Security Model Evolution

Research conducted in partnership with

proofpoint®

Version notes

Version	Date	Comments
1.0	24/01/2021	

Contents

1. Foreword

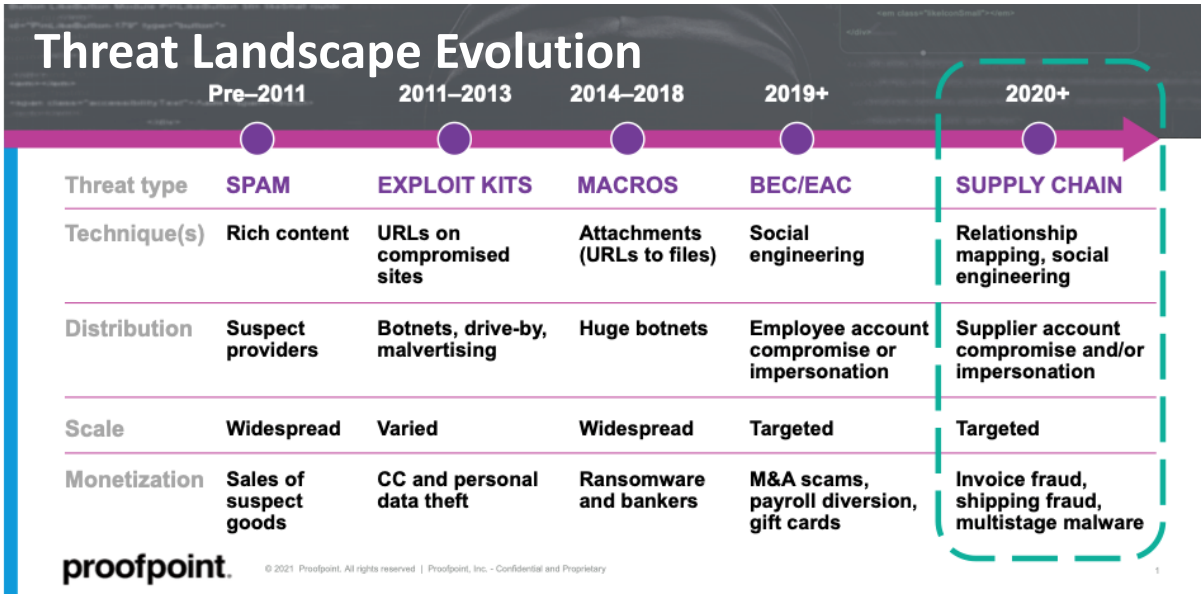
The purpose of this document is to present and explain the paradigm shift that has been taking place in companies over recent years, and which has become even more apparent since the start of the COVID-19 pandemic. In fact, the pandemic has highlighted certain obstacles and issues that had to be addressed, sometimes urgently (e.g., providing ability to perform remote working, enable access to certain sensitive applications, workstation monitoring, etc.). At the same time, cybercriminals have taken advantage of this period to step up their attacks. In some cases, a period of regularisation was needed to restore a more manageable situation including security controls, that better aligned with the company's security policy. However, over and above the findings from this period and the actions carried out or undertaken to improve security, there are other key considerations that should be taken into account (threat evolution, faster digital transformation, ever-increasing use of the cloud, need for greater responsiveness and ergonomic access to services, etc.), which prompt us to reconsider and, in all likelihood, re-examine our security models and strategy. This document presents an overview of these requirements and difficulties, and provides guidelines for a possible new approach to security strategy.

It is intended for any business, IS, or CISO manager with the aim of shedding some practical light on the findings of the current IS/cybersecurity context, and suggesting ways of thinking about how to develop strategies and solutions.

2. Background

2.1. Evolution of security attacks

As illustrated below, cyber security threats have evolved significantly over the last 20 years. Attacks are now complex, targeted, and use social engineering techniques.



2.2. Outsourcing

Our information systems have opened up to the outside world with the arrival of a host of online services, communication tools, exchange platforms and many other features. In addition, some online information systems have been outsourced using, for example, online office automation.

2.3. Mobility

Employees are now regularly away from company premises, working remotely or at home, or are even forced to stay away from the company for months on end, as was the case with COVID-19.

2.4. Digitisation

Customers visit bank and insurance branches less and less, preferring – or being required – to carry out tasks online.

