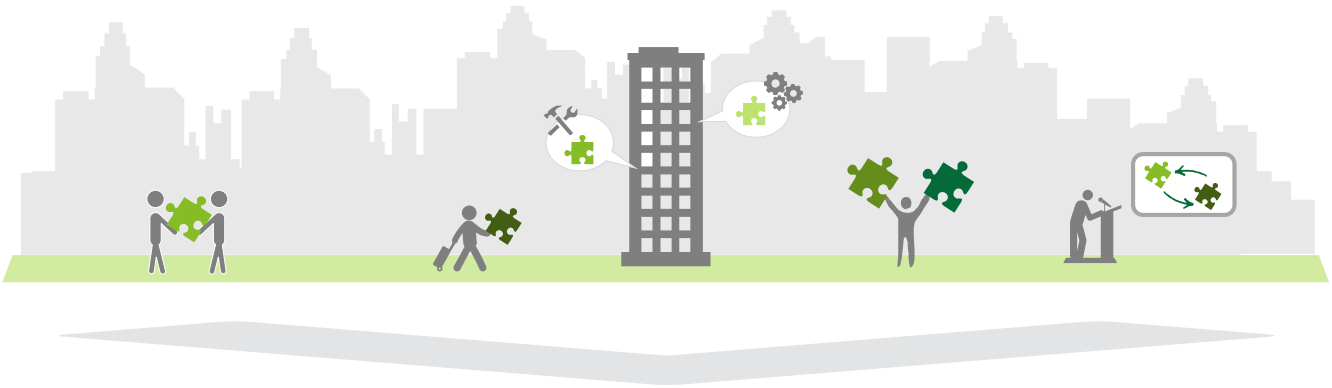
The journey to Zero Trust is different for every organisation and will be shaped by your business priorities, the benefits you are seeking and your ambition to change. This is what that journey may feel like:

Your organisation's journey to Zero Trust will be different, depending on your drivers, the benefits you want to gain and your ambition to change

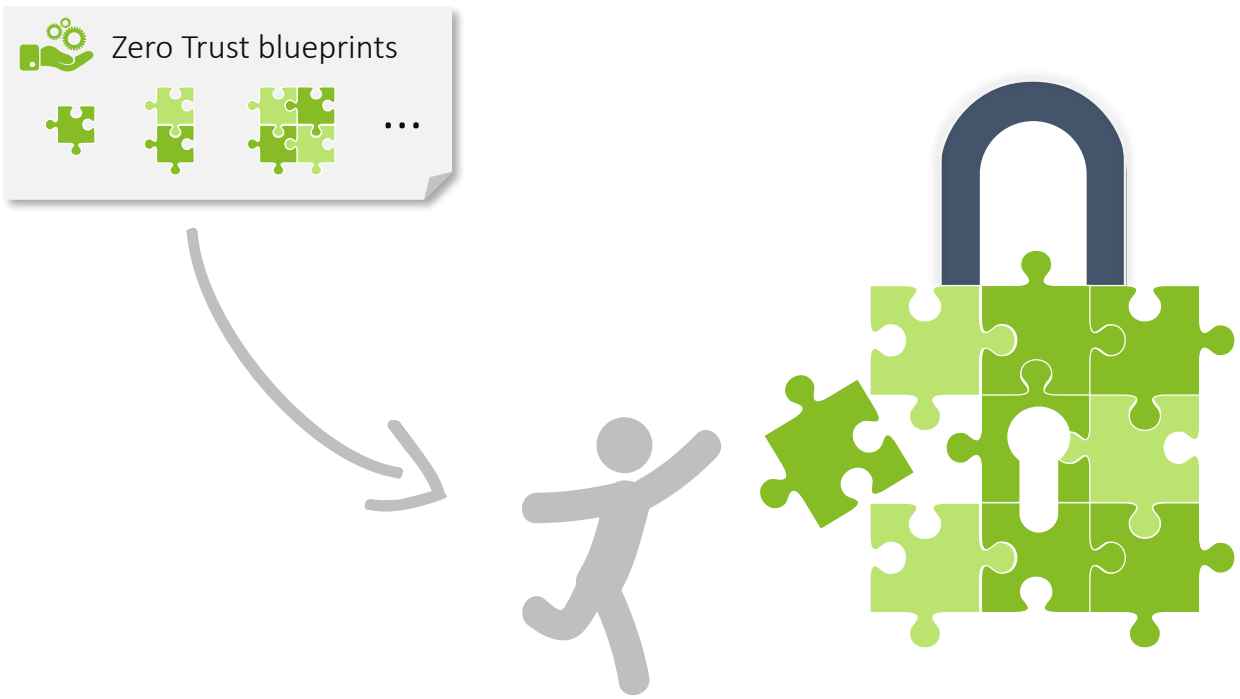
Taking the first step

Adopting Zero Trust doesn't mean starting afresh

While Zero Trust can help organisations achieve transformational business change, the adoption of a Zero Trust framework does not necessarily entail a radical overhaul of your existing cyber capabilities. From our experience, most organisations already have some of the key building blocks and fundamental capabilities required to embark on a Zero Trust journey and realise some of the potential benefits.



Zero Trust environments are primarily built through the integration and evolution of existing cyber capabilities, supplemented by the introduction of next generation technologies. With a clear line of sight to the benefits that are being sought, organisations must set clear architectural principles and roadmaps, which provide a common Zero Trust blueprint from which capabilities can be built around.



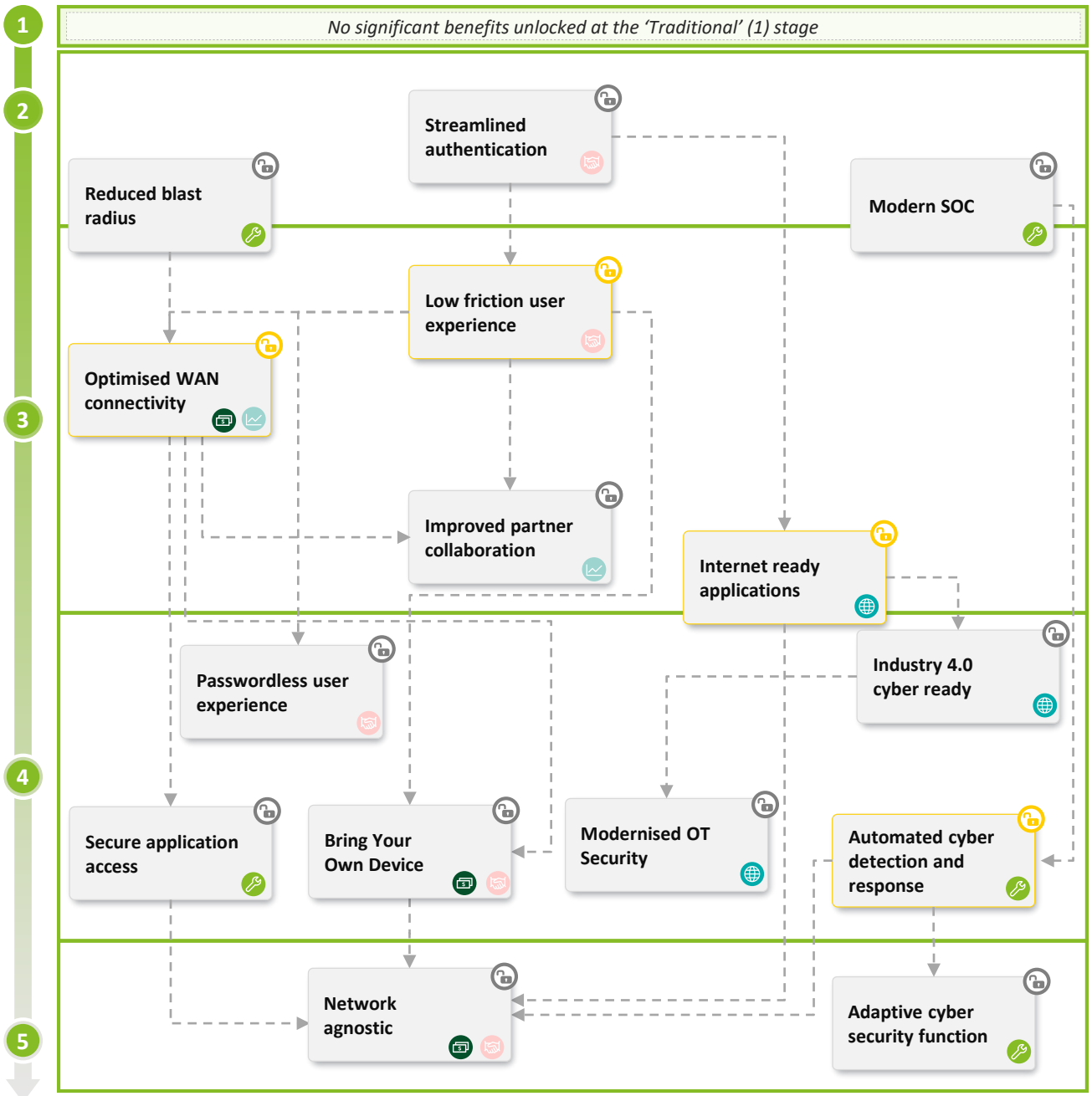
Moving to Zero Trust doesn't mean throwing everything out and starting again. Zero Trust involves the evolution and integration of existing capabilities with next-generation technology

What benefits does Zero Trust unlock?

Unlocking benefits along the Zero Trust journey

Across the Zero Trust journey, capabilities can be built and integrated to 'unlock' a series of benefits – from decreasing cyber risk and improving user experience to reducing IT costs and enabling better digital collaboration. With clarity on your business priorities, and leveraging our Zero Trust framework tool, Deloitte can support you in mapping the right path for your organisation, providing clear and measurable alignment to defined business outcomes.

Example Zero Trust Roadmap



Key: Zero Trust Benefits

Enabling the modern workplace | Supporting digital products & services | Reducing and managing risk | Sustainably reducing cost | Enhancing business agility | Critical benefit unlocked

Challenges in adopting Zero Trust

Exploring the common obstacles in implementing Zero Trust

While every organisations' journey to Zero Trust will be different and shaped by their business priorities, there are often a common set of obstacles and pitfalls that will need to be navigated – some of these include:

Embracing change

Zero Trust must be supported by a dynamic and **adaptive cyber organisation**, which embraces new ways of working

Integrating legacy

Bespoke approaches are often required to **enable legacy systems** (IT & OT) to participate in Zero Trust environments

Having end-to-end visibility

Zero Trust requires **end-to-end visibility** of what you have and how it is used in order to provide the basis for trust

Incomplete solution

There is **no silver bullet for Zero Trust**, with no vendor providing an end-to-end solution

Business collaboration

Close collaboration is required between Cyber and the rest of the organisation to ensure clarity of purpose and alignment

Designing for adaptability

Zero Trust is evolving **rapidly.** New capability arrives frequently – a Zero Trust programme must be **agile** to keep pace

Making it all work together

The **lack of common Zero Trust standards** leads to integration challenges between solutions

Taking the first step

Establishing the right governance and **understanding where to start** is fundamental to success

Any Zero Trust journey will be faced with pitfalls and obstacles that will require support, investment and buy-in from across your organisation to successfully navigate

Case studies

How Deloitte is supporting organisations on their Zero Trust journeys

Transport and Logistics Company

Main drivers: *Closer relationship with customer and digitalisation of value chain*

Situation:
A global transport and logistics company is on a transformational journey to become the global leader in the industry. As part of this transformation, the organisation are modernising their legacy application portfolio and seeking to open it up to trading partners.

Action:
Deloitte is leading the delivery of this transformational programme. We're currently working hand-in-hand with the client to modernise legacy applications, implement new SaaS applications and perform the various integrations. Applications are being deployed on an API-centric, zero-trust, cloud-native architecture, which means that employees, trading partners and application APIs are able to securely connect and communicate via the public internet, without the need for VPNs or private connections.

Industrial Conglomerate

Main drivers: *Digital transformation, secure and protect customer critical IT and OT assets*

Situation:
An Industrial Conglomerate needed support in getting executive level buy-in and funding for a Zero Trust programme.

Action:
Deloitte worked closely with the client to understand their ambitions and drivers, and develop a compelling business case and vision for Zero Trust that was anchored to the business' strategic priorities. Deloitte also developed a capability assessment model to assist the client with making the right decisions along their journey and provided a roadmap with prioritised initiatives to meet the benefits being sought by the programme.

Global Aircraft Engine Manufacturer

Main drivers: *Easier M&A integration and ability to collaborate with third parties*

Situation:
A global aircraft engine manufacturer needed to create a new technology environment to accommodate a newly acquired business. This challenge was compounded by requirements of flexibility and high availability.

Action:
Deloitte was responsible for delivering an end-to-end Zero Trust solution, from defining programme requirements and building the conceptual architecture, through to the implementation. This highly-scalable Zero Trust solution enabled frictionless collaboration with third parties, whilst achieving high availability and resilience requirements for this essential business function.

Why Deloitte?

Our experience and what sets us apart

Breadth of our offering

We see the Zero Trust big picture and understand the scale of change required – from networks and identity, to changing the organisation itself to work in a more adaptive way. We understand the 'why' of Zero Trust as well as the 'how'.

Depth of our experience

We have in-depth experience in delivering and implementing the programme of change, with specialist skills across all nine domains of Zero Trust.

Technology independence

Our independence ensures our credibility as a trusted advisor and enables us to provide clients with unbiased advice on the pitfalls and challenges in implementing Zero Trust, while still allowing us to bring the right technical skills to the table.

Deloitte's Zero Trust framework

Our assessment and planning tool supports clients in choosing their Zero Trust journey, helping them to make the right decisions along the way and flex the programme to accommodate any changes during delivery.

Passionate Partnership

We are passionate about partnering with clients on Zero Trust to work together to build innovative solutions and tackle the big challenges head on.

Contact us

Wil Rockall
wrockall@deloitte.co.uk

Matt Holt
maholt@deloitte.it

Fadi Mutlak
fmutlak@deloitte.com

Serdar Cabuk
scabuk@deloitte.dk

Karthi Pillay
karthi.pillay@deloitte.fi

Richard Price
richardprice@deloitte.co.uk

Luís Abreu
labreu@deloitte.pt

Marius von Spreti
mvonspreti@deloitte.de