Cigref

Towards a Zero Trust philosophy

A break in continuity for application security

February 2022

Towards a Zero Trust philosophy

A break in continuity for application security

Intellectual property rights

All Cigref publications are made freely available to the general public but remain protected by the applicable laws on intellectual property.

EDITORIAL

During the first meeting of our working group, we wondered about the relevance of the concept and the implementation of "Zero Trust": was it a buzz word or a reality?

The concept of Zero Trust, often summed up by the injunction: "*never trust, always verify*", is based on the idea that the identity of users must always be verified before giving them access to applications, for all access requests.

Zero Trust introduces in-depth, real-time management of identities and accesses, generalised to all information system (IS) assets. The model transforms network logic (internal/external) into dynamic application logic.

As many security practices pre-existed, this concept introduces a major break in the holistic, systemic and real-time nature of the subject. With this concept of Zero Trust, IT departments must **deal with a break in continuity**, in the same way as the cloud, for example, in its relationship with IT production.

The work of this working group and the examinations we conducted have enabled us to better understand this issue and to form certain convictions that we share in this report. The working group was made up of players with a wide variety of profiles: infrastructure, application, security, architecture, etc. This testifies to a structural subject that is fairly transversal to the entire IT department.

We approached participants from the following companies:

- Akamai, as an edge platform and tools provider;
- Forrester, to define the principles of Zero Trust and their adoption in business;
- Microsoft, because of their global positioning on identity and access management tools;
- Wavestone, IT strategy and cybersecurity consulting firm.

We also benefited from feedback from a company in the banking sector regarding their microsegmentation project to illustrate this type of complex project in a large organisation.

Finally, this working group also highlighted the role of the Internet as the main network for the company of tomorrow. Thus, Internet access and infrastructure providers will have to meet the specific needs of businesses. This echoes the current developments of the cloud and also of 5G (see Cigref report). Moreover, this trend is an additional sign, if needed, of the importance of the regulatory and geopolitical challenges of Internet governance.

Thierry Borgel,

Leader of the working group

ACKNOWLEDGEMENTS

We would like to thank **Thierry BORGEL, CIO of the ICADE group,** who steered this study, as well as all those who participated and contributed to this Cigref working group:

Wilfrid ALLEMBRAND - SOCOTEC

Patrick ARMUSIEAUX - MSA

Mathieu ARQUES - AIR FRANCE KLM

Christophe BANDINI - ESSILOR INTERNATIONAL

Laurent BENDAVID - DASSAULT AVIATION

Laurent BONNET - AIR FRANCE KLM

Philippe BOUET - AMUNDI

Sonia BOUROUH - AXA

Philippe BRON - MINISTRY OF THE INTERIOR

Fabrice BRU - GROUPEMENT DES MOUSQUETAIRES

Francis CAUVÉ - BANQUE DE FRANCE

David CHALLUT - GEODIS INTERSERVICES

Cédric CHEVREL – MATMUT

Claudio CIMELLI, MIN. OF NATIONAL EDUCATION

Alexandre CHOPIN - BNP PARIBAS

Christophe DEJOIE – LEGRAND

Massimo DEVINCENTI - AXA

Marie DUVAL SOYEZ - ENEDIS

Olivier GUILLEMINOT - NEXANS

Saïd KHALDOUNE - AUCHAN

Jean-Christophe LALANNE - AIR FRANCE KLM

Jean-Louis LARGERON - SNCF

Sylvain LAUMAILLE - SODEXO

Pascal MARY - HAGER GROUP

Thierry MOINEAU - BNP PARIBAS

Pierre NARBEY, POLE EMPLOI

Philippe NETZER-JOLY - ARKEMA

Pascal PELONI - BIOMÉRIEUX

Julien RAUX - BNP PARIBAS

Alexandre RAYNAUD - AIR FRANCE KLM

Frédéric RIGA - GETLINK

Manuel ROCHA - ENEDIS

Franck ROUSSET - MINISTERE DES ARMEES

Philippe SOLINI - AIR FRANCE KLM

Marc-Michel STACK - BNP PARIBAS

Julien STANKIEWICZ - AMUNDI

Vincent TASSY - AIR FRANCE KLM

Grégoire TURCAT - GROUPE SAVENCIA

Nicolas VERMUSEAU - KEOLIS

We would also like to thank all of the participants whose input significantly guided our thinking (in alphabetical order):

- Gérôme BILLOIS, Partner, Cybersecurity & Digital Trust, WAVESTONE
- Fabio COSTA, Senior Solutions Security & Edge Technology Engineer, AKAMAI
- Jean-Yves GRASSET, Chief Security Advisor, and Patrice TROUSSET, MICROSOFT
- Paul McKAY, Senior Analyst Serving Security & Risk Professionals, FORRESTER

This document was written by Clara MORLIÈRE, senior project manager at Cigref, with the contribution of Thierry BORGEL and the Cigref permanent team.

TABLE OF CONTENTS

EDITORIAL 1

ACKNOWLEDGEMENTS 2

TABLE OF CONTENTS 3

TABLE OF FIGURES 4

OVERVIEW 5

1. INTRODUCTION TO THE CONCEPT 6

1.1 A state of mind, almost a philosophy 7

1.2 A context conducive to the development of the Zero Trust concept 9

1.1.1. The cyber threat, internal network insecurity and so-called supply chain cyberattacks 9

1.1.2. The fragmentation of the IS and the migration of applications to the cloud 9

1.1.3. Employee mobility, with widespread adoption of remote working 10

1.1.4. Technological developments and the increase in digital projects 10

2. WHO ACCESSES WHAT, WHY, HOW, AND FROM WHERE? 11

2.1 Conditional access through identity authentication 11

2.2 Internet as a corporate network 12

3. A TRANSVERSAL AND PROGRESSIVE PATH OF TRANSFORMATION 14

3.1 Adoption at the level of French and European companies 14

3.2 Combination of multiple projects 15

3.3 Cross-functional approach 16

3.4 Focus on microsegmentation 17

4. IMPLEMENTATION CHALLENGES 20

4.1 Security culture evolution 20

4.2 Hybrid architecture management 21

4.3 Coordination of IT activities and teams 21

4.4 Emergence of a solutions market 22

5. SUCCESS FACTORS AND RECOMMENDATIONS 23

5.1 Break in continuity 23

5.2 Working group recommendations 24

6. CONCLUSION AND OUTLOOKS 26

APPENDICES 27

SOME EXAMPLES OF THE ZERO TRUST APPROACH 28

Akamai: a step-by-step approach 28

Microsoft: towards Internet Only 30

MATURITY PRINCIPLES AND LEVELS 31
Zero Trust architecture design principles by The National Cyber Security Centre 31
Zero Trust architecture key questions by US department of defence 31
Microsoft's Zero Trust Maturity Model Assessment 32

BIBLIOGRAPHY 33

TABLE OF FIGURES

FIGURE 1: MICROSOFT CONDITIONAL ACCESS 12
FIGURE 2: IMPLEMENTATION OF THE CONCEPT OF ZERO TRUST BY FORRESTER 2021 17
FIGURE 3: USE CASES FOR MICROSEGMENTATION 19

OVERVIEW

Zero Trust is a development of IT security principles and a philosophy that organisations will need to adopt to strengthen the security of their digital assets. This concept requires an in-depth transformation approach, and a multi-year deployment roadmap; it is therefore not a question of applying a single solution or a single good practice but of implementing a programme including multiple projects in several areas: infrastructure, network, security, applications, cloud, etc.

This thought pattern or state of mind describes an approach where equipment and users are considered untrustworthy until proven otherwise. Thus, the concept of Zero Trust is based on the belief that trust must be established and verified with rules: "*Never assume, always verify, give minimal privilege, monitor and respond quickly".*

The current context shows the limits of the traditional model of the fortified castle – consisting in protecting the internal IS in a perimeter fashion (equivalent to ramparts and moats) – and promotes the emergence and development of the concept of Zero Trust. Among the contextual phenomena identified, we converged on the exponential increase in the cyber threat, the explosion of the IS associated with migration to the cloud, the mobility of employees and service providers, as well as technological developments and the increase in digital projects.

Today, most Cigref organisations are studying the concept, are beginning to understand it and are taking ownership of it. Some members are already "doing Zero Trust" without knowing it, but most are still only at the beginning of the process, and are seeking to identify the opportunities that they would have to integrate it into their security strategy and policy.

The participants of the Cigref working group formulated a global questioning to summarise all of the elements to be checked in the implementation of a Zero Trust project: "who accesses what, why, how, and from where?". The "who" represents users and services, the "what" represents applications, whether in the cloud or not, the "why" concerns the reasons for the access, based on specified rules, the "how" refers to the network used, either the corporate network or, increasingly, the Internet network, and finally the "from where" refers to the user's terminal equipment and its location, all of which must comply with the GDPR and other applicable regulations.

The working group has thus made it possible to understand that the subject is structural, complex, transversal, and part of the long term. As of today, in each of the projects under consideration, organisations can begin to integrate the principles of Zero Trust, regardless of whether around the workstation, user awareness, the identity repository, access techniques and the network. They must also question their ability to use the Internet as their majority corporate network and the impacts for their infrastructure and security model.

