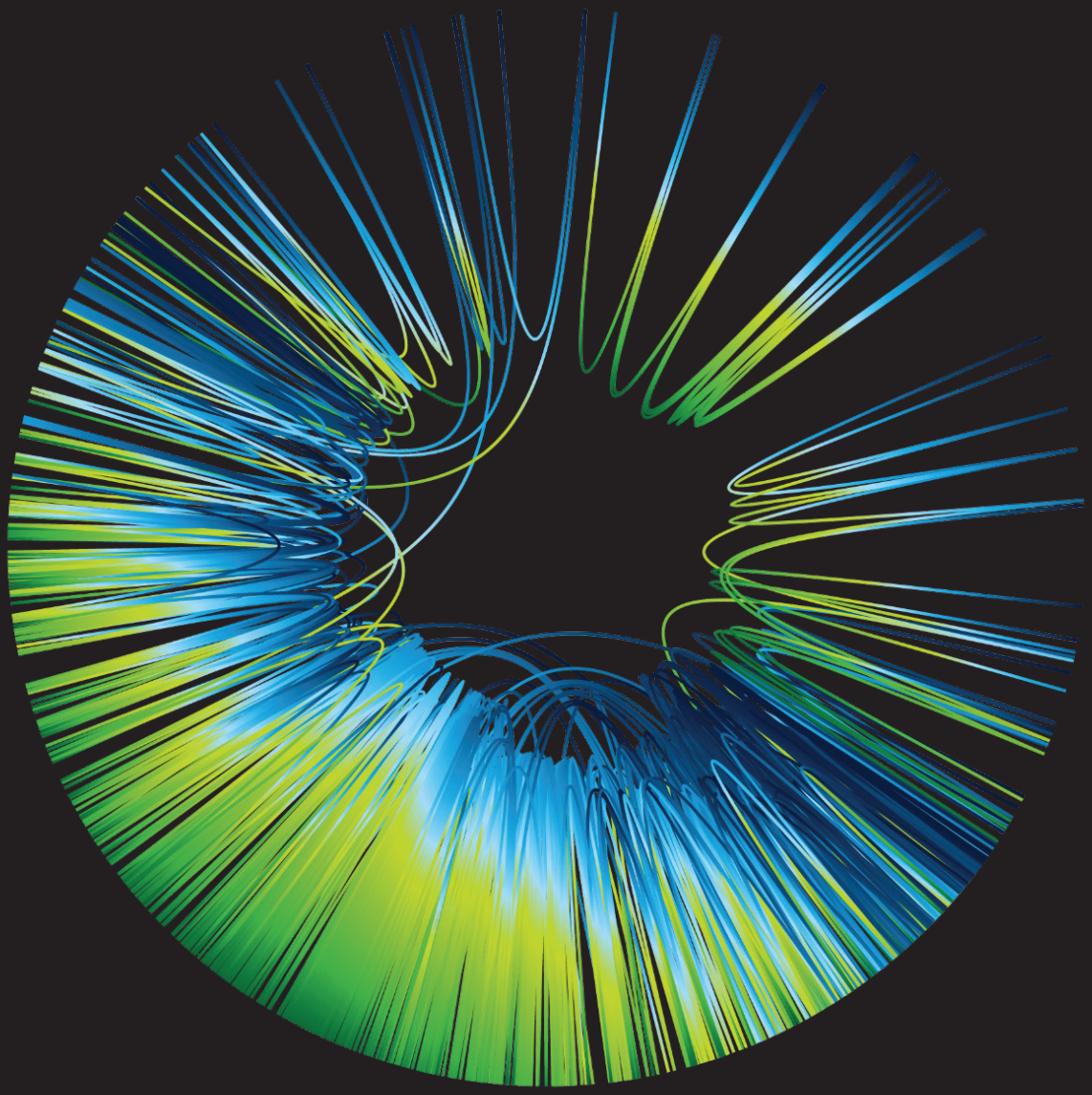
Deloitte.



Journey from a defence in depth approach to a Zero Trust access model

Enterprise Network Security Architecture Evolution

December 2020

Enterprise network security architecture evolution **Deloitte's point of view**

In this era, markets are becoming increasingly fast-paced with significant evolving technologies and shifting towards digitalisation. Enterprises are adapting networks in order to meet the challenges faced by a hyperconnected world and corresponding raising risk of exposure to cyber threats. Currently, there is a gap on comprehensive knowledge and information available regarding the journey ahead for the evolution of enterprise networks in this context. To fill in this gap, in this paper Deloitte proposes a view on the different stages for the network security evolution, addressing the architectural and capability requisites.

Through this document, we will look at the evolution of network security architectures from a defence in depth layered approached with usage of private networks to public cloud based connectivity, SDPs and micro-segmentation. Moreover, we will also explain Deloitte's approach and how these new architectural changes can be implemented.

A hyperconnected world

Today's world is about connecting people, systems and sharing data everywhere at anytime, enabling new digital solutions and products

In an increasingly connected world, the speed at which data flows is rapidly evolving and new digital business models intensify markets competition. With the digital transformation and developments in technology, more devices and "things" are getting connected, increasing the enterprises' network dimensions and complexity while bringing as many domains as possible to the public internet (cloud centricity). Moreover, COVID-19 has accelerated the digital economy and changed the ways of working, and the ways on which connectivity resources are consumed.

Main trends influencing hyperconnectivity

Global Footprint & Connectivity

The digital transformation has dramatically affected today's ways of working, allowing borderless expansion and instant communication from anywhere in the world

***59 ZB** **data to be created, captured and consumed** in 2020. Data becomes the most transacted 'good'*

Source: Statista

Remote Work

With the rise of communication platforms, workplaces started to embrace remote working, allowing to set up talented remote teams across the globe

2.7 billion** **workers** affected by COVID, challenging organisations to **embrace remote working

Source: Deloitte

Internet of Things

Connects people, processes, and data to deliver a unified experience, with the goal to have new capabilities and unprecedented economic opportunities

***31 billion** of **IoT connected devices** estimated in 2020, according to Statista*

Source: Statista

Emerging Technologies

The hyperconnected world is driven by new technologies working in conjunction such as SDN, cloud computing, 5G, Big-Data, Cybersecurity, AI and ML

***>1,000** **companies expected to test private 5G deployments** by the end of 2020*

Source: Deloitte

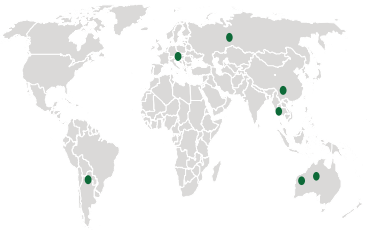
Increasing risk of exposure

Whilst hyperconnectivity transforms how network is used, attackers' behaviour is also changing by becoming more active, spread and causing higher damages

Today, cyber threats and attacks are recognised as significant global challenges which have serious financial and reputational consequences and damages. The cyberattack landscape has evolved as cybercriminals changed and adapted their behaviour and approach, by adopting a business-like mind-set, with streamline processes and tools. Furthermore, with an increased footprint, attacks are becoming more complex, strategic and sophisticated, impacting enterprises operations, its data confidentiality, integrity and availability.

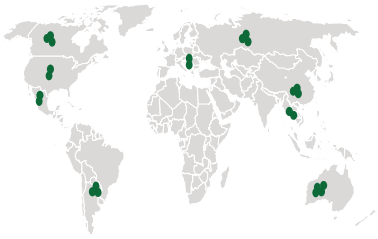
The evolution of attackers and caused damages

Standalone Attackers
Viruses, Trojans, Worms,Spam



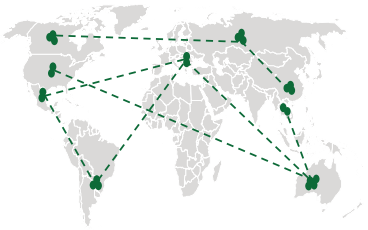
Attackers had an urge to prove that they could 'hack' and that things could be 'broken into' despite antivirus technology

Cluster of Attackers
OT/IT attacks, data breaches using sophisticated tools, espionage



They became more public and targeted victims based on geography, political ideology and strong financial standing

Network of Attackers
'Crime as a service', IT/IoT attacks, advanced malware



Attackers have established cybercrime networks that operate and profit like regular businesses. They recruit on a global scale

$6 trillion is the expected cost of **damages from network attacks** by 2021 (vs. $3 trillion in 2015)
Source: Cybersecurity Ventures

The **average time** to identify and contain a data breaches was **280 days** in 2020
Source: IBM

The worldwide **information security market** is forecast to reach approximately **$170.4 billion** in 2022
Source: Gartner

71% of breaches were **financially motivated** and **25%** were motivated by **espionage**
Source: Verizon

Every 11 seconds businesses will fall victim to a ransomware attack **by 2021** (vs. 40 seconds in 2016)
Source: Cybersecurity Ventures

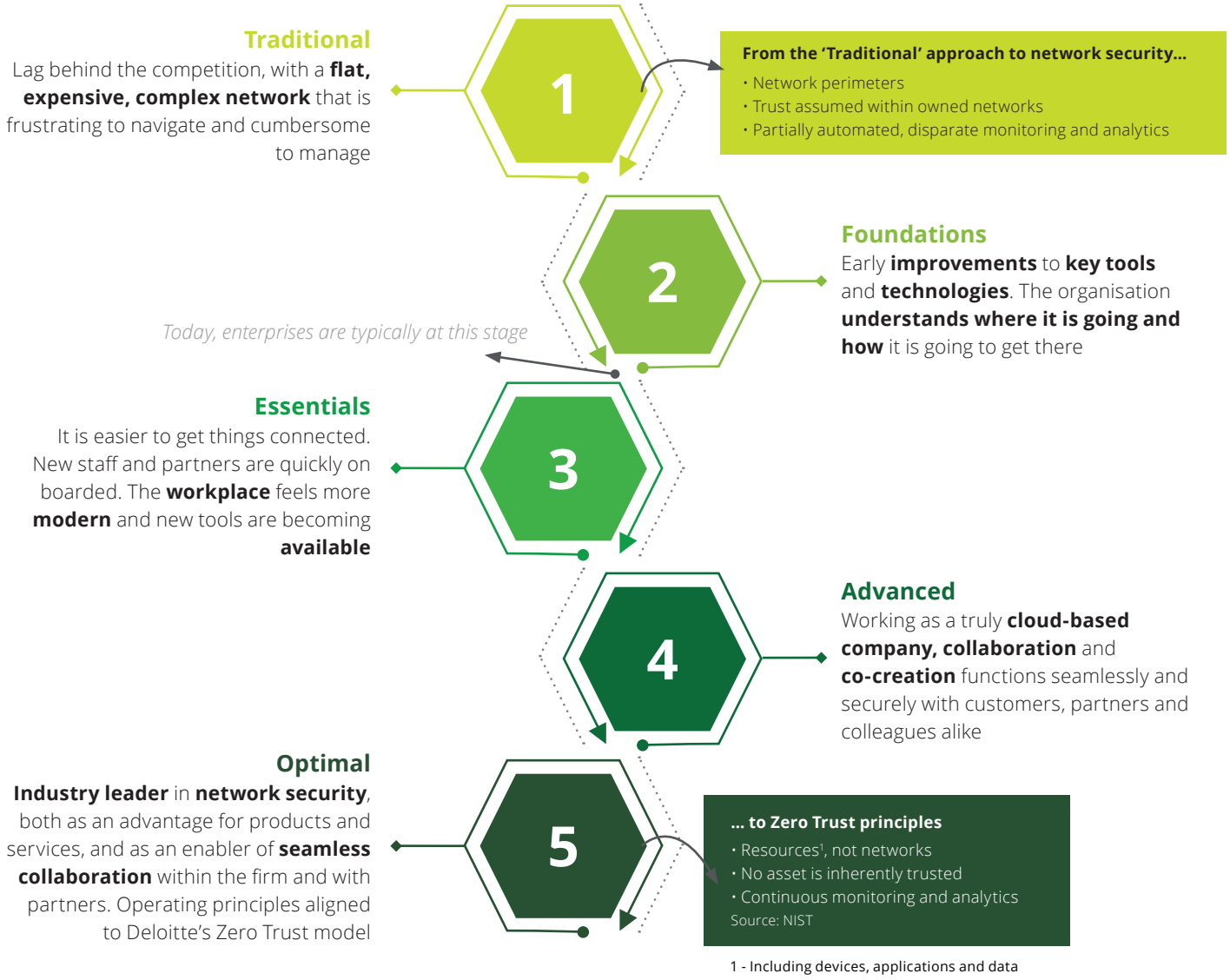
Enterprises need to invest on the evolution of their network security architecture and capabilities to face current challenges and not jeopardise the monetisation of digital products & services

The network security journey

Deloitte's network security maturity model identifies five stages, from a complex and flat network to a Zero Trust based strategy

Deloitte's view on network security encompasses five stages of maturity. Pursuing an evolution of the network does not assume throwing out everything and starting again, as there are critical existing foundations which should be leveraged to accelerate the transformation. From our experience, most enterprises tend to be around the second stage (Foundations) and third stage (Essentials).

Stages of the network security architecture maturity model



1 - Including devices, applications and data

Today enterprises are typically between stages 2 and 3, meaning there is still a significant path ahead where architectural changes and capabilities need to be build up along the way

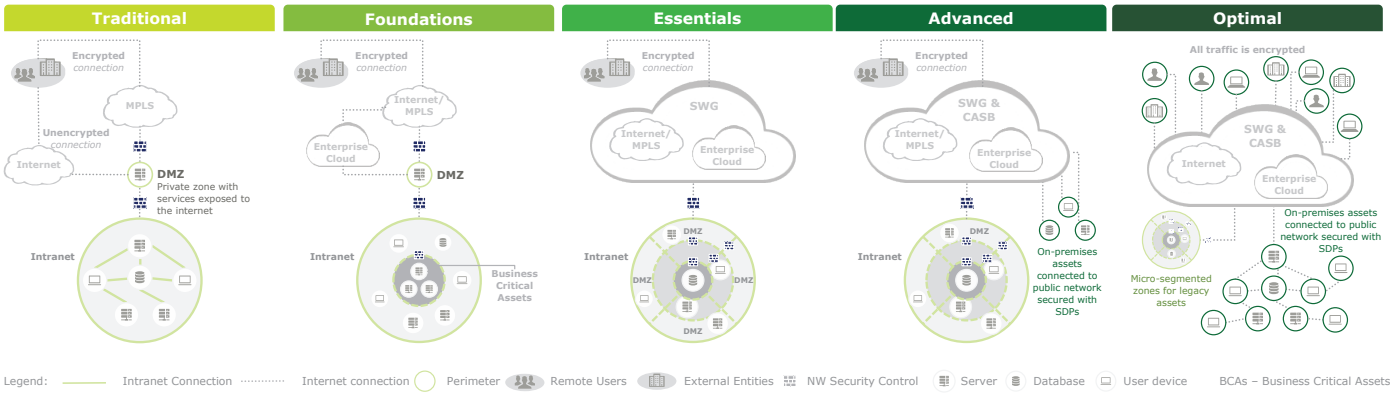
Architectural evolution

Along the journey, enterprises will aim to retire private networks moving towards public cloud based connectivity, SDPs and micro-segmentation

Today, enterprises face several challenges such as operating on various internal and external networks, managing different infrastructures and providing services in the cloud. The typical enterprise network increased in complexity but security architecture did not follow the pace. Solely relying on traditional network security strategies, such as segmentation, is no longer as effective since once an attacker penetrates a security perimeter, it is extremely difficult to ensure that the network is not compromised.

The evolution of the enterprise architecture security model should thrive towards the 'never trust, always verify' principle. Location is no longer the single critical component since the network perimeters are left behind to focus the security strategy on identity, cloud based connectivity, SDPs and micro-segmentation.

Architecture evolution



1 Traditional

- **Limited North-South protection and no East-West defence**. Open and flat LAN network or with some DMZs in place as a defence zone between intranet/internet
- **VPNs used only for critical applications** and lack of encryption on most connections
- **Static coarse-grained** controls based on IP addresses with static firewall rules and inconsistent ruleset management

2 Foundations

- **Higher ability to contain attacks** on the intranet
- **Higher operational flexibility and response times** due to core network functions virtualisation
- **Adoption of traffic profiling, URL filtering and WAFs** security controls
- **Remote access encrypted by default** based on Secure RDP, SSH, VDI (Client and Clientless), SSL and/or IPsec VPNs

3 Essentials

- WAN, LAN and DC networks **SD solutions introduction**
- **Enable remote access without VPN**, replacing it for a cloud based secure security gateway service (Secure Web Gateway, SWG)
- **Encrypted user to app traffic**
- **E2E segmentation**, based on assets and app locations within the network
- **Network security controls enhanced** with IDS/IPS, NGFWs and Anti-bots

4 Advanced

- **Cloud** first architecture with **reduction of intranet** footprint
- **Public cloud and private cloud remote access treated similarly** supported by Cloud Access Security Broker (CASB)
- **Decouple application access from the network**
- Reduced number of defence perimeters, **based on software defined perimeters (SDPs)**
- Use of **SSL inspection on all encrypted traffic**

5 Optimal

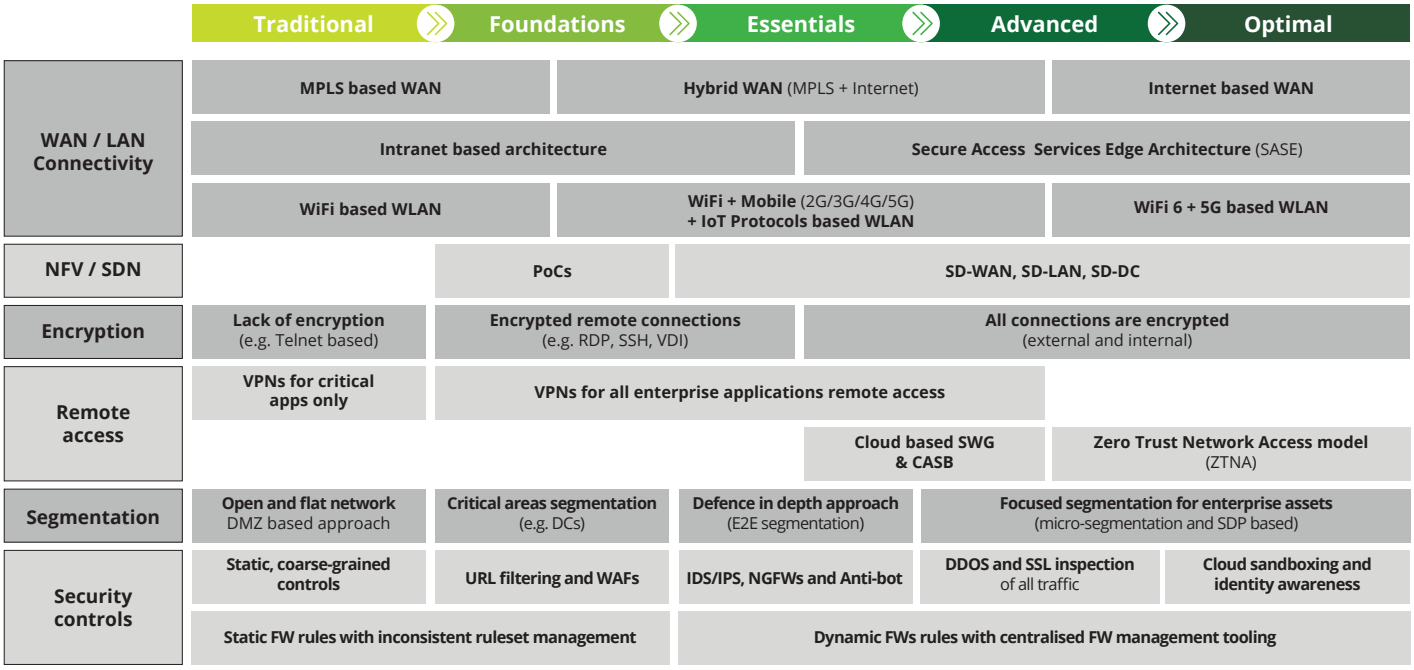
- **Intranet-less and VPN-less** approach
- **Focused micro-segmentation** for legacy assets
- **Fully automated and orchestrated** NW management
- **All traffic is encrypted** including M2M
- **Identity and behaviour as the base** for remote access permissions
- **IP addresses are never exposed** to the internet

Capabilities evolution & benefits

The evolution of security capabilities should be aligned with the architecture vision to support the security advancements for each stage of the journey

The transition to a network security optimal stage involves much more than an architecture transformation or the implementation of an off-the-shelf solution. There are required capabilities to be developed, focused on various areas of the network. None of the capabilities or solutions should be addressed in isolation. It is critical to analyse and specify the dependencies and integrations to achieve the desired outcomes.

The benefits unlocked in this evolution are visible throughout the journey, covering several areas such as enabling the modern workplace, reducing and managing risk, optimizing costs and streamlined collaboration.



Main Benefits

1 Traditional

- **Intranet as the main defense** perimeter, covering most of the users and assets
- **Segmentation** between **internal** and **external** communications

2 Foundations

- Further ability to **contain attacks** on **critical** parts of the network
- **Connectivity encrypted** by default
- Higher **operational flexibility**

3 Essentials

- **Reduced blast radius**
- **SD** capabilities **introduction**
- **Reduced costs with remote access and WAN connectivity**

4 Advanced

- Higher **simplicity** and **easier integration**
- **Automated** network security management
- **Reduced costs with FWs equipment**

5 Optimal

- **Optimized connectivity costs**
- Access management based on **real-time dynamic** contextual information
- Connections **secured** independent on the **user/device location**

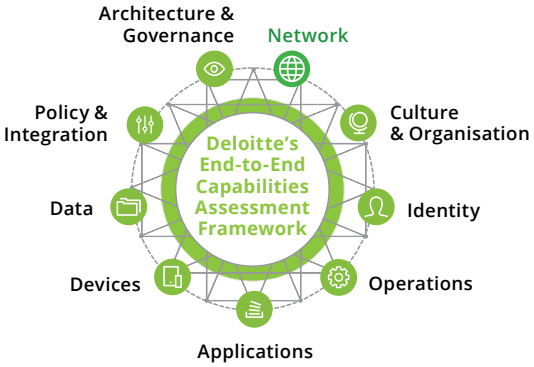
Deloitte's approach

We work closely with our clients to help them craft and shape their network security evolution journey and support their transformation efforts

Assess
as-is capability maturity

To truly unlock the benefits, a **range of capabilities** across Cyber, IT and the wider organisation **must be analysed**

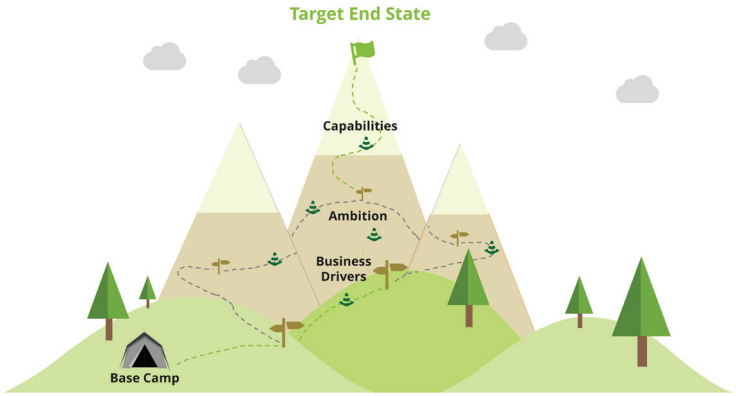
Deloitte's **framework encompasses 9 critical domains**, including Network, to perform the assessment



Define
tailored target state & roadmap

The **journey is different** depending on the **drivers, starting point** and **capabilities** you want to leverage, the **benefits** you want to gain and your **ambition** to change

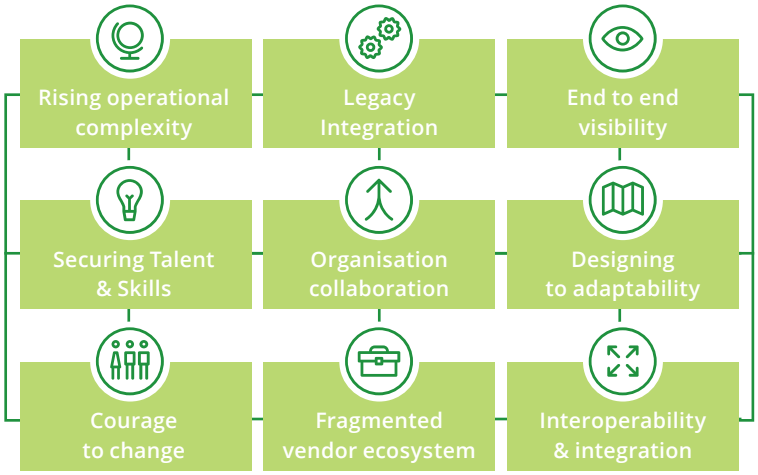
Deloitte will **help you build a pragmatic roadmap**, by prioritising the most relevant initiatives that unlock value to you sooner



Implement
effectively & overcome challenges

It is critical to ensure **operations readiness** through an **effective implementation** and **sustainable transition to BAU**

Deloitte can **support you through the journey**, anticipating and addressing common challenges **to achieve** the **target state**



Why Deloitte?

Deloitte's unique engineering and cybersecurity capabilities present the right set of skills needed to support our clients on network security transformations

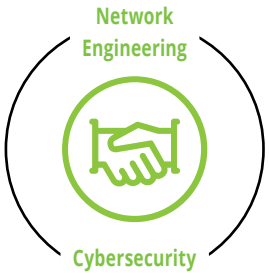
Our skills and experience

Unique fingerprint
Engineering background and **multidisciplinary teams** bridging technical expertise with strategic **consulting** skills

Network Security Experience
Worldwide proven track record of our network protection offering portfolio covering all the **lifecycle of enterprise networks**, aiming to increase security across the entire organisation

Independent Advisory
Recommend the best solution for clients working in a close **agnostic cooperation** with major **vendors and other service providers**

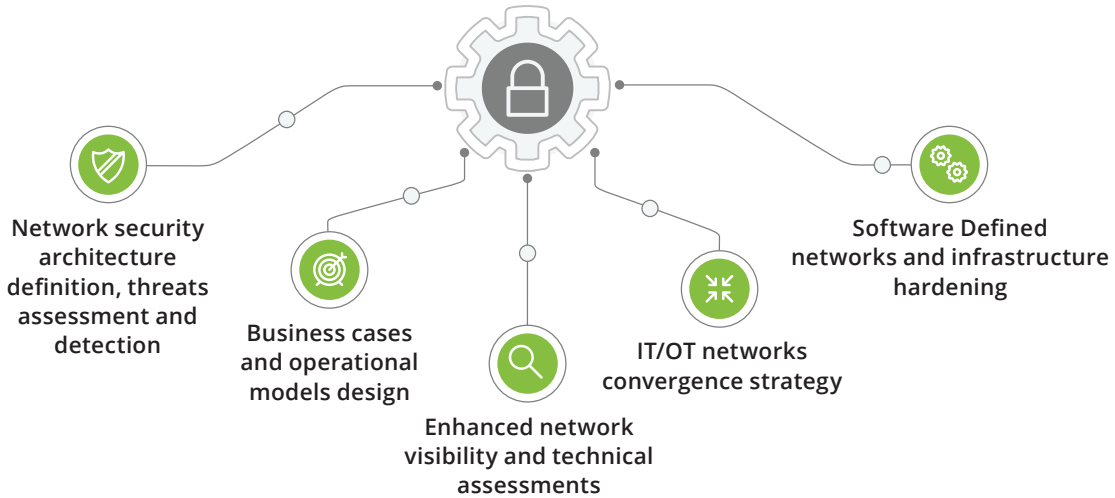
Community Presence
Active participation in worldwide reference organisations, giving more value to the telecommunications sector



Deloitte is unique in its service offerings in the **Network Engineering and Cybersecurity domains**, associating high technical expertise with **business strategic consulting skills**

We have experience, resources and tools to help organisations craft an effective network security strategy, as we specialise in running integrated transformation programs and understand the complexity of change. Deloitte designs integrated solutions that are fit-for-purpose according to the needs and business outcomes defined by our clients.

Our Network Security Portfolio



Contacts

Sponsor

Pedro Tavares
Telecom Engineering Centre of Excellence (TEE) Leader
petavares@deloitte.pt

Experts

Luís Abreu
Telecom Engineering Centre of Excellence (TEE) Partner
labreu@deloitte.pt

Vikash Laxmidas
Telecom Engineering Centre of Excellence (TEE) Manager
vlaxmidas@deloitte.pt

André Santiago
Telecom Engineering Centre of Excellence (TEE) Manager
ansantiago@deloitte.pt

José Miguel Mesquita
Telecom Engineering Centre of Excellence (TEE) Manager
jmesquita@deloitte.pt

Acknowledgements

Special thanks to whom contributed to this publication in terms of researching, providing expertise, and coordinating:
Sara Soares | Carolina Rodrigues | Ricardo Duarte | Rita Ferreira | Benedita Sobral

Deloitte.