Company boundaries have thus changed, so much so that the traditional security model of recent years has to be updated to take these new elements into account.

The following observations and findings result from a desire to maintain a certain distance, and to offer recommendations for a security model at macroscopic scale that can be applied to any company today.

3. Scope of the study

3.1. Stakeholders

"Know the stakeholder" means knowing enough about them to ensure they are provided with the best possible service, a service that meets their needs and is most useful to them.

This means obtaining a "segmentation", i.e. categorising stakeholders in accordance with the nature of the relationship that the company intends having with them.

In formal terms, such a categorisation involves:

- Dividing all stakeholders, without omission or duplication, allowing each stakeholder to be assigned to one – and only one – category
- A set of parameters observable for each stakeholder
- Rules that will enable identification of the category to which the stakeholder belongs if stakeholder-specific parameter values are known (categorisation).

The grouping of stakeholders together into a category will allow a distinct set of needs to be identified and addressed. It is assumed that all stakeholders within a given category are sufficiently similar in terms of their needs.

To serve information system stakeholders, companies must segment the population they represent (internal marketing). The aim is not to adapt stakeholders to the information system, but to define what the information system must do to meet their requirements.

In order to consider all of the stakeholders involved in the security model, it is proposed to categorise them according to both their origin as well as their interactions with the company. Thus **14 types of stakeholders or divisions** can be split into *3 categories or classes*: **employees** (or internal third parties) and **temporary staff** as well as **IT processing** belong to the *business* sphere, while **clients, prospects**, **law enforcement**, **parties to a contract**, and **internet users** are part of the *public* environment. Lastly, **service providers, intermediaries, distributors, suppliers** and **peers** make up the group of *partners* (or external third parties – not the public).

An information system's stakeholders can be internal (with **employees** and **temporary staff**) using the information, handling the information system tools, as well as building and managing the information system, or they can be external economic partners (**customers**, **suppliers**, subcontractors, service providers, software publishers, etc.).

In a company, the information system becomes the most important asset. It records the language of the company, which uses it to store the concepts with which it organises itself, segments its clients, and defines its products. The company's Information System (IS) stores data intended for company **employees**, and increasingly also for the *public domain* and for *partners*, and assists them by automatically classifying, researching, processing, translating and communicating tasks (**IT processing**). The relationship between this asset and the people who use it is highly diverse, although we often speak about "users" or "stakeholders".

3.1.1. Company

The company's internal representatives or **employees** consist of staff members: those with permanent and fixed-term contracts, work-study students, trainees, but also **temporary staff** (traditionally called internal service providers or cost-plus contract workers), and virtual employees such as bots or batches needed to carry out operations.

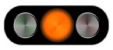
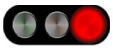
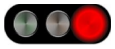
Together they form part of the company's resources, consisting of users and specialists (particularly IT specialists).

Knowing how the company's data is used by its stakeholders helps define security rules that limit the risks involved in accessing and processing unwanted information.

The diagram below briefly illustrates the various characteristics of employees:

Figure 1 - presentation of different employee types

Identity and Access Management (IAM) is a set of processes set up to manage user authorisations (users may be **employees**, service providers, **temporary staff**, etc.) in order to regulate access to the network and applications. These processes make it possible to adapt company users' authorisations or access rights according to their role, function, or hierarchical responsibilities depending on their movements (entry, exit, mobility) or their status at a given moment (inventory). Within these processes it is particularly important to target access accounts with human privileges (super-user accounts, administrator accounts, emergency accounts, access to financial or HR systems, etc.) or non-human privileges (application accounts, service accounts, etc.).

Company	
Stakeholder	**Criticality**
Employees	
Temporary staff	
IT processing	

3.1.2. Public

The *public* environment generally corresponds to **clients** or **prospects**. In some specific cases **law enforcement** (subject to letters rogatory from a judge), **contracting parties** or **internet users** also fall into this category.

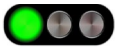
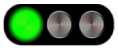
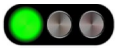
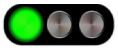
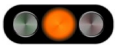
A **client** can be defined as a person who receives a service or good from a company in return for payment of a sum of money.

A **prospect** refers to a company's potential **customers** with whom its departments aim to establish a commercial relationship (prospection).

Law enforcement represents all institutions whose task is to ensure public order and respect for the law.