The Zero Trust model must be added to the good security practices to be implemented by all organisations. In a dedicated opinion on the subject, the ANSSI (French National Agency for the Security of Information Systems) recommends a certain vigilance in the deployment of solutions to avoid installation or configuration errors. With this approach, the intrinsic vulnerabilities of applications are indeed still problematic. Organisations therefore need to rely on applications that are secure by design and secure by operation.

To prepare for the future, this involves laying the foundations of the requirements for future networks now, notably 5G, identity and access management modes, in particular by anticipating passwordless approaches, and other possible organisational and technological breaks in the continuity of this philosophy.

1. INTRODUCTION TO THE CONCEPT

After a short retrospective of the appearance of the term and the notion, we will introduce the concept of Zero Trust and its main principles and will explain the main reasons at the origin of the favourable context in which we find ourselves for the emergence and development of this concept.

In 2004, at the Jericho Forum, "Network Access Control" was developed, initiating the beginnings of Zero Trust. Then in 2010, John Kindervag, a former Forrester employee, developed the more marketing term of Zero Trust based on his observations[1]. He observes, in those years, that people and companies "anthropomorphise" IT and its environments, applying the concept of trust to it. Organisations defined – and sometimes still define – their security policy according to the location of the systems: if they were located inside the so-called internal perimeter of the company's network, then they could be trusted. Nevertheless, it was already noticed that the networks could be hijacked and hacked by means of the information allowing access to this internal perimeter. This is why John Kindervag proposes the concept of Zero Trust according to which no user, interface or network device, whether internal or external to the network, must be trusted.

A structuring white paper, "Zero Trust Networks", was then published in 2017, by Evan Gilman and Doug Barth through O'Reilly media. It is recommended reading for anyone wishing to find out more about it[2]. It shows how to create strong authentication, authorisation, and encryption, while helping to provide corporate networks with compartmentalised access and improved operational agility.

At the end of 2018, the American National Institute of Standards and Technology (NIST) published the report "NIST (SP) 800-207, Zero Trust Architecture" and in August 2020, it published the proposed definition of Zero Trust based on a framework with 5 pillars: Identify, Protect, Detect, Respond, Recover, to address the challenges and opportunities of implementing the so-called Zero Trust architecture across US government networks. However, the NIST framework does not yet fully integrate all of the elements of Zero Trust. According to some participants, they will probably be added soon.

Today, the concept of Zero Trust must still be linked to major norms, certifications, and standards for it to be truly recognised and adopted much more widely worldwide.

Following the recent attacks by SolarWinds and Microsoft Exchange on American companies and administrations, President Biden incidentally issued an executive order obliging the upgrade of American federal agencies to a Zero Trust architecture in 180 days.

In the United States, the concept therefore started to spread from these agencies to the public sector, then has gradually been adopted by the private sector over the past 3 or 4 years. After the United States, awareness of the concept grew in Europe, starting with the United Kingdom and the Netherlands, and later in Germany and France. The UK National Cybersecurity Centre published its Zero Trust Principles at the end of 2020. The ENISA (European Union Agency for Cybersecurity) should start looking at it, to mirror what has been done in the United States.

Among the most advanced players, Google has made the concept operational with the BeyondCorp[3] but took more than 10 years to set it up, linking it to the renewal of their IS and Beyond Trust Corporate

[1] *Build Security Into Your Network's DNA: The* Zero Trust *Network Architecture*: Forrester_zero_trust_DNA.pdf
[2] Zero Trust *Networks*, O'Reilly, 2017, https://www.oreilly.com/library/view/zero-trust-networks/9781491962183, an extract is available for free: https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html
[3] Zero Trust Enterprise Security with BeyondCorp, Google Cloud, https://cloud.google.com/beyondcorp/#researchPapers

has only been on the market for about a year. Google's vision is not shared by everyone. Google itself indicates in its white papers that each company or player has its own vision depending on its maturity.

1.1 A STATE OF MIND, ALMOST A PHILOSOPHY

Zero Trust is a philosophy, a model of thought and not a tool or a single good practice. It materialises through multiple projects in several areas of expertise: infrastructure, network, security, applications, etc.

Players often choose to use the term philosophy to refer to the concept, to emphasise that it is a state of mind to adopt and not a solution to buy. It is a philosophy that describes an approach where equipment and users are considered untrustworthy until proven otherwise.

The concept of Zero Trust represents principles, a transformation approach, deployment, technical tools, etc. Thus, the concept of Zero Trust is based on the belief that trust must be established and verified with rules:

> **"*Never assume, always verify, give minimal privilege, monitor and respond quickly*".**

Zero Trust introduces a change in vision of security. Previously, security management was more focused on network security ("the network never lies"). This view has evolved over the past few years. Identity has become an important part of system access management. The two approaches took time to converge, to find themselves today within the concept of Zero Trust.

Every attempt to access systems is monitored as if it came from an untrusted, hostile network. One of the objectives of Zero Trust is to harmonise the security levels between the external environments and the internal network, with the lowest level. The change of paradigm on the transition from a network logic to an application logic is very structuring, implying a change in the global approach.

Zero Trust thus aims to bring the perimeter of control of access rules closer to the workstation and to directly secure the connection of equipment, so as not to depend on the network or the external ecosystem. The concept of defence in depth is important in linking trusted people to untrusted people. Zero Trust goes further, without any guarantee of trust beforehand.

Five fundamental principles of the concept of Zero Trust:

- **The network is always assumed to be "hostile".**
- **External and internal threats exist on the network at all times.**
- **Network location is not sufficient to decide trust in a network.**
- **Every device, user and network flow is authenticated and authorised.**
- **Access policies must be dynamic and calculated from as many data sources as possible.**

It should be noted that each company and market player emphasises a part of the concept of Zero Trust. A few quotes from the working group's interventions that show these different aspects:

> ***"Instead of connecting users to networks providing access to applications, users are connected to applications".*** **Akamai**

"Zero Trust is not about not trusting anything, but about adopting a smarter way of trusting". **Microsoft**

"Zero Trust is a dynamic trust model that allows global control of access to applications according to rules established according to users and their environment". **Wavestone**

Zero Trust Principles as presented by Forrester

1. Never trust and verify all identities and data access requests before authorising them. Never assume trust.
2. Make decisions based on transaction risk, never authorise access based solely on network location: who is making the request, who is usually concerned, who makes the decision to authorise or not.
3. Record and monitor as much information as possible.
4. Use network microsegmentation to contain security threats.
5. Automate and orchestrate security tasks to improve execution consistency. This applies to all areas of IT (especially highly distributed IT architectures), automating and orchestrating as much as possible helps deliver data and improve initiative maturity.

Zero Trust Principles as presented by Microsoft

1. All data sources and processing services are considered as resources.
2. All communications are secure **regardless of network location**.
3. Individual access to corporate resources is granted on a session basis.
4. Access to resources is determined by a **dynamic policy** – including the observable state of **the identity of the customer, application or service and requesting asset** – and may include other behavioural and environmental attributes.
5. The company monitors and measures the integrity and security of all owned and associated assets.
6. All of the **resource authentications and authorisations** are dynamic and **strictly enforced before access is authorised.**
7. The company collects **as much information as possible about the current status of assets, network infrastructure and communications,** and uses them to **improve its security posture.**

1.2 A CONTEXT CONDUCIVE TO THE DEVELOPMENT OF THE ZERO TRUST CONCEPT

The current context favours the emergence and development of the concept of Zero Trust: the exponential increase in the cyber threat, the explosion of the IS associated with migration to the cloud, as well as technological developments and the increase in digital projects. These transformations are amplified by the need for employee mobility, in particular due to remote working, and the scope of the IS for service providers.

The traditional model of the fortified castle has reached its limits for several reasons: the implementation of advanced security systems to reinforce the moat between the castle and the outside is becoming very complex and inefficient; the use of more and more equipment is a new requirement, and we are reaching the limits of the capacities of the VPN (virtual private network). This model consisted in protecting the internal IS at the perimeter (equivalent to ramparts and moats), the interior of the castle represents the IS with the applications but also the users, and the workstations. The IS is delimited by the ramparts of the castle to which are added the moats as an additional system of protection. The old peripheral model is thus increasingly complex to maintain in the current context.

1.1.1. The cyber threat, internal network insecurity and so-called supply chain cyberattacks

As announced by the ANSSI in its annual report, the number of cyberattacks increased fourfold in 2020. Many of these so-called supply chain attacks use the access of IS users, whether employees or service providers, to enter the internal network and to exploit vulnerabilities in information systems.

Today, we are seeing a proliferation of internal network compromises. Every day, new incidents occur and new perimeters are compromised. All organisations report experiencing at least one insider attack in a year. 30% of data breaches come from internal players, who are not necessarily malicious but victims (through phishing in particular to recover identifiers). We have therefore come to the conclusion that the "interior" of the castle is no longer trustworthy. The company can no longer consider its internal network as reliable.

1.1.2. The fragmentation of the IS and the migration of applications to the cloud

The majority of systems are increasingly fragmented with an IS that is more open to the ecosystem, with multiple interdependencies between systems. The applications are no longer within the company's internal information system, but gradually in the cloud, or even in several clouds. It would therefore be necessary to create new perimeter protections to secure the new applications, which introduces multiple complexities on a large scale.

Indeed, on-premises applications were hosted in the company's datacentres. Their number is gradually decreasing today in favour of their migration to the cloud.

Moreover, ten years ago, IS users were only company employees. Today, the scope of users is very extensive (employees, subcontractors, partners, customers, etc.).

In addition, all of the devices used were previously managed by the company, but Bring Your Own Device (BYOD) policies are growing and therefore diversifying the provenance of the systems used by employees.

Previously, about 80% of network traffic was on the internal network. Now, for some companies, 70% to 80% of flows go out to the Internet directly. The situation is therefore now reversed: flow inspection

has changed with SaaS applications (notably messaging and collaborative tools). You need to be able to manage increasingly large external (Internet) flows.

1.1.3. Employee mobility, with widespread adoption of remote working

The lockdown decreed due to the Covid-19 crisis by several national governments has forced companies to provide access to their applications outside the internal network or via VPNs. Users could be anywhere, without the required security environment. This brutal upheaval, the date of which, 17 March 2020, that will remain in all memories, forced most companies to change the paradigm for the protection of their information systems and the securing of accesses.

This remote working situation created security problems, in particular to access applications that were not necessarily designed to be accessible from outside the corporate network. Some companies have reached or even exceeded the limits of their VPN, in particular the bandwidth limit.

In this context, many organisations are beginning to adapt their operations to remote work and their interest in the concept of Zero Trust has increased in order to establish a bond of trust between the user and the machine.

Okta's "State of Zero Trust Security 2021" report gives some figures: more than three quarters of companies worldwide (78%) say that the understanding of a necessary implementation of the approach has increased, and nearly 90% are currently working on a Zero Trust initiative, compared to only 41% a year ago. This shift in interest in the concept is therefore very significant.

1.1.4. Technological developments and the increase in digital projects

Moreover, the digital transformation of companies is accelerating, bringing about fundamental changes in the way companies operate. We are witnessing an accelerated growth of digital projects. The weeks of delay to open network streams are no longer tenable.

In addition, new business requirements, such as faster mergers and acquisitions (M&A) processes, require adapting to more sustained rhythms and having the tools to deal with them.

2. WHO ACCESSES WHAT, WHY, HOW, AND FROM WHERE?

The concept of Zero Trust consists in verifying the request for access to each application by managing the identity of the user and their context, regardless of the legitimacy of their network connection.

Networked devices, such as laptops, should not be trusted "by default", even if they are connected to the corporate LAN and even if they have been previously verified. The identity repository must be able to verify the trust of users and devices (authentication) and what they can access (authorisation). Each access request requires authentication and authorisation.

The working group has therefore formulated a global questioning to summarise all of the elements to be verified: **who accesses what, why, how, and from where?**

Thus, we can define each of the questions of this global questioning:

- **Who**: users and services (later resources);
- **What**: applications, whether in the cloud or not;
- **Why**: reason for access, based on specified rules;
- **How**: business networks, and increasingly the Internet network;
- **From where**: equipment and its location.

Compliance with the GDPR and other regulations in force is a transversal requirement for these questions.

However, we find that while the questions are simple to formulate, these elements are often complex to define in the case of large organisations that must manage multiple profiles, hundreds of applications and hybrid infrastructures.

2.1 CONDITIONAL ACCESS THROUGH IDENTITY AUTHENTICATION

The Zero Trust security model assumes that every user and every device is considered untrusted until proof of trust is collected. Identity management is carried out according to the user's profile and the conditional access to the applications in relation to the rules set by the company.

Identity is therefore the most important point in order to control access to any type of application. The user's context is taken into account in the access decision. It is therefore necessary to control, via signal feedback from the identity repository, with a real-time risk assessment:

- The device (new terminal, integrated into the fleet, with security patches, etc.);
- The user;
- Its location (normal or not, double connection);
- The application (restriction according to its criticality).

Even before the validation of the identity of a user, the verification of the profile of an equipment ensures that it meets certain security criteria. For example: having a client certificate, running the latest version of the operating system, being protected by a password or strong authentication, or having an appropriate and operational endpoint detection and response solution.

The model must ensure that all resources (applications, servers) are securely accessed, regardless of their location or the hosting model employed. Zero Trust requires the adoption of a **"least privilege" policy,** which consists in granting only the necessary rights **resource access**, and of **"deny by default"**

when executing the access to applications. As part of privileged access management, it is possible to increase privileges for a limited time to perform a clearly identified task.

Thanks to the new tools, the company can configure different reactions from applications depending on the level of trust. For example, if the user is using a computer provided by the company, then there are more functionalities available with a client application installed on the workstation than with access via a browser.

This is why each application must be classified according to its use and its criticality in the face of the evolving risks experienced by the organisation. The company sets the rules for conditional access to applications in relation to this classification.

Microsoft Conditional Access

Microsoft first addressed the concept of Zero Trust through identity management and control before dealing with the "network" part of Zero Trust. Zero Trust is based on 6 pillars according to the company: identity, device, data, applications, infrastructures, network. In 2019, when their Zero Trust Architecture report was published[4], conditional access control added a new brick to managing identity and access in real time. Microsoft offers a model broken down by technological brick:

1. Explicitly verify identity (Azure Active Directory)
2. Implement Least Privilege Access (Conditional Access)
3. Assume Breach

The challenge for Microsoft is to capture, within its solutions, the greatest number of relevant signals in order to have the right user qualification information. This makes it possible to make better decisions on access authorisation and to detect compromises and abnormal behaviour in a preventive way, thanks to artificial intelligence models.

Microsoft has also developed and adopted another principle called "Assume Breach". This represents the ability to accept compromise and to be able to react. This involves adopting a security approach with an omnipresent risk of breach to be organised in order to react better.

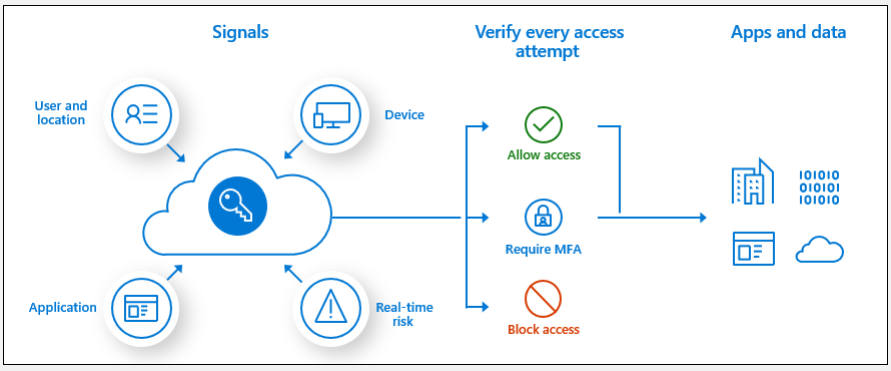


Figure 1: Microsoft Conditional Access

2.2 INTERNET AS A CORPORATE NETWORK

Strengthening the outer perimeter of the network is no longer enough. Network perimeter security is no longer effective in keeping businesses secure in a world of increasingly sophisticated threats.

[4] Zero Trust strategy—what good looks like, https://www.microsoft.com/security/blog/2019/11/11/zero-trust-strategy-what-good-looks-like/

The goal of the new security models is that users can be anywhere and can access any application, whether working remotely, on the road or in the office, and this also applies to access by partners, customers, subcontractors, etc.

Thus, **this security model considers the network to be compromised and hostile** and treats all applications as if they were connected to the Internet. The concept of Zero Trust changes the network paradigm of the company: it is a design of architecture "without perimeter" which makes it possible to reduce the exposure to the risks.

Network access must integrate many security components and prerequisites such as accessibility, availability, flexibility of the IS architecture (future of inter-application exchanges, terms of service exposure). This requires traffic inspection and logging to identify malicious activity. In a project to overhaul the LAN of its datacentre, the creation of new network zones makes it possible to integrate a logic of exposure of services and opening of port bundles rather than a flow-by-flow approach. Some solutions on the market use detection techniques (signature, signatureless and machine learning) to identify and block known or suspicious threats and deal with them with the appropriate tools.

The culmination of the Zero Trust philosophy is to consider the Internet network as the company's own network. The transition to "Internet Only" requires mastering Internet controls (speed, performance, control). The idea of changing the network by going only through the Internet can nevertheless frighten organisations due to a lack of control capacity.

In this reflection, new players appear such as Akamai, intervening during the working group, to propose an edge platform for Zero Trust to control the level of redundancy and ensure good performance. It goes beyond a VPN infrastructure. It should be noted that this type of platform must make it possible to manage countries with specific regulations on the Internet. This may gradually replace the use of MPLS (Multiprotocol Label Switching). This is why this kind of platform needs a global presence.

Zero Trust is often linked to other concepts such as "SASE" (Secure Access Service Edge). The two concepts start from the same observations on the current context, but differ in their proposal. SASE can be presented as a "perimeter cloud approach" while Zero Trust is going to be a "non-perimeter cloud approach". Zero Trust considers that it is necessary to disregard the network and the place where the user is located, favouring the most direct connection with the Internet which carries all flows.

One of the starting assumptions of SASE, developed by the firm Gartner, is that all systems will migrate to the cloud. SASE is the convergence of the network market (SD-WAN in particular) and network security services, which materialises in the form of a cloud service. The company will then use its network to join that of the cloud provider SASE using several solutions or even use the supplier's SD-WAN network, geographically distributed[5].

[5] Le SASE: un concept pour le long terme - L'informaticien, 2021, https://www.linformaticien.com/dossiers/58722-le-sase-un-concept-pour-le-long-terme.html (in French)

3. A TRANSVERSAL AND PROGRESSIVE PATH OF TRANSFORMATION

The approach to Zero Trust is a transversal and structural path of transformation that requires a global vision of enterprise architecture. Achieving a good level of maturity in Zero Trust is estimated at within 5 years, or even 10 years, depending on the companies and their current level of maturity.

Today, most Cigref organisations are studying, beginning to understand and adopting the concept. Some members are already "doing Zero Trust" without knowing it, but most are still only at the beginning of the process, and are seeking to identify the opportunities and interest in integrating it into their security strategy and policy. Few have already established a coherent global vision. It should be noted that no company in the world has already "completed its journey" towards Zero Trust. Only Google and Microsoft can possibly be considered as organisations that have reached the highest levels of maturity.

Adoption of the Zero Trust concept is **presented as accessible for organisations with a significant historical IS** if the process is carried out very gradually – which is important to consider for companies that are members of Cigref.

The comparison with a staircase makes it possible to show that, even if there are a large number of steps to climb to achieve the implementation of the Zero Trust concept, each step is achievable and effective and it is possible to measure a real reinforcement of the security at each level.

Finally, it is essential to understand that the Zero Trust model is in addition to the good security practices to be implemented by all organisations (in particular the effective management of vulnerabilities). The ANSSI recommends great vigilance[6] in the deployment to avoid installation or configuration errors, which would contribute to a greater vulnerability of the systems. Managers need to be aware of the appropriation time needed to avoid the feeling of false security.

3.1 ADOPTION AT THE LEVEL OF FRENCH AND EUROPEAN COMPANIES

Internationally, the majority of organisations are between 5 and 10% maturity according to Forrester. Maturity really depends on the sector context: the telecommunications sector was among the first to adopt the Zero Trust approach, the banking sector being more mature with a level of 20 to 25%.

Wavestone, which intervened during the work of our working group, evaluated a panel of its customers, mainly companies with a historical and international IS. The firm finds that:

- 5% maintain the "fortified castle" model, in particular sectors, with strong business challenges;
- 20% who have a defence in depth model, have also adopted the "airport" model, the objective of which is to further secure internal resources, especially sensitive ones, based on the security model of an airport: a hall accessible to everyone, and sensitive and secure areas to access aircraft and the tarmac.
- 70% are studying how to develop this model to move towards Zero Trust;
- 5% have started the first initiatives and projects, and are beginning their implementation.

However, it is difficult to say whether a company "is" Zero Trust or not. Even within the same company, there are several speeds of Zero Trust. You can do Zero Trust on new cloud environments more easily than on-premise.

[6] The ANSSI's scientific opinion on the model Zero Trust, April 2021, https://www.ssi.gouv.fr/uploads/2021/04/anssi-avis_scientifiques_et_techniques-modele_zero_trust.pdf (in French)

We can cite a few initiatives currently being developed in certain sectors of activity such as the banking sector, energy, transport and the media:

- Deployment of Conditional Access to resources in the cloud or for remote users;
- Study of microsegmentation and first deployments;
- Definition of an open network architecture;
- Development of a security model based on Zero Trust.

However, few large companies have begun more global reflections in order to completely redefine their security model and to apply Zero Trust in the security projects.

The 3 pillars of Zero Trust by Wavestone

1. **Know your environment**

It is necessary to have specific rights and identity repositories, and to "inject" the Zero Trust touch and the behavioural dimension into them in order to allow the differentiation of rights according to the levels of trust – determined elsewhere. In the future, the resources will also have an identity that will have to be managed with rights. It is not realistic to apply conditional access to IT resources (in the event of patching non-compliance for example) but there may be business operational impacts. The tool called the "Policy Decision Point" makes it possible to develop a confidence algorithm and define the access rights to such and such an application according to the level of trust.

2. **Adjust trust dynamically**

The change lies in the administration of "just-in-time" access thanks to an automated IS, in which there is no longer any administrator at all, or only temporary administrators, via a dedicated process (possible on new Microsoft environments). The "Policy Enforcement Point" tool serves as a watchdog for access algorithms.

3. **Automate reactions**

Finally, it is necessary to automate as much as possible the detection and reaction to incidents, in particular by deploying machine learning, especially on IaaS or PaaS environments.

3.2 COMBINATION OF MULTIPLE PROJECTS

The roadmap towards the implementation of Zero Trust is long in large companies with many projects to be carried out successively and in parallel, in particular tooling and change management.

Effective Zero Trust strategies leverage a mix of existing technologies and approaches, such as Multi-Factor Authentication (MFA), Identity and Access Management (IAM), Privileged Access Management (PAM) and network microsegmentation. Projects also include the inventory of systems, classification of applications, documents, data, installation of Zero Trust agents for applications, etc.

Typical roadmaps to Zero Trust often first start with securing identity and access with IAM programs. If identity and access management has reached a good level of maturity, then it is possible to start doing Zero Trust more holistically across the corporate network. The organisation then develops a coherent vision for the different layers of the IS and the end-to-end approach.

The basic bricks according to Akamai

Zero Trust is a transformation process rather than a "package" of solutions to be installed overnight. Akamai recommends several steps:

1. Start with specific issues or easy user groups (e.g. purely web applications).

2. Implement the new model alongside the VPN, without replacing it overnight, then start by eliminating the VPN for selected groups of users.
3. Create the conditions so that there are promoters of these changes: distribute internal promotion documents and ensure that users are interested or even enthusiastic.
4. Expand the number of applications and users gradually.
5. Automate the discovery of apps and their inclusion (discover apps to complete the mapping).
6. Implement levels of control gradually:
   - Identity and role
   - Check the adequacy between the device and the criticality of the app
   - Behavioural controls.

The 3 key projects of Zero Trust by Wavestone

Wavestone offers three major projects to meet the challenges of Zero Trust:

- **Identity and Access Management (IAM)**

Identity becomes key to any system: an identity for both resources and users. The most important thing is not to assign the same rights according to the level of trust, while taking into account the complexity of introducing too many trust categories.

- **From VPN to Zero Trust Network Access**

This is the replacement of the VPN by Zero Trust Network Access integrating a study of the conformity of the equipment. The objective is to make it possible to offer the same experience to the user regardless of whether the latter is on the premises or on the move without having the same requirements and rights (MFA, different access, performance of certain functions).

- **Cloud Security Monitoring**

The objective is the monitoring of events and the conformity of the infrastructure. There is, particularly among large accounts, and more generally, a difference in treatment between the detection of conformity and the compliance with infrastructure, architecture and security rules. In cloud environments, a misconfiguration can lead to a security incident, with greater consequences. However, there are automation tools in the cloud to monitor this compliance with the rules on a permanent basis (automatic reaction), unlike the annual verification by audit in the case of the historical IS.

3.3 CROSS-FUNCTIONAL APPROACH

The multi-dimensional aspect of Zero Trust requires significant cross-functionality within the organisation. Currently, several programs already tend to link teams, the Zero Trust will reinforce this phenomenon. Authentication, identity or the network are not just infrastructure, security or application issues: it is a common ambition of the IT department. The responsibilities of the teams can then evolve and be redefined, particularly in the context of microsegmentation, which must be prepared with a coherent and collective discourse, integrated at the highest level.

The 4 areas of implementation according to Forrester

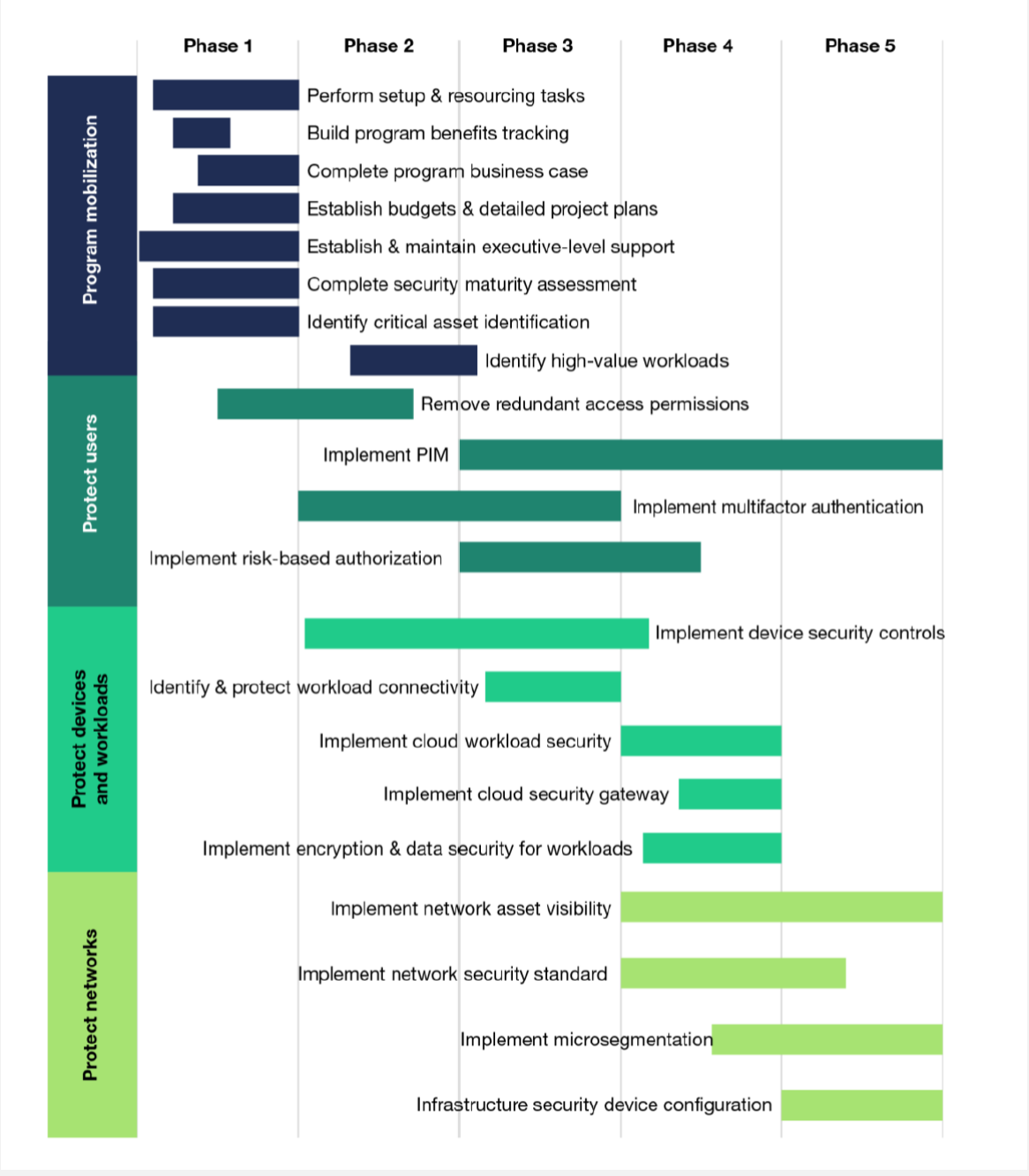


Figure 2: Implementation of the concept of Zero Trust by Forrester 2021

3.4 FOCUS ON MICROSEGMENTATION

The microsegmentation of a network consists in managing the flow control at the level of each server and not via perimeter firewalls which filter the exchanges towards zones of the network (DMZ). The DMZ, demilitarised zone, is a sub-network separated from the local network and isolated from it and from the Internet (or from another network) by a firewall. The principle of microsegmentation is to use firewalls at the most elementary level possible – for example, at the level of the native OS of the servers in order to protect them individually in an *ad hoc* way.

Historically, application filtering is performed by firewalls. In a synthetic way, it concerns centralised equipment which makes it possible to authorise or filter the types of communication on a network or a sub-network. This equipment makes it possible to segment the networks. However, if an attack flow has passed through the firewall, then there is no longer any limit to the propagation of viruses and other attack vectors inside the network.

The advantage of operating a firewall at the finest level is to define a rule that will be specific to the server to protect it from its entire ecosystem, external or close to the datacentre. Nevertheless, local firewalls are relatively expensive and, for large organisations, the quantity required makes it difficult to implement on each of the servers.

Microsegmentation is a new security paradigm. It is an important step towards Zero Trust, not necessarily the first, but it is effective when implemented well. The principle of microsegmentation that is in line with Zero Trust is to close all of the flows and to open only the flows essential to the operation of the server or the application.

Microsegmentation helps limit the number of flow openings to a minimum, which is in line with the Zero Trust philosophy. The first benefit makes it possible to simplify the understanding of flows in real time and to benefit from an accurate functional representation.

Application flows can be modelled via labels allowing the abstraction of technical parameters. Labelling makes it possible to define rules on functional criteria of the App (application) type and no longer on technical criteria of the IP type, to share them and have them inherit between servers labelled in the same way. We are moving from the IP world to the world of Apps.

This approach, however, requires rigorous management that should not be overlooked, but allows several improvements to be made, particularly in terms of:

- compliance checks on exchanged flows,
- improving security by closing open flows,
- knowledge of the server park and mastery of the company's IT asset repository.

FEEDBACK

NETWORK MICROSEGMENTATION PROJECT

A company in the banking sector presented a microsegmentation project with a market solution in order to unclog its corporate network. This organisation adopts Zero Trust as an opportunity to solve current network issues.

The Business case is based primarily on operational simplification over time. The cost of implementing microsegmentation is favourable compared to the investment in firewall boxes. The difference between the maintenance costs of firewalls and those of software maintenance, at an equivalent run, is favourable. This represents a very significant operational gain once the solution is well implemented.

Although the observation on the problems represented by the VLAN is shared, the IT department benefited from strong sponsorship from management in order to defend the approach in the face of certain resistance and preferences for other proposed choices. To get the operational teams on board, we had to show concrete use cases that provide relevant functionalities and uses.

The company worked on 3 specific use cases:

- **New application:**
  Cross-functional rules make it possible to operate various servers, if the rules are pre-implemented, the labelled server inherits the rules. Two servers with the same labels inherit the same rules.
- **Major update of an OS version:**
  The servers will fulfil the same functionalities, put the same labels and thus the same rules, which makes the update more automated.
- **New infrastructure service, change of tool to perform backups:**
  You can easily, in a few minutes, implement a rule on all of the selected servers.

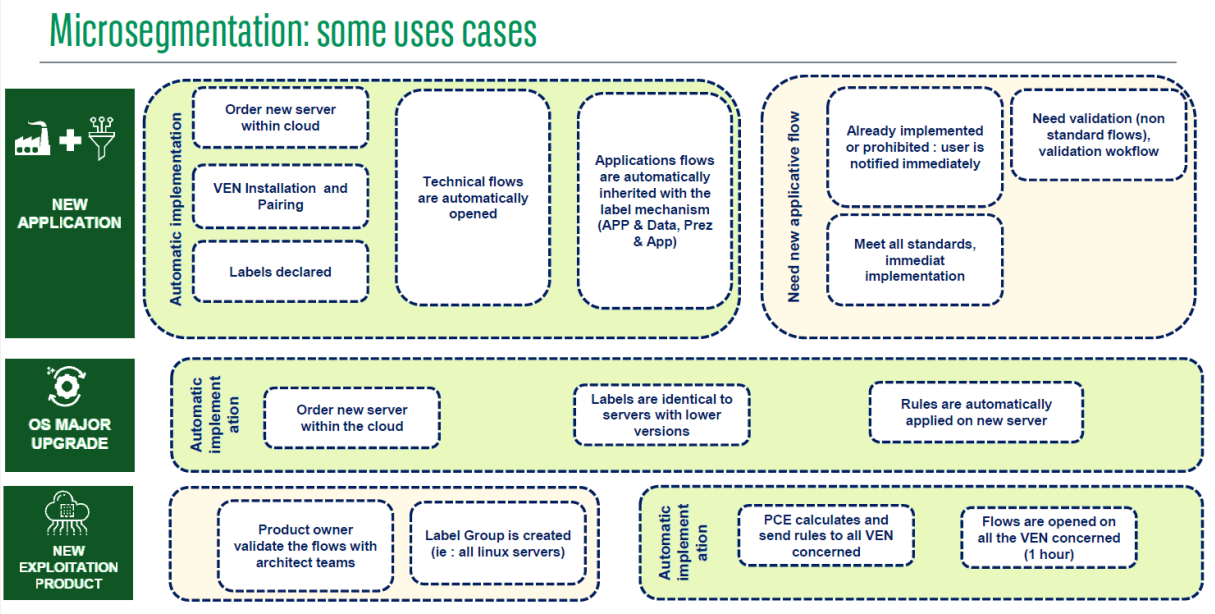


Figure 3: Use cases for microsegmentation

4. IMPLEMENTATION CHALLENGES

According to the previously cited Okta study on the state of the art of Zero Trust, the biggest challenges for European companies in adopting a Zero Trust infrastructure are cost issues (26%), technology gaps (22%), stakeholder buy-in (19%), and awareness of solutions (15%).

Within the Cigref working group, what mainly emerged was the need for a change of mindset to include Zero Trust in all current reflections on the evolution of the company's IS.

Zero Trust is an evolution of architectural models with a core decision making the link between identities, data, applications. The approach must be global, coherent and integrated into a complex architecture with coordination of the teams around this common objective.

Moreover, the market is emerging, it is still finding its way and does not yet provide all of the solutions and services to address the different aspects of the security model. As Zero Trust is a multidimensional strategy, there is no single product to cover everything, but rather a portfolio of solutions that are currently being developed. The Zero Trust philosophy is much broader than a solution.

However, it seems that certain regulations do not allow Zero Trust to be fully implemented on legacy and/or business applications, for example due to certain PASSI (Information Systems Security Audit Service Provider) activities.

4.1 SECURITY CULTURE EVOLUTION

The challenge for IT departments today is to demystify the concept, to identify the added value of Zero Trust for the user, for the IT department, for security management, and to see if this can simplify other processes.

It is not necessary to be "over-equipped" with solutions. Technology makes it possible to detect behaviour, but the main thing is to know how to educate, train and raise awareness of employees and partners, explaining the threats and benefits. The challenge is to develop the state of mind of employees towards the philosophy of Zero Trust: to raise awareness of the need, to accept further identification, to systematise reflexes, to allow the right to make mistakes, but to demand strong responsiveness in the event of a problem. Testing users is also necessary via fake phishing attacks.

For better adhesion, the solutions used must be simple and practical, integrate the best practices of UX design in order to attract users and simplify their user experience (no more VPN - easier nomadism - reduce the use of passwords - web app). Good practices can also come from the private sphere and in particular from banks for strong authentication techniques.

Thus, it is necessary to make sure that employees are provided with a lot of information that at the same time is practical, informative, stimulating and to combine it with mandatory training on good Zero Trust practices and increasingly strict security policies to be respected. The Zero Trust approach will affect all users employed outside the IT department, and the organisation must aim to encompass all populations.

4.2 HYBRID ARCHITECTURE MANAGEMENT

In most modern business environments, corporate networks consist of many interconnected, cloud-based segments (services and infrastructure, connections to remote and mobile environments) with more and more connections to non-conventional equipment such as IoT.

Organisations with a significant historical IS will not be able to become 100% Zero Trust in the short or medium term. This is due to the fact that these historical systems will not be able to be compatible to meet the challenges of Zero Trust. Organisations may also choose not to adapt these systems for strategic reasons. This approach also depends a lot on the choice of migration to the cloud.

As part of migrating to the cloud, many organisations are implementing security control over the data between users and the cloud. The use of Zero Trust makes it possible to add a checkpoint to learn more about the use of cloud services (and the flow of data). For existing IS environments, organisations must adopt a risk-based judgement to migrate to cloud services and prioritise high-risk applications (see Cigref report Strategies for migrating IT to cloud computing).

Several difficulties arise during the implementation. It is necessary to manage, during the transition period, several systems at the same time, and the complexity induced by this transition. In addition, several techniques must be mastered, including automation, integration of controls and orchestration of infrastructures.

There are few Zero Trust projects on industrial environments (OT). There is a security gap between IT and OT, the latter having availability or real-time requirements that reinforce this gap. It is likely that the next industrial network protocols will be compatible with the Zero Trust concept. This compatibility of the concept would be particularly interesting for securing fleets of connected objects on any type of network. But there is still a long way to go.

4.3 COORDINATION OF IT ACTIVITIES AND TEAMS

In this type of approach, the IT department must form multidisciplinary teams to acculturate and make the project understood, and in particular dissociate the technical and application teams.

Greater team coordination is necessary with impacts on the network and security businesses. We must also anticipate a reconfiguration of responsibilities. During the project phase, explaining the use cases requires a lot of education and moving away from dogmas for the rules avoids long technical discussions that are not very useful.

As part of the reorganisation of certain activities, companies are experiencing some resistance from teams. For example, microsegmentation brings the responsibility for controlling flows between applications back to the application teams who will be able to implement one by one all of the rules that make it possible to operate the applications. Leaving responsibility to another team or, conversely, taking responsibility can cause tension. However, in the event of a problem, when responsibility is better defined, there is a real gain in terms of incidentology (ability to trace and understand the incident).

On the application development side, we must also think about simplifying the developer experience, in particular by providing tools that help the latter to secure their work and give them confidence in the level of security of the interfaces with which they will exchange. There is a real stake in the quality of the internal code.

4.4 EMERGENCE OF A SOLUTIONS MARKET

Over the last 2 to 3 years, the market has started to offer dedicated services to meet the challenges of Zero Trust. In this context, several players are positioning themselves, in particular telecommunications service providers, consulting service providers and software publishers.

As the concept of Zero Trust is based on already known principles, but pushing them much further to meet the philosophy, publishers are tending to give their legacy products or solutions a Zero Trust touch. The term "Zero Trust" is thus often used in marketing, in the same way as that of artificial intelligence for the field of data. Many present their vision in theory, but implementation in large historical groups is difficult to understand and achieve.

The market is changing rapidly but is not yet mature in a number of areas. No publisher can claim they cover all layers, but some cover multiple layers. There are important issues of compatibility, interoperability, reversibility of offers. As in other fields, the difficulty is to compare the offers on sometimes very different criteria.

Today, suppliers with the broadest offerings and portfolios include Microsoft, Google, Palo Alto Networks, and Cisco. Some publishers are investing in the evolution of networks, others are focusing on a portfolio around identity and access (IAM), others on security. Microsoft, which we received in the working group, summarised in a graphic all of the tools that it offers (see Appendix).

Zero Trust solutions most often offer tools that are aimed at the employee population because it is larger and is located within the scope of direct action of the organisation, so the solutions are easier to implement and more profitable. Then, the organisation can consider the customer population. The hardest part is applying Zero Trust to the partner population, because organisations do not have a holistic view of the players in the supply chain.

In addition, special attention must be paid to regulations. Zero Trust solutions, as well as their implementations, must comply with the General Data Protection Regulation (GDPR), with a point of vigilance in terms of identity control and the use of these solutions.

The adoption of SASE will also require the use of several solutions such as the Secure Web Gateway (SWG), the Cloud Access Security Broker (CASB), the Firewall as a service, which may be useful in the case of large companies that will mix approaches. Zero Trust can act "like a cement" around the CASB. Indeed, a number of solutions are integrated, and it is necessary to use conditional access to access them. For CASBs, this means less functionality.

It is therefore necessary to have a good understanding of what each of the solutions offers so as not to create too much redundancy.

In addition, organisations will develop their thinking in terms of digital trust and controlling their dependencies. They will need to determine their need in this context and what they can do through Zero "+Epsilon" Trust.

5. SUCCESS FACTORS AND RECOMMENDATIONS

5.1 BREAK IN CONTINUITY

All of the principles of Zero Trust are based on good practices that pre-existed, which are becoming widespread and systematic. The Zero Trust approach does not contradict the conventional principles of digital security. What changes is the fact that they apply to all systems, to the entire company.

However, some turning points have been identified with respect to previous approaches:

- The Zero Trust model leads to real-time dynamic access and identity management.
- This implies a generalisation to the entire IS with a telling example: while multi-factor authentication was reserved for certain critical applications or populations, it is becoming the systematic standard.
- The company must carry out a transformation of the network logic, with a gradual decommissioning of the LAN to move towards "Internet First", and finally achieve "Internet Only" (or similar, in parallel with the VPN initially).

	Without Zero Trust principles	**With Zero Trust principles**
ASSIGNMENT OF TRUST	Default in internal network	On proof
IDENTITY	Manual and fixed	Dynamic
AUTHENTICATION	Passwords	Multi-factor, Biometrics, One Time Password (OTP) devices
NETWORK	Internal network	Internet First network then Internet Only network
SECURITY	Perimeter	Non-perimeter

This comparative table is obviously not exhaustive. Each company interprets **Zero Trust in its own way, which can impact these items to a greater or lesser extent or even lead to other breaks.**

The maturity scales given in the appendix can be useful for understanding the path to follow.

5.2 WORKING GROUP RECOMMENDATIONS

The first step is to **fully understand all of the issues of Zero Trust** and the state of mind that it represents within the IT department, before being able to address it in the organisation. This is necessary so as not to imagine that it would simply be necessary to integrate new solutions to become Zero Trust. It is first and foremost a security model.

From the moment we have properly grasped the model, it involves **integrating this philosophy into the reflection of any new IS project.** The projects launched today are gradually contributing to the implementation of the long and cross-functional approach of Zero Trust. Today, each digital project must respond to business challenges, be part of the company's overall strategy, and improve knowledge of the systems, but in the same way it must make it possible to strengthen business security and resilience. Thus, the IT department can choose to add the need to be part of a Zero Trust roadmap in the project arbitration criteria.

In order to be able to see the organisation's evolution towards Zero Trust in the medium term, the working group proposes **setting up a "Zero Trust Project"** or "Zero Trust Compliant" label within IT departments to identify projects that integrate the Zero Trust roadmap or that could integrate it today or later, in progressive developments. This system makes it possible to notch the progress of the strategy. The most important is to **proceed gradually.**

The Zero Trust strategy cannot be completely dissociated from the migration programme to the public or private cloud if the company chooses to adopt the cloud (see Cigref report[7]). These two projects are inevitably dependent, since the cloud brings new security challenges but also new interesting possibilities very much related to Zero Trust.

Integrating the Zero Trust philosophy into projects also means integrating it into applications. Preparation is needed to **design applications compatible with Zero Trust solutions**, in terms of identity management, network, etc. The objective is thus to dry up the flow of problems for the architectures of tomorrow.

Since the Zero Trust approach is transversal to all IT departments, the entities must **organise themselves to allow a multidisciplinary dialogue**. This is particularly necessary in order to bring together the various teams that will be impacted by the change in model and to anticipate the shifting of certain responsibilities.

[7] Strategies for migrating IT to cloud computing: a strategic adventure for enterprise - Cigref 2021 https://www.cigref.fr/strategies-for-migrating-it-to-cloud-computing-a-strategic-adventure-for-enterprise

Akamai's advice based on their feedback

It is always a good time to start deploying Zero Trust, as the available agile solutions make it easier to adapt to different contexts.

Start with web applications: this is more transparent and simpler.

Start with certain applications or populations.

Microsegmentation: it is important, but it must be implemented. Do not use microsegmentation with traditional firewalls because this is complex and expensive. Indeed, traditional firewalls are not designed for the operational management of so many filtering rules.

Automate as much as possible: it is difficult to draw up a reliable inventory of the applications: for this, we can take advantage of technologies to "discover" applications (this is better than a manual inventory). Automating deployment (DevOps) is also one of the recommended actions.

Reduce latency: we may fear a degradation of the latency of the network with Zero Trust if there are additional checkpoints: pay attention therefore to the decentralisation of the infrastructure used. This is possible with an edge platform, namely with a massively distributed presence at the edge of networks. This ensures better performance and reliability while using the Internet network.

Strengthen authentication: the objective is to reduce the use of basic passwords and to resort to client certificates. Putting multi-factor authentication (MFA) everywhere is a strong industry trend, highlighted recently by recommendations from government institutions (for example, a recent order from the US government). Not all MFA solutions are created equal, with many vulnerable to man-in-the-middle attacks.

Wavestone recommendations based on their observations

Recognise that it is a challenge: Zero Trust is not a magic bullet, it does not solve all of today's security issues. But Zero Trust requires a combination of a set of technologies and solutions.

Develop your own vision and target: there is not just one definition. Zero Trust is not just an "IAM" project or a microsegmentation project. Every company makes Zero Trust their own, with multiple speeds in different environments. It is not the same Zero Trust project if it is implemented on on-premise bricks or on cloud environments.

Start humbly and choose your battles wisely: the implementation of Zero Trust is a big project, but be careful not to make it too perfect and complex. Do not define too many rules, or too many different trust levels, otherwise it is not realistic. Stay small and humble to start and identify the "small" technological or functional bricks to put in place by working by use case.

Do not Forget Fundamental Security and Resilience: there are two missing in the Zero Trust model, fundamental security – with patching, clean code, the quality of the applications developed, basic cyber hygiene – as well as the resilience of the company once attacked. The reconstruction of the IS once compromised is not dealt with in Zero Trust. Be careful not to focus too much on Zero Trust, which is driven by the market, but is not "magic".

6. CONCLUSION AND OUTLOOKS

Integrate this philosophy into each of the next projects

With remote working, SaaS solutions, extended IS, migration to the cloud, the market and its customers are now facing a divide, a crossroads. The Cigref working group is convinced that the subject is structural, complex, transversal, that it is part of the long term and is materialised by various coordinated projects. As of today, in each of the projects under consideration, organisations must begin to integrate the principles of Zero Trust, whether around the workstation, user awareness, the identity repository, access and network. Companies will also reflect on the integration of this approach with the other steps already taken within them.

Prepare for tomorrow today

To prepare for the future, now is the time to lay the foundations of the requirements for future networks and modes of identity and access management. It is necessary to ask to what extent the principles of Zero Trust can be gradually applied internally and to products in companies. In 10 years, the existing IS (legacy) will be the one we are building today.

Project yourself into future modes of identity and access management

The market will one day adopt a passwordless approach. Biometrics will gradually develop, but there are a few regulatory and ethical steps to take before massive adoption of biometrics. There are also one-time password (OTP) devices. What other breaks should be considered in this field?

Questioning your ability to be "Internet Only"

With the migration of applications to the cloud, the growing use of SaaS applications, and the disappearance of the LAN, a large part of the business flow finds itself using the Internet first and foremost. What does it mean for the company to switch completely? What service guarantee? What sensitivity in terms of availability? Will the Zero Trust model ultimately be the security model that must necessarily be adopted? What impact will the advent of the 5G network have on this strategy?

Strengthening security by design and by operation of applications

With this Zero Trust approach, the intrinsic vulnerabilities of applications are still largely problematic. As each application is thus accessed by any user without an additional "layer", the possibility of hacking them remains intact. Organisations need to rely on applications that are secure by design and by operation (see OECD report[8]).

[8] Enhancing the digital security of products: A policy discussion, OECD Paper on the Digital Economy, 2021, https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-digital-security-of-products_cd9f9ebc-en;jsessionid=s2YIFK-_vqg93a-45hj9gs4k.ip-10-240-5-104

APPENDICES

SOME EXAMPLES OF THE ZERO TRUST APPROACH **28**
Akamai: a step-by-step approach 28
Microsoft: towards Internet Only 30

MATURITY PRINCIPLES AND LEVELS **33**
Zero trust architecture design principles by The National Cyber Security Centre 31
Zero trust architecture key questions by US department of defence 31
Zero Trust Maturity Model Assessment by Microsoft 32

BIBLIOGRAPHY **33**

SOME EXAMPLES OF THE ZERO TRUST APPROACH

AKAMAI: A STEP-BY-STEP APPROACH

While bringing its own Zero Trust solutions to market, Akamai has set ambitious goals to apply this philosophy to its own enterprise ecosystem. This is also a way to showcase what is possible with Akamai's solutions and show that the goal is achievable for any company today. To achieve this, Akamai has pursued a progressive trajectory, with a test & learn approach and a cohabitation of old and new solutions. The important thing is to reduce the attack surface: even a partial deployment of Zero Trust initially is already a good thing, without wanting to cover everything from the start.

The company has set itself several objectives which it is advancing in parallel:

- Remove the notion of "inside"
- Gradually remove the VPN
- Reduce reliance on passwords
- Make every application look like SaaS
- Make every office a Wi-Fi hotspot, with Internet access to the Zero Trust platform

Akamai summarises Zero Trust through these four categories.

- **More security checks:**
  - Contextual user validation
  - Multi-Factor Authentication (MFA)
  - Content validation
- **Simplified IT management:**
  - Easier provisioning
  - Global access model
- **Better monitoring and visibility:**
  - Single bracket
  - Security Information and Event Management (SIEM)
- **More fluid and flexible user experience:**
  - Access from anywhere
  - Single Sign-On (SSO)
  - VPN postage.

In 2016, the teams started by reducing passwords with multi-factor authentication via a client certificate. In 2017, they implemented Zero Trust access control for web applications.

Akamai therefore started this path with web applications because there was no need to install software on user devices, the applications being available directly via a browser (thanks to Enterprise Application Access). Access control therefore becomes more precise and more ergonomic (SSO, elimination of passwords, use of certificates and MFA).

The security team challenged itself to integrate with Zero Trust "100 applications in 100 days". The team even exceeded its goal, with more than 150 applications integrated within this time frame. The company also reviewed and improved the protection of employee equipment against Internet threats such as phishing or access to dangerous resources or software (with Enterprise Threat Protector).

In 2018, the teams installed software (Enterprise Application Access agent) on all customer workstations in order to extend Zero Trust access to applications other than web (for example those

with a native client, such as Outlook). They also launched a Proof of Concept (PoC) for microsegmentation. Throughout that year, they reached the figure of 400 applications accessible via the Zero Trust solution. These applications, which previously could only be reached via a VPN, became easier to reach, without a VPN, but also in a more secure way. Business applications in web version are also became available on employees' mobile phones, without VPN, which was not possible before and this is particularly appreciated by mobile salespeople. Overall, in 2018, 6,500 users benefited from these solutions, representing the vast majority of employees.

In 2019, additional layers of control were added with the deployment of the Zero Trust agent on 3,000 user stations: this not only makes it possible to support more applications, but also to control the adequacy of the employees' workstations in relation to the criticality of each application. Therefore, there is an automatic check for the presence of an antivirus and software updates, more or less demanding depending on the application accessed.

That year, the Akamai solution also implemented an expansion of application flow controls, application attack detection (WAF) and bot management. This makes it possible to prevent vulnerability scans or targeted attacks on business applications, even when these attacks come from employees or partners (by an intention to harm or by malware installed without their knowledge).

2020 made it possible to make a Zero Trust agent completely widespread for all employees and to eliminate the VPN. Up to that point, VPN had remained available alongside the Zero Trust solution, in order to support a smooth transition. From that moment, the server of an application irrelevant with the role of a user becomes completely invisible, as if it does not exist, and cannot be the object of scans or attacks without intervention of prior Zero Trust checks (identity, role, workstation, etc.).

In 2021, the company continued to implement microsegmentation with new technology (application servers or containers without using firewalls on the outside). This allows for increasingly edge-oriented deployment, with more redundancy and security.

MICROSOFT: TOWARDS INTERNET ONLY

Microsoft's IS is already quite mature in implementing Zero Trust principles. Beyond the technological dimension, governance, change management, and communication are essential. It is not recommended to be "over-equipped" with technical solutions. The approach towards Zero Trust is managed by the Security entity of the IT department, consisting of 500 people and extends over a wide scope that goes from IT security to business continuity and stops only at physical security.

Microsoft IT is the laboratory and the company's showcase. The employees are the testers of the new functionalities of the solutions via a deployment by concentric circles, test & learn, then the functionalities are made available off the shelf, before company-wide deployment and for the customers.

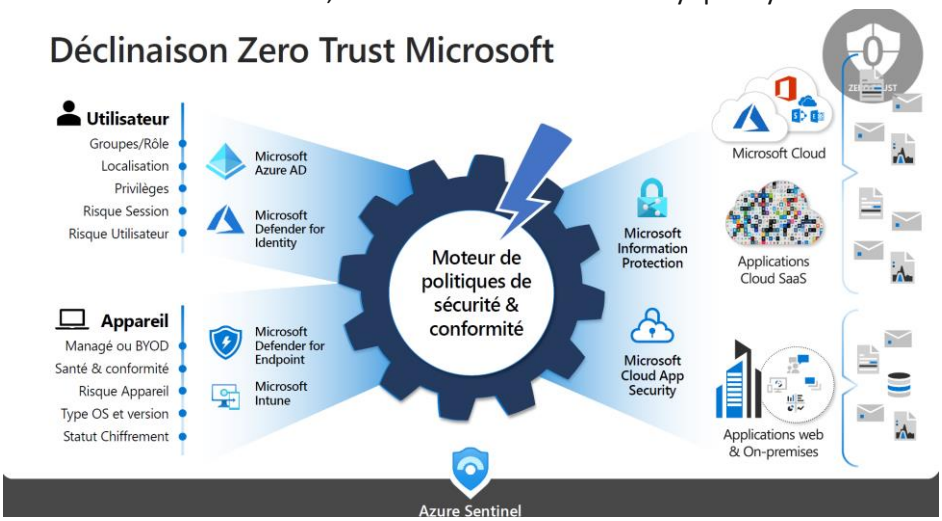
The IT teams have been working for some time on:

- The elimination of passwords in order to be based on biometrics in particular facial.
- The transition from perimeter security to security based on two factors: identity and data.
- The complete redefinition of their network to decommission the historical network (of very high quality, however) in order to switch to "Internet First", and tomorrow to "Internet Only".
- The implementation of a hybrid device management mode.

The implementation of Zero Trust is not carried out in Big Bang mode. The approach is carried out by successive samples, with identified populations. Change management and user information are key success factors to consider, including for a technology company like Microsoft.

Conditional access was put in place before the pandemic, thus making remote working secure. Security is provided end-to-end, depending on the user consuming the cloud service in an open mode. Indeed, the technology company has migrated nearly 96% of applications to Azure, with an on-premise residual. Tools allowing the security of the hybrid application fleet make it possible to open the IS to customers and partners, and to interact with third parties.

In applying its "Assume breach" principle, Microsoft collects more than 18 billion security events every day. Machine learning makes it possible to process this flow of signals that exceeds human capacity, and to create new models and new alerts as quickly as possible to take the right actions and inform customers. Zero defects does not exist, but it must be corrected very quickly.



MATURITY PRINCIPLES AND LEVELS

ZERO TRUST ARCHITECTURE DESIGN PRINCIPLES BY THE NATIONAL CYBER SECURITY CENTRE

1. Know your architecture, including users, devices, services and data:
In the Zero Trust network model, knowing your assets is more important than ever.

2. Know the identities of your users, services and devices:
In a Zero Trust architecture, identity becomes the new perimeter, it is important to have a single source of identity for each of the following: user (human), service (machine or software process) and device.

3. Know the "health status" of your users, devices and services:
Device health, user behaviour, and services are some of the most important signals used to build trust.

4. Use policies to authorise requests:
Each data or service access request must be verified by a central policy engine, which compares signals to access policies to determine an access decision.

5. Authenticate and authorise everywhere:
In a Zero Trust architecture, we assume that the network is hostile, we authenticate and authorise all connections that access data or services.

6. Focus your monitoring on devices and services:
Since devices and services are more exposed to attacks from the network than in traditional architectures, it is important to perform comprehensive attack monitoring.

7. Do not trust any network, including your own
In a Zero Trust context, the network is considered hostile. Trust users, devices and services rather than the network.

8. Choose services designed for Zero Trust:
Choose services with built-in support for Zero Trust network architectures.

ZERO TRUST ARCHITECTURE KEY QUESTIONS BY US DEPARTMENT OF DEFENCE

1. Does your organisation have a plan to ensure that 100% of the data transmitted between devices, and stored on mass media, are securely encrypted? Does the organisation have a robust and secure encryption key management strategy?

2. Does your organisation find and mitigate traditional vulnerabilities inside the network, such as data stored in insecure locations, overuse of service accounts, and permanent administrative rights?

3. Does your organisation apply 100% multi-factor authentication to user-accessible services and servers on all equipment, including mobile devices?

4. Does your organisation have processes in place to continuously scan all end-user devices for malware, and is device health a real-time criteria for accessing your organisation's services?

5. Does your organisation have a strategy in place to apply access rights strictly based on a user's role and to dynamically change those rights when a user's role in the organisation changes?

6. Does your organisation plan the migration of all critical services to connect directly to the Internet and put in place the necessary security to allow these services to be secure in this Internet focused build?

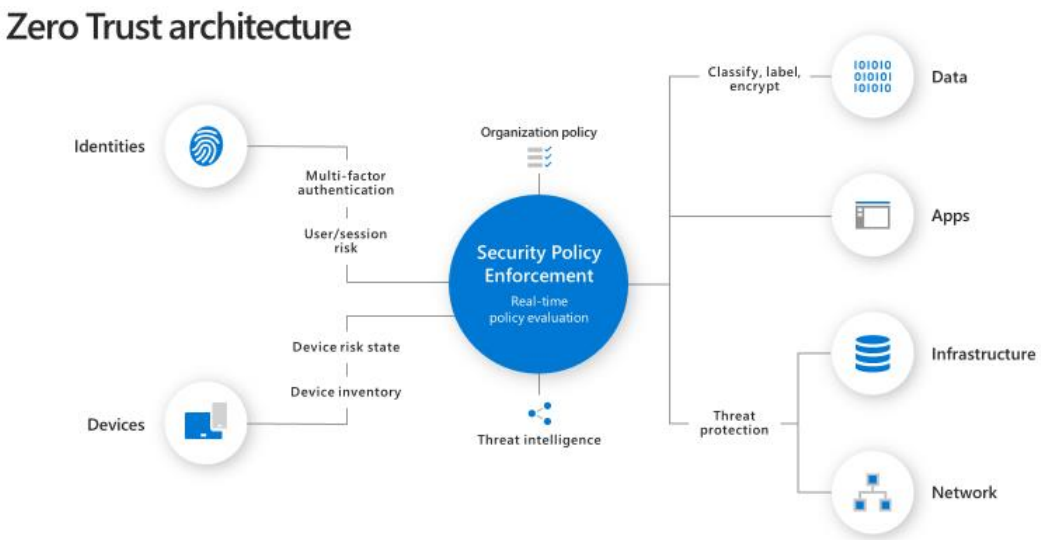
7. Does your organisation design Zero Trust for scalability, support, and lifecycle management?

8. Does your organisation have a strategy for determining what you buy (commercially) and what you custom develop (or pay for custom development)?

MICROSOFT'S ZERO TRUST MATURITY MODEL ASSESSMENT

Microsoft offers an online maturity assessment tool, with recommendations for starting a Zero Trust project. The six main pillars are: Network, Infrastructure, Devices, Applications, Data, Identity. Each of these major pillars is broken down into several questions to find out about the current state of organisations.

[Zero Trust Maturity Model Assessment Tool (microsoft.com)]



BIBLIOGRAPHY

Documents (in chronological order)

- Forrester Zero Trust, 2010: Forrester_zero_trust_DNA.pdf
- NIST Zero Trust Architecture, 2018: Zero Trust Architecture (nist.gov)
- Zero Trust Architecture Key Questions By US Department Of Defence, 2019: DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF (defense.gov)
- UK National Cybersecurity Centre, 2019: GitHub - ukncsc/zero-trust-architecture: Principles to help you design and deploy a Zero trust architecture
- ANSSI, Avis scientifiques et techniques sur le modèle Zero Trust, 2021: ANSSI, Avis_scientifiques_et_techniques-modele_Zero_trust.pdf (in French)
- President Biden's Executive Order for the Adoption of Zero Trust in administrations, 2021: Executive Order on Improving the Nation's Cybersecurity | The White House
- Okta, State of Zero Trust Security, 2021: State of Zero Trust Security 2021
- Microsoft documentation, 2021:
- Microsoft Zero Trust Adoption Report and Implementing a Zero Trust security model at Microsoft,
- Download Initiating a Zero Trust transformation project from Official Microsoft Download Center
- Cisco, Gartner's SASE model, 2021: What Is Gartner's SASE Security Model? - Cisco Umbrella

Videos

- [TECH AU CARRE] Initier un projet Zero Trust - partie 1 - YouTube (in french)
- [TECH AU CARRE] - Zero Trust vs SASE : où se situe la vérité ? - YouTube (in French)

Podcasts

- NoLimitSecu, Episode #284 on Zero Trust with Thomas Burnouf and Etienne Ladent: Zero Trust - NoLimitSecu (in French)

Cigref
SUCCEED WITH DIGITAL

Achieving digital success to help promote the economic growth and competitiveness of its members, who are major French corporations and public administrations, and users of digital solutions and services

Cigref is a network of major French corporations and public administrations set up with a view to developing its members' capability to acquire and master digital technology. It is a unifying player in the digital society, thanks to its high-quality thinking and the extent to which it represents its members. Cigref is a not-for-profit body in accordance with the French law of 1901, created in 1970.

To achieve its mission, Cigref counts on three business units, which make it unique.

Belonging

Cigref speaks with one voice on behalf of major French corporations and public administrations on the subject of digital technology. Its members share their experiences of the use of technology in working groups in order to elicit best practices.

Intelligence

Cigref takes part in group discussions of the economic and societal issues raised by information technologies. Founded nearly 50 years ago, making it one of the oldest digital associations in France, it draws its legitimacy from both its history and its understanding of technical topics, giving it a solid platform of skills and know-how, the foundation stones of digital technology.

Influence

Cigref ensures that its member companies' legitimate interests are known and respected. As an independent forum in which practitioners and actors can discuss and create, it is a benchmark recognised by its whole ecosystem.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr