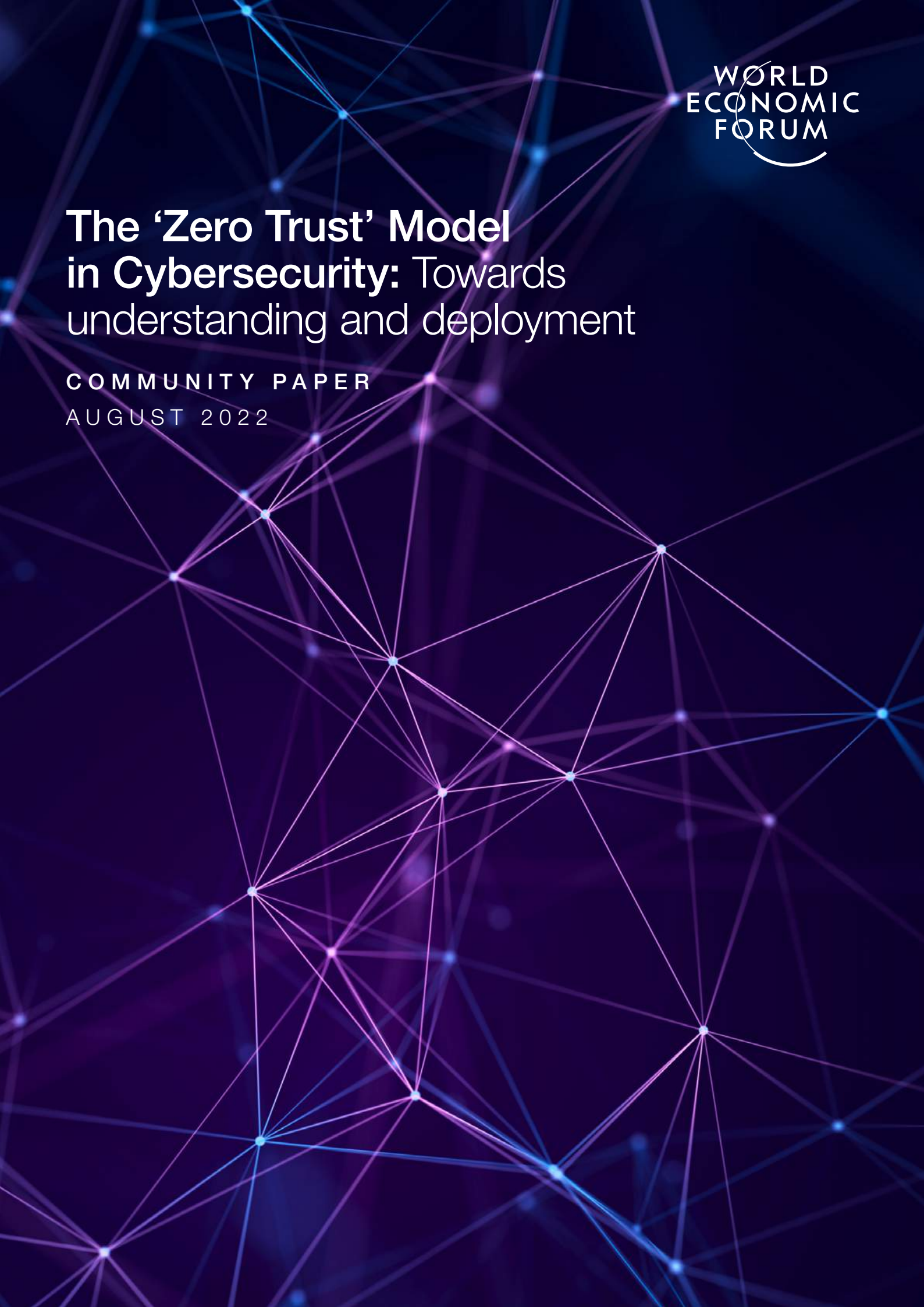


WORLD ECONOMIC FORUM

The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment

COMMUNITY PAPER

AUGUST 2022

Cover: @Olena Lishchyshyna/Gettyimages

Contents

Executive summary

In the last couple of years, “zero trust” has gained significant traction in the cybersecurity realm as a means to protect networks and increase security across organizations. In part, the growing popularity of this security model can be attributed to the shift to hybrid working practices that call for a more secure work environment whether on- or off-premises.

As organizations across industries including the oil and gas sector start to design and deploy this security concept, what zero trust is in practice is a matter of some confusion. In addition to the various overlapping and at times contradictory definitions of zero trust, the recurrent overuse of the term for marketing purposes adds to the confusion. This Community Paper aims to demystify zero trust.

In contrast to the perimeter-based security model that considers anything from inside the corporate network to be secure and trustworthy, zero trust assumes that no user or device can be inherently trusted. Threats can be both external and internal. That said, zero trust is not a silver-bullet solution to all the cybersecurity challenges within organizations.

For organizations to effectively adopt zero trust, this paper proposes a set of guiding principles:

- Establish no trust by default.
- Ensure visibility.
- Apply trust with dynamic and continuous verification.
- Use “least privilege”.
- Ensure the best possible end-user experience.