The various **parties to a contract** present in the IS should not be forgotten either, as they may have temporary or permanent access to it (beneficiary, claimant, tutor, guardian, parent, guarantor, payer, etc.). Not to mention all the **internet users** who access the IS via the institutional site(s).

This extended company implies dealing with multiple external stakeholders and therefore with users who generally have their own working environments and means of access to the information system, and who have a digital identity specific to their own organisation. Similarly, IAM offers all the features adapted to the extended company.

Public	
Stakeholder	**Criticality**
Clients	
Prospects	
Law enforcement	
Contracting parties	
Internet users	

3.1.3. Partners

Use of a service provider has various names depending on which legislation we refer to (see. Appendix 1.2).

Before entering into a business relationship with a commercial *partner* (**client**, **supplier**), a company must always conduct prior checks called due diligence (financial health, reputation, partner integrity, etc.).

This analysis is not only limited to new *partners*; the existing portfolio must also be monitored. To do this, priority must be given to the quality of information, and this can come from either inside the company, through **client** questionnaires, or from outside the company, through information gathering from reliable sources.

External third parties or *partners* (excluding the public) include all external parties with whom a formal or informal (i.e. oral) contract (or equivalent) is entered into: **service providers** (project, maintenance, etc.), **suppliers** (hardware or software), **intermediaries**, independent **distributors,** as well as a particular type of stakeholder, **peers** in expert associations, inter-company working groups, etc.

A **service provider** is a person who undertakes or who is responsible for providing work, a service, for supplying a deliverable or performing a service. They interact directly with the company's information system.

A **supplier** is a legal entity or natural person who provides, a purchasing company, with certain goods or services.

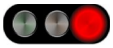
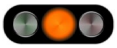
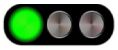
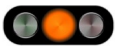
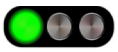
Thus, the **supplier** delivers to the company the inputs needed for production, which it will transform into deliverables. Integrating these into the company is the responsibility of company stakeholders.

An **intermediary** is a professional whose role is either to seek a return or to represent one or more persons for the purpose of conducting one or more civil or commercial transactions with others (e.g.: broker, commercial agent, sales representative, trustee, del credere agent, commission agent, etc).

Distributors are **intermediaries** who enable companies to reach their **clients**. Without **distributors**, products are generally not sold and companies go bankrupt. As such distributors contribute to creating and modifying data – of value – in the company's IS, while accessing a large amount of private information made available to them to carry out their activities.

A **peer** is a person with the same position or role as another person.

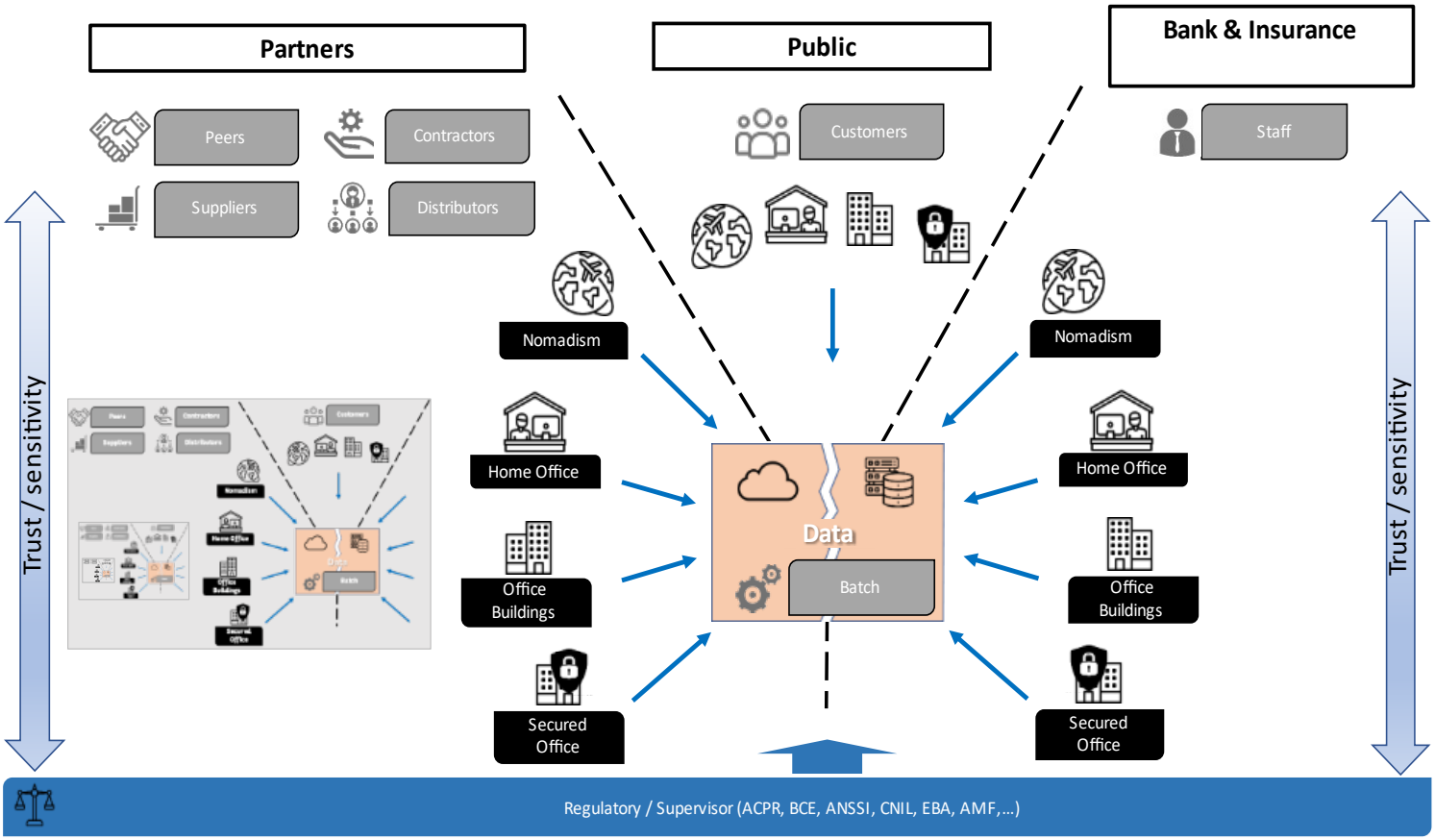
In order to open up its information system to all internal or external users, a company should not use multiple solutions depending on the accesses to be protected, or limit itself to specific complex developments: mutualisation and standardisation are the keywords here. A well-designed IAM can accommodate all three of the defined categories.

Service providers	
Stakeholder	**Criticality**
Service providers	
Suppliers	
Intermediaries	
Distributors	
Peers	

3.2. Presentation of the information system and its interactions

Figure 2 - Macroscopic view of today's companies

This macroscopic presentation of today's companies and the links between the various stakeholders in the security model helps highlight the channels at risk for companies' physical and digital security.



4. Usage scenarios to consider

Information systems are increasingly open to a wide range of stakeholders with extremely varied uses. An IS access controlling system has thus become an essential building block in preserving IT resource security, even more so as CISOs remain responsible for all accesses to their IS.

In the event of a critical incident or attack, it is these access management systems that will provide the ability to react or investigate, based on the audit trails they generate.

However, the COVID-19 pandemic has severely disrupted this sound management. In order to maintain IS access for staff members under lockdown, companies urgently needed to extend access. As well as providing remote access on a mass scale to non-equipped users, services or applications also had to be opened up for remote access, despite some of them having previously been considered too sensitive.

Access granting was generally decided on the basis of simplified risk analyses, subject to new checks and with the intention of withdrawing such access again once the pandemic was over. All of these temporary authorisations were recorded and managed in the form of derogations (known as "COVID derogations") as that seemed the most suitable system owing to the fact that they were non-permanent.

However, the lasting health crisis, the generalisation of remote working, and establishment of a "new normal" have raised the question of whether this type of access will continue to be considered non-permanent. These COVID derogations used to grant new accesses are therefore a potential fresh source of risk, and it is essential to review them periodically in order to maintain good control over IS security levels.

4.1. Access via company resources

4.1.1. From company premises

Insofar as data can be hosted outside company premises, access to this data (cloud, etc.) requires securing communication channels (encryption), and ensuring that access points used and users are both legitimate. In addition, as premises have modern access (e.g. company wi-fi) it means securing them to prevent any intrusion into the IS via external access to these premises.

4.1.2. From secure premises

Secure premises include the various sensitive zones of banks and insurance companies (e.g. trading floors, vaults, data centers, SOCs, etc.). The ability to monitor these zones is increasingly being impacted by the adoption of IoT, making such detection and supervision ever more complicated.

4.1.3. From home

With no access to company premises (e.g. due to COVID lockdowns), it became essential to have the possibility of carrying out sensitive tasks from home. Being able to trust the local network, (use of wi-fi, private devices, etc.) is all the more necessary, as is provision of resources for secure connectivity to company data.

NB: the presence of a virtual assistant at home is a risk which brings the home into the same category as the following “nomadic” use case.

4.1.4. Nomadic

In addition to the requirements mentioned previously, no trust can/should be placed in public internet access points, or even other people around (risk of “shoulder surfing”).

4.2. Access by the general public

Clients' interactions with their bank or insurance advisors have changed tremendously in recent years: falling numbers of visits to physical branches has gone hand in hand with a massive uptake in "consumer" solutions, as well as new features in the digital applications made available by their establishment. Some of these changes include:

- Dialogue with advisors via a secure messaging system, or in some cases via the company messaging system
- Possibility of carrying out routine transactions or taking out subscriptions online without having to go into a branch (multichannel), or of finalising an action started on the internet with an advisor (omnichannel)
- Extended accessibility allowing any type of device to be used (personal computer, cybercafé, smartphone, telephone, etc.), irrespective of location (at home, while travelling, abroad)
- Provision of documents in digital format (via USB stick, messaging system, personal cloud storage, dedicated portal)
- Account aggregation features (using APIs) to view assets that are spread across several establishments on a single page
- Increased security for access to online banking and internet payments.

Although there are obvious benefits for customers, new risk scenarios have emerged or become more prevalent, fuelled by these trends.

The proliferation of digital client journeys, emails, and notifications sent by establishments make clients even more vulnerable to phishing. Once victims have been infected, malware harvests their personal or banking data, which can then be exploited for resale or financial fraud.

Similarly, the use of unsecured messaging systems increases the risk of spoofing: a client's hacked online messaging system could be used to carry out banking transactions. In addition, use of a company messaging system by an advisor could also lead to spoofing of the company's domain name (DNS) by display, or it could be maliciously exploited (typo squatting of similar domain names).

The lack of control over the level of security of clients' devices is also a source of risk: websites and mobile applications constantly have to incorporate new defence mechanisms to minimise the potential impact of client devices being infected by malicious code. In addition, checking technical specifications (version and type of browser, language used, operating system) and contextual features (connection dates and times, types of usual/unusual transactions, etc.) makes it possible to combat crude spoofing attempts relatively effectively. However, these techniques have developed to meet clients' need for mobility.

Remote interactions also require exchanging large quantities of supporting documents containing personal data via the internet: e.g. when taking out life insurance or a mortgage. Although establishments have often implemented tools specifically for this purpose, there are also other, simpler use cases: bringing a USB stick to a branch, asking the customer to download documents from Dropbox, etc.
A document carrying malicious code could infect an advisor's workstation, and then spread through the establishment's IS.

New uses related to bank aggregation tools – made mandatory since DSP2 regulations were introduced – are also a source of risk. This type of service is based on the opening of APIs on the internet: such application interfaces can be a new vector of infection if security is not sufficiently taken into account right from the outset (security by design). They can also be the source of data loss.

This same regulation is also behind increased security of access to online banking (as well as online payments): use of Multi-Factor Authentication (MFA) has become more widespread. However not all MFA solutions offer the same level of security, particularly when 2 channels for distribution of authentication secrets end up being read on the same device. For example, this is the case for the following entirely smartphone-based processes:

- Initial password sent by email, to be changed at first login
- Distribution of a 2nd factor by text message or notification.

Note that it will be easier to use a malicious application to access text messages as opposed to notifications. The latter, although based on cloud services, are provided by major digital stakeholders, and thus feature sophisticated monitoring systems and features.

4.3. Partner access

A partner's access to our information system and interaction with it will depend very much on the type of partner in question (see section 3.1.3). It is assumed that prior – not only technical – checks will have been carried out (e.g.: KYC, GDPR, Sapin Law, etc).

Vetting and security solutions with different levels of stringency could be implemented depending on the type of partner. It should also be noted that a contractual relationship generally exists with the partner. This contractual relationship must be put to good use by asking for formal, specific security guarantees (e.g. security insurance plan) as soon as the service or relationship begins. It should be possible to formally check these guarantees and