These principles, combined with a set of best practices intended to secure zero trust buy-in across the organization and to also maintain, monitor and improve the framework, can help cyber leaders ensure that change does not derange the organization’s business continuity.

While many organizations may already have some measures and technologies in place for a successful deployment of zero trust, future trends deserve attention. New technologies such as artificial intelligence and biometrics can help manage cyber risks better and contribute to the implementation of the guiding zero trust principles.

This paper therefore provides clarity on the definition, development and deployment of the zero trust model to improve cybersecurity across industries.

Introduction

Cybersecurity is a continuously evolving field as threats and risks become more advanced, sophisticated and costly for organizations across sectors. In 2021 alone, the average cost of a data breach amounted to $4.24 million.[1] The same study found that the average cost of a data breach was $1.76 million higher for organizations that did not have a mature security strategy in place.[2]

Industries such as oil and gas have faced disruptions due to malicious cyber activities. To cope better with cyber threats such as the Colonial Pipeline ransomware attack that affected the largest refined-oil pipeline in the United States of America (US), industry players are increasingly turning to the zero trust security model.

> **Many cybersecurity challenges arise with the adoption of digitalization. With the new threat landscape introduced by multi-cloud hosting, industrial Internet of Things (IIoT), mobility, remote working and other developments, trust can no longer be implicitly assumed in an internal corporate network. We look at zero trust as a comprehensive and transformative model that replaces implicit trust with explicit and continuous monitoring and verification based on the risk factors and the threat landscape, regardless of user location or used device. The collaboration effort under the zero trust workstream within the World Economic Forum's Centre for Cybersecurity is geared towards unifying the approach to zero trust.**
>
> Yousef Al Ulyan, Vice-President, Information Technology, Saudi Aramco, Saudi Arabia

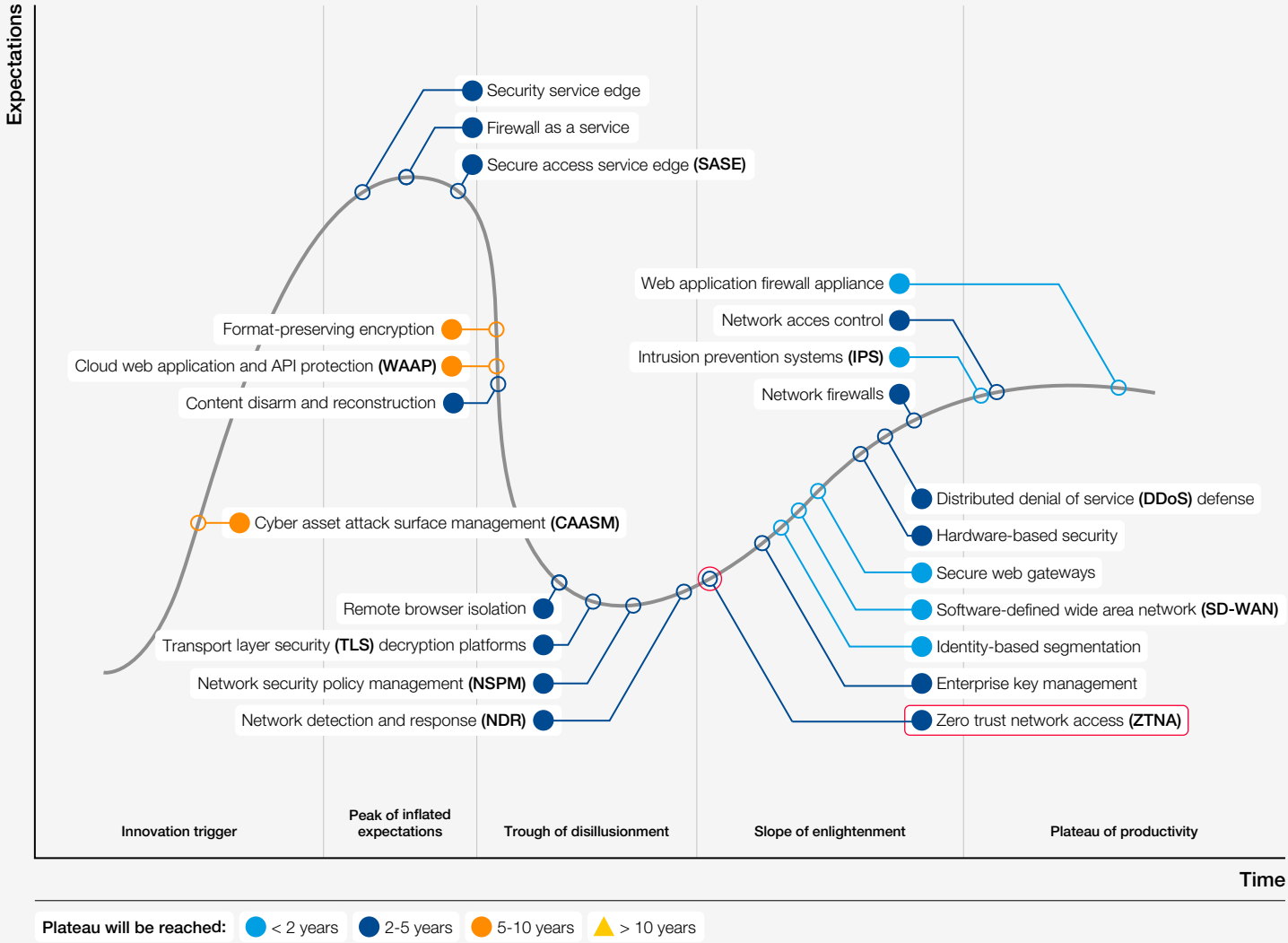
Below: @da-kuk/ Gettyimages

Why zero trust – and why now?

Although not a new concept, zero trust has become more prominent in the last couple of years for a number of reasons. First, it is a central feature of the US Presidential Executive Order 14028 focused on improving the nation`s cybersecurity posture.[3] The executive order calls on government agencies to implement zero trust as part of the steps taken to modernize approaches to cybersecurity. The increase in attention on zero trust is also, in part, a result of the massive shift to remote work as well as the growing popularity of the "bring your own device" (BYOD) practices that emphasize the need for organizations to secure their workforce and digital workplaces.

Gartner highlights this increase in interest for certain key elements of zero trust. For instance, the popularity of Zero Trust Network Access (ZTNA) increased by 230% between 2019 and 2020 and is expected to reach the so-called "plateau of productivity" characterized by wide-scale adoption and use in the next five years.[4]

FIGURE 1 **Hype cycle for network security, 2021**



Source: Gartner, Security Hype Cycle, 2021

It is therefore no surprise that more than 80% of C-suite leaders consider zero trust a top priority for their organization.[5] However, many are only just embarking on zero trust initiatives. Research suggests that 21% of surveyed organizations have some sort of zero trust architecture in place, while an additional 25% plan to adopt one in the coming 12 months.[6] The predicted growth in adoption is also supported by market value projections where the zero-trust market is expected to grow from $27.4 billion in 2022 to $60.7 billion by 2027.[7]

Below: @magann/Gettyimages

1 Decoding zero trust: Giving a meaning to the buzzword

A quick search on the internet results in a myriad of definitions of zero trust from numerous sources, including research firms, cybersecurity companies and other organizations that have begun to implement the concept. The definitions often overlap and contradict each other.

The confusion is exacerbated by the frequent overuse of the term for marketing purposes, creating the illusion that zero trust is a universal remedy to all cybersecurity issues. This uncertainty around the meaning of zero trust has, at times, made it difficult to implement zero trust initiatives.

1.1 What is not zero trust? And what is?

What is not zero trust?

- It is not a silver bullet to all the cybersecurity challenges within organizations.
- It is not a single technology, product or service that will enable companies to redefine their cybersecurity approaches and practices.
- It is not a one-time task nor a one-size-fits-all solution that can be purchased, installed and completed once and for all.

What is zero trust?

- It is a philosophy or mindset to build a defensible security model encompassing a variety of different safety measures, capabilities, best practices and technological bricks.
- It is a shift in the security approach on how to dynamically and holistically establish trust with “an unknown”, whether a human being or a machine.
- It is a principle-based and data-centric model that enforces continuous verification and visibility of trust based on risk.

Below: @monsitj/Gettyimages

For the purpose of this community paper, the definition of zero trust based on community consensus is:

“Zero trust is a principle-based model designed within a cybersecurity strategy that enforces a data-centric approach to continuously treat everything as an unknown – whether a human or a machine, to ensure trustworthy behaviour”.

While zero trust is not a turnkey cybersecurity solution, it can provide organizations with guidance on how to continuously mitigate and manage evolving risks in order to protect their digital landscape, specifically, data, networks and operational technology (OT).

Whereas certain companies may have a strong cybersecurity baseline and require only minor refinements for a successful deployment of zero trust, others may need to build new, foundational elements of security to confidently protect their assets and data.

Irrespective of the starting point, zero trust is a multi-year, multi-domain and multi-stakeholder effort that comes with its own share of benefits and challenges.

What are the benefits of zero trust for organizations?

- It helps organizations be more successful in stopping or limiting security events in contrast to the very structured but increasingly ineffective perimeter-based security models.
- It provides a more structured and risk-based approach to implementing cybersecurity within an enterprise.
- It also facilitates a greater degree of understanding in terms of availability and employment of corporate assets and resources. In this respect, it allows for better protection of data and the network.
- It allows for visibility into the corporate network to ensure that only authorized users, devices and services can access specified resources. Better situational awareness ultimately contributes to improved compliance with cybersecurity regulations and standards.
- As the workforce shifts to a hybrid working model, zero trust can allow workers to securely access the corporate network and resources irrespective of whether they are on- or off-premises.

What are the challenges of zero trust for organizations?

- It requires organizations to have a detailed inventory of applications, data assets, devices, networks, access rights, users and other resources.
- It demands that organizations have financial and non-financial resources to support the implementation of the zero-trust programme in the long run.
- It requires cyber leaders to communicate clearly to business executives why a change in the security architecture is being introduced.
- It inevitably necessitates a change of mindset and needs support from all staff throughout the organization.

Below: @Olena Lishchyshyna/Gettyimages

Repsol embraces two approaches to zero trust

Repsol has embraced zero trust with two different approaches – as a mindset and as a programme.

As a mindset: Every initiative and security requirement is thought through with the zero trust principles in mind as part of a security-by-design process.

As a programme: To reach maturity in this architecture and truly change the paradigm, Repsol recognizes that some transformational projects and a dedicated multidisciplinary team are needed. The key piece for succeeding in the programme is adequate sponsorship to drive the transformation. Senior management have to be briefed about the concept and must support the programme, while key teams from areas such as architecture, applications and infrastructure have to be highly engaged.

The organization is aware that this is a continuous journey on which it needs to adjust its action plan to the readiness of the environment and the always evolving nature of the threats.

1.2 Limitations and possibilities of zero trust in an industrial environment

In its current form, the concept of zero trust has mostly been applied within the information technology (IT) area. As the IT and OT (operational technology) systems converge across industries, keeping both secure is a challenge in the age of digitalization. Thus, the concept of zero trust must go beyond the sole focus on the IT environment to ensure that the entire organization is protected from cyber risks and threats. Even though certain zero trust practices (e.g. network segmentation and multi-factor authentication) can be adopted from the IT environment and translated into the OT context, it is important to understand that OT systems were not designed with cybersecurity in mind.

Consequentially, the full implementation of zero trust in the OT environment faces significant barriers, such as:

- The perception that production lines must keep running and security is a roadblock.
- The need to evolve the cyber capabilities of the OT workforce.
- The lack of technological readiness of the OT environment:
    1. A significant number of legacy systems in the operational space do not support modern authentication such as multi-factor authentication.
    2. Protocol support within the major industrial protocols is missing.
    3. Computational resource constraints exist in the internet of things (IoT) and IIoT devices.
    4. Identity and access management between physically and logically isolated networks is a challenge.
- The lack of precedent, with implementation examples being largely unknown.

Schneider Electric takes a principles-driven approach on zero trust and OT

Given the constraints of the OT environment, Schneider Electric is pursuing an approach that focuses on aligning ongoing and future OT security efforts towards a set of core principles, rooted in zero trust best practices.

The current and future efforts include improving authentication in the factory environment through:

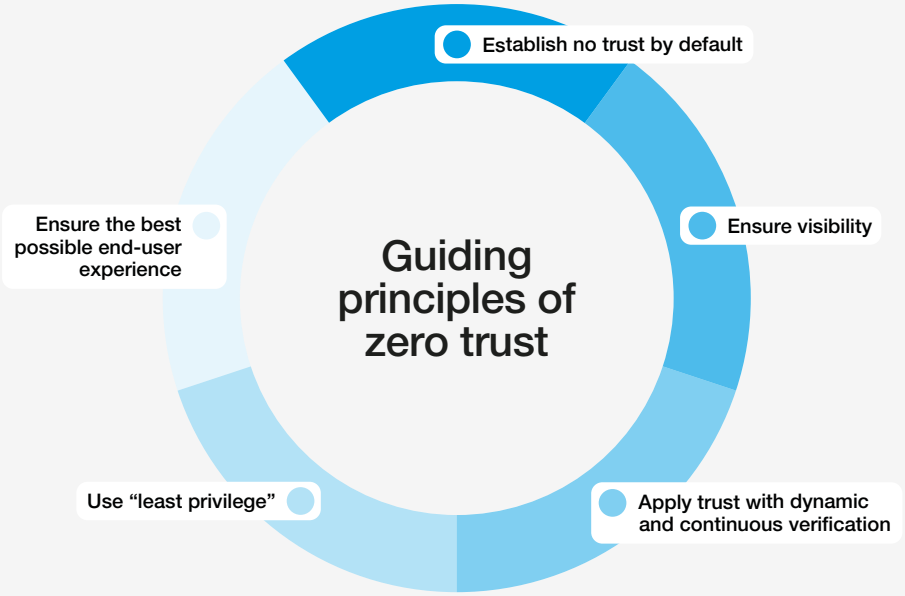
- Identity-based authentication across industrial personal computers (PCs) and human-machine interface software (HMIS).
- Role-based access control for key systems.
- Replacement of obsolete, legacy or insecure-by-design equipment where possible.
- Increased security oversight of third-party suppliers and manufacturing partners.
- Certification of control systems against IEC 62443 standards that secure the development and maintenance of industrial automation and control systems.
- Instating of systematic backup, restoration and management of all OT devices such as PCs, programmable logic controllers (PLCs) and printers.
- Education of OT actors on this upcoming change.

Over time, efforts will convert into impact since the organization is just launching this initiative.

2 Guiding principles of zero trust

"Never trust, always verify" is perhaps the most cited principle of zero trust. However, oftentimes the security model is based on a wider collection of guiding principles, some of which have been provided by the National Institute of Standards and Technology (SP 800-207) and the National Security Agency in the US.

While each organization should analyse which contextual principles it should consider according to the feasibility of their implementation, the Zero Trust action group has identified the following five as key for designing a broad approach to zero trust:



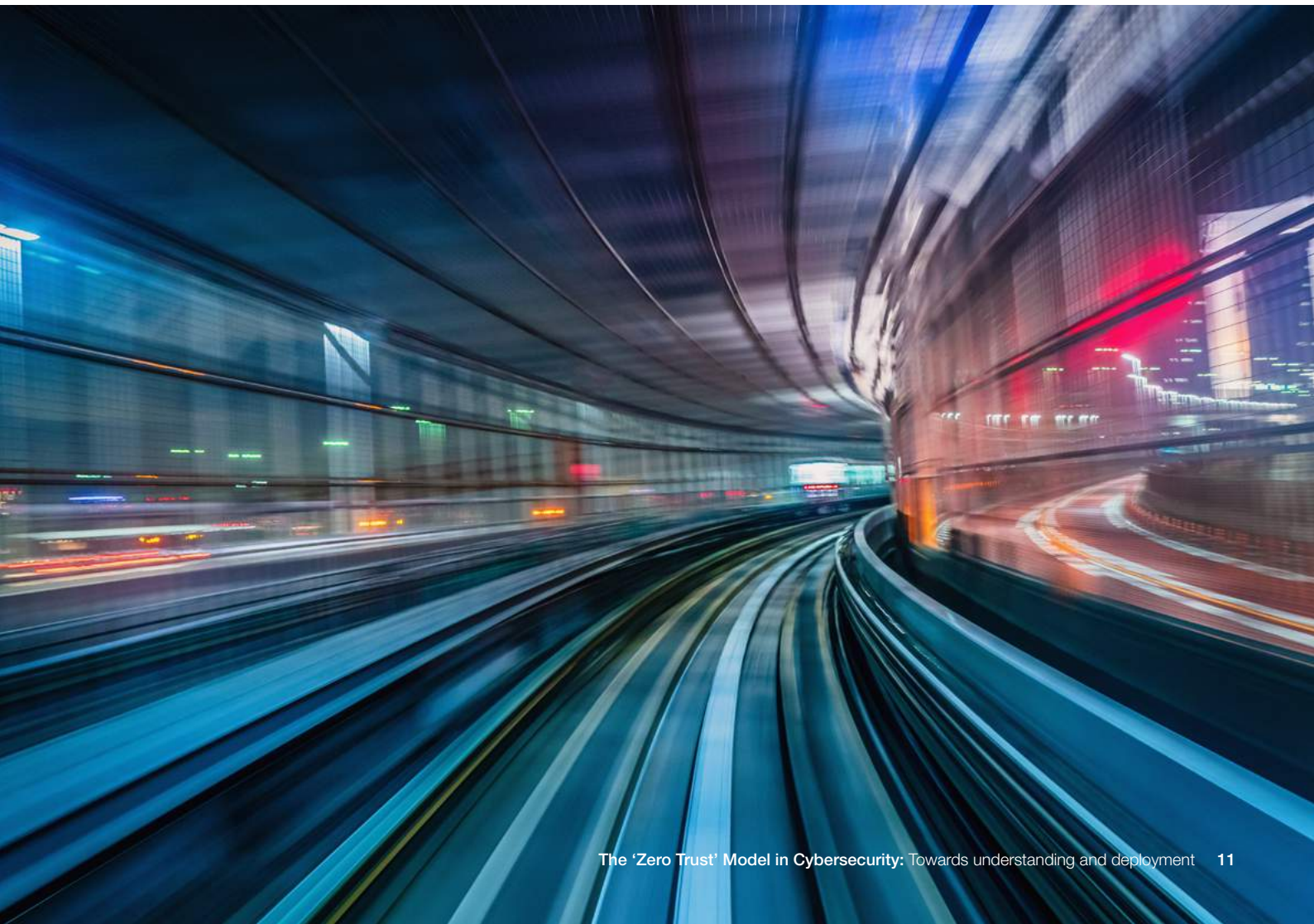
- Assuming that cyber threats can come from inside and outside the corporate network perimeter.
- Mapping the "protect surface" of the network including the "crown jewels", i.e. critical applications, data, devices, users, etc., and maintaining automated and continuous visibility into these resources.
- Continuously and dynamically verifying and validating access for all users/devices to all resources.
- Limiting user access rights to only the necessary resources depending on the role of users/devices.
- Ensuring security controls do not negatively impact end-user experience and productivity.

Below: @Mlenny/Gettyimages

3 Best practices and steps for a successful deployment of the zero-trust model

Rather than thinking of zero trust as a destination, it should be regarded as a journey that needs to be approached systematically and revisited constantly. To navigate the journey and deploy a zero-trust model successfully, the following best practices should be adopted sequentially:

- Ensuring buy-in across the organization with tangible impact.
- Understanding and mapping the “crown jewels”.
- Introducing adequate control mechanisms.
- Implementing the zero-trust model.
- Maintaining, monitoring and improving the model.



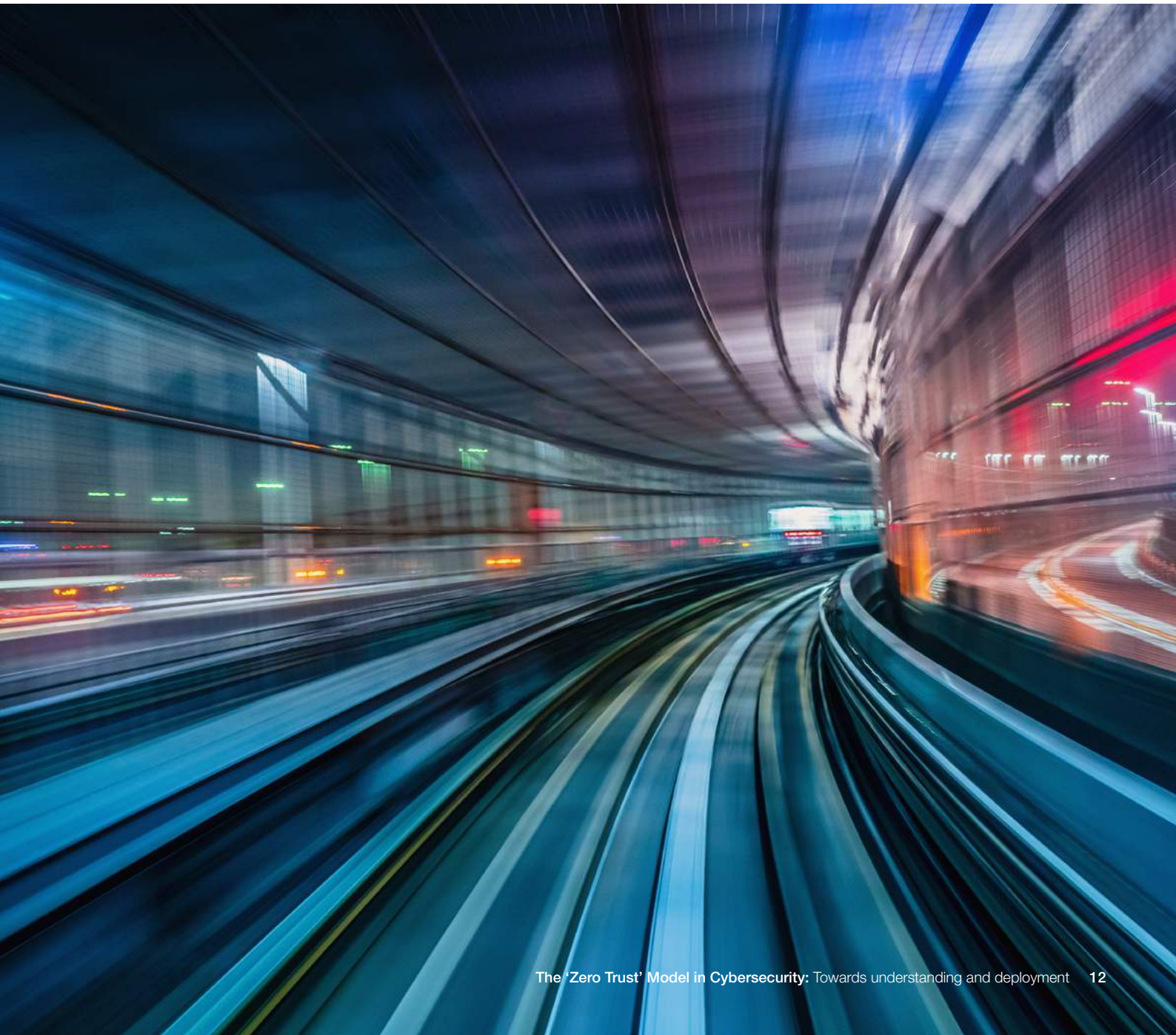
3.1 Ensuring buy-in across the organization with tangible impact

The starting point for a successful deployment of zero trust is to involve all stakeholders throughout the organization – including the leadership, IT professionals and all staff – in the development and implementation process.

Zero trust is a long-term commitment that requires both financial and non-financial resources, as well as continuous prioritization and support throughout the organization. As such, stakeholder awareness, alignment and support are key for reducing challenges and roadblocks during deployment. To ensure that all stakeholders are aware and able to participate in the zero-trust project, cyber leaders should:

- Explore the zero-trust practices already in place within their respective organizations and identify what additional capabilities the organization may need.
- Present their organization with a zero-trust strategy. The strategy should be developed as an enterprise-wide initiative with strong governance as well as clear roles and accountabilities. When presenting, cyber leaders should avoid a technology-driven discussion, and avoid a technology vendor presenting the strategy with them or on their behalf. Instead, they should focus on explaining how critical this strategy is for enterprise security.
- Anticipate that disruptive changes such as the deployment of a new security model are not always welcome and that at a group level, it may require a shift in mindset and workplace culture.

Below: @kokouu/ Gettyimages



3.2 Understanding and mapping the "crown-jewels"

Research from 2021 shows that 98% of organizations are concerned about insider threats.[8] Unlike the traditional security model that assumes that anything from outside the network perimeter cannot be trusted, zero trust recognizes that users, devices and services from inside are also a potential threat. To reduce the attack surface, the network is segmented into countless micro-perimeters, which prevent infiltrators from progressing towards the "crown-jewels". In addition, users and devices are constantly verified.

However, in order to know what to verify, cyber leaders need to clearly identify what the "crown jewels" are that they need to protect. To that end, an essential part of the shift to zero trust is understanding and mapping the valuable critical data, assets, devices (such as laptops, smartphones and IoT devices) and other resources that make up the protect surface. Cyber leaders should therefore:

- Recognize that the zero-trust approach must cover the converging IT and OT systems. OT devices should be identified and considered as an entry point into the corporate environment.
- Understand that the inventory is not static and that it needs to be constantly updated to reflect changes such as recently procured products, as well as dormant and orphaned accounts due to employee changes or movement within the company.
- Determine who needs access to what specific devices, applications and networks, and work towards gaining visibility into asset usage and data flows.

Cloudflare manages zero-trust access controls

Companies must walk the tightrope in ensuring that everyone has access to the tools and data they need, but no more than that. For IT organizations around the world, particularly, managing these access controls is a real challenge, which is exacerbated when each employee has multiple accounts across different tools in disparate environments.

Cloudfare, a company that builds security products, was in a unique position to solve this problem for both itself and its customers. It built Cloudflare Access to secure its software-as-a-service (SaaS) and internal applications with a zero-trust approach.

Securing its internal applications made employee and contractor on- and off-boarding much smoother. Now, each new employee and contractor is quickly granted rights to the applications they need.

By authenticating every packet, Access makes it possible to assign granular permissions to employees and contractors, and enables the security team to detect unusual activity on any applications. Together, more granular control and enhanced visibility enable more comprehensive management of attack surfaces.

3.3 Introducing adequate control mechanisms

On the basis of clear insights into the inventory, organizations can devise appropriate policies and security fundamentals including zero-trust principles, the structure of the zero-trust project and control mechanisms. When drawing up policies, cyber leaders should:

- Establish a clear vision on what the scope of the zero-trust strategy should be for better oversight, domain ownership and effective mitigation.
- Identify priority use cases that would address higher cyber and business risks (e.g. remote workers and branch offices).
- Define scope, domain ownership and appropriate controls, with contextual principles to be applied across the company (including in the IT and OT environments)
- Use/adopt technologies that are already available and licensed. Considering that no organization is "starting from scratch" on zero trust, existing security practices (such as multi-factor authentication) should be calibrated and retained.
- Ensure cybersecurity guidelines are observed and updated by, for instance, defining and applying guidance on how to onboard suppliers, clients and others impacted by the strategy or ensuring that access logs are logged into a centralized log database.

3.4 Implementing the zero trust model

The zero-trust model aims at serving corporate strategy and as such must be aligned with business priorities. To be done well, the transition to zero trust should be made in stages and scaled up over time. To ensure a flexible implementation approach, cyber leaders should:

- Consider deploying zero-trust technologies in smaller use cases first, ensuring the staff understands why the new security procedures are being introduced and what they consist of (e.g. what the new procedures/protocols for remote access are), and then expand across the enterprise.
- Appoint an officer (e.g. a Chief Information Security Officer, or CISO) to be responsible for overseeing and delivering the zero-trust roadmap adapted to the organization's context. Along the journey, the officer responsible should seek assistance and advice from experienced external actors who have already implemented a zero-trust model and learn from peers in the industry.

Zero trust as a fundamental security pillar for Eni

The fast-evolving cyber threat scenario requires a rapid mindset change. To this end, Eni is focusing on building the consciousness and sensibility that zero trust needs.

The foundation of its zero-trust strategy is the existing infrastructure, whose core functionality will be expanded by capitalizing on the investments already in place. The thrust will be on identity, of both users and devices, to be able to build security around this new organizational perimeter. Eni is evolving its access methodologies with modern and flexible technologies that allow for continuous risk assessment.

Since cybersecurity objectives can only be met with the broader engagement of all IT functions, brief workshops have been held to create awareness and share how this new way of thinking about security can bring less complexity and more adaptative security.

In Eni's "IT Strategic 4Y Plan", zero trust will feature as a fundamental pillar to increase the security posture, enable new business and lead technology improvements. At the same time, it is expected to increase scalability and visibility, while facilitating easier compliance with standards.

The relevance of the zero-trust approach will be shared with Eni's top management to ensure effective risk mitigation amid constantly changing threat scenarios.

3.5 Maintaining, monitoring and improving the zero trust model

As a continuous journey, the approach to zero trust needs to be evaluated and challenged constantly. To that end, cyber leaders should:

- Develop the expertise to gain insights and visibility into the global threat landscape in order to refine their zero-trust strategy to correspond to evolving risks and threats.
- Explore mechanisms for continuous improvement and adaptability, for instance with new technologies such as AI and machine learning that could help monitor the network in real time for the zero-trust environment.

Below: @blackdovfx/Gettyimages

4 Vision for the future: New technologies and zero trust

As innovation continues to transform the industrial environment from the perspective of the IT and OT environment, emerging technologies could be employed to enable novel cyber capacities and improve existing ones.

Technologies such as biometrics and artificial intelligence (AI) can play a key role in supporting some of the foundational principles of zero trust. For instance, facial, fingerprint and voice recognition could be used to identify users, verify access and detect intrusions. AI could, among other things, automate the detection of threats and abnormal behaviour in real time. In the long run, this would enable organizations to take preventive rather than reactive measures.

To avoid the hype surrounding emerging technologies, organizations should be aware of the technologies that they already have at their disposal and identify how these differ from the new ones that are supposed to accelerate the shift to zero trust.

It is also worth highlighting that a single new technology will not be responsible for the implementation of a single zero-trust principle. Rather, it will need to work in sync with other technologies to ensure that all principles of the security model are observed.

The deployment of zero trust must keep pace with new technologies and the digital transformation of the cybersecurity industry. For instance, the shift to cloud technology means that organizations store their valuable assets and data outside their perimeter, making it difficult to apply a single security control system across the entire network.

The widespread use of IoT devices is also a challenge from the point of view of zero trust – not only does a diverse range of devices performing various functions make cybersecurity standardization difficult, devices also often lack in-built security controls. Moreover, smart devices are not always recorded in the IT inventory, making it difficult to ensure their visibility in the network.

Conclusion

Going beyond the hype around zero trust and addressing the challenge of multiple interpretations, this report defines zero trust as a principle-based model designed within an existing cybersecurity strategy that enforces a data-centric approach to continuously treat everything as an unknown in order to ensure trustworthy behaviour.

As such, zero trust is a powerful model that can help enhance the cybersecurity posture of an organization. Nevertheless, to realize its full potential, it must be viewed in the context of the security practices that already exist. A good understanding of the best practices in the industry, a clear deployment plan based on a clearly defined set of principles applicable to the current state of the organization, and a future-looking vision where technology has a key role to play are essential for a successful implementation of zero trust.

Rather than being seen as a destination, the zero trust transition should be seen as a journey, with all employees having a role to play in embracing, adopting and constantly challenging the model for an enhanced security posture.

Contributors

Lead authors

Natasa Perucica
Research and Analysis Specialist, Centre for Cybersecurity, World Economic Forum

Elisabeth Williamson
Project Fellow, Centre for Cybersecurity, World Economic Forum

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

Akshay Joshi
Head of Industry and Partnerships, Centre for Cybersecurity, World Economic Forum

Community

The World Economic Forum would like to extend its sincere thanks to the cyber leaders who contributed their valuable insights and perspectives to this Community Paper. The following individuals led in-depth discussions as part of the Zero Trust: Towards a Unified Approach action group to address some of the most pressing questions around the security model.

Mansur Abilkasimov, Schneider Electric, France
Abdullah Almutlak, Saudi Aramco, Saudi Arabia
Zarul Annuar Hamzah, PETRONAS, Malaysia
Danilo Arduini, Eni, Italy
Mazen Baragaba, Saudi Aramco, Saudi Arabia
Molly Cinnamon, Cloudflare, US
David Corral Morgadez, Repsol, Spain
Alessandro Curio, Eni, Italy
Tim Dalhöfer, Institute for Security and Safety, Germany
Octavio Herrera, Occidental, US
Sigmund Kristiansen, Aker BP, Norway
Suzanne Lemieux, American Petroleum Institute, US
Sean Morgan, Palo Alto Networks, US
Rishi Muchalla, Check Point Software Technologies, US
Rahayu Ramli, PETRONAS, Malaysia
Kadeon Reid, Baker Hughes, US
Arno Sevinga, Royal Vopak, Netherlands
Amr Sherbeeni, Saudi Aramco, Saudi Arabia
Joe Sullivan, Cloudflare, US
Quint Van Deman, Amazon Web Services, US
Swantje Westpfahl, Institute for Security and Safety, Germany
Olivera Zatezalo, Suncor Energy, Canada

The World Economic Forum also wishes to acknowledge the contribution of John Kindervag, SVP, Cybersecurity Strategy at ON2IT to the action group's activities.

Endnotes

1. Cost of a Data Breach Report 2021", IBM, https://www.ibm.com/security/data-breach, accessed 10 June 2022.
2. Ibid.
3. "Executive Order on Improving the Nation's Cybersecurity", The White House, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed 10 June 2022).
4. Colombus, Louise, "Zero trust and UES lead Gartner's 2021 Hype Cycle for Endpoint Security", Cloud Security Alliance, 2021, https://venturebeat.com/2021/10/06/zero-trust-and-ues-lead-gartners-2021-hype-cycle-for-endpoint-security/ (accessed 10 June 2022).
5. "CISO Perspectives and Progress in Deploying Zero Trust", 2022, Cloud Security Alliance, https://cloudsecurityalliance.org/artifacts/ciso-perspectives-and-progress-in-deploying-zero-trust/ (accessed 10 June 2022).
6. "Security Priorities Study", Foundry, https://f.hubspotusercontent40.net/hubfs/1624046/R-ES_SecurityPriorities_02.17.22.pdf?__hstc=241435677.021a956aac98635ec886839d69807d86.1649914372803.1649914372803.1649914372803.1&__hssc=241435677.1.1650007992063&__hsfp=3133718954&hsCtaTracking=a1cce2be-68d1-4dcf-92ac-a961522206bf%7C082b65d7-e59b-4e2f-b691-27d1b24914f6 (accessed 10 June 2022)
7. "Zero Trust Security Market worth $60.7 billion by 2027", Market and Markets, 2022, https://www.marketsandmarkets.com/PressReleases/zero-trust-security.asp (accessed 27 June 2022).
8. "Insider Threat Report", 2021, GURUCUL, https://gurucul.com/2021-insider-threat-report (accessed 27 June).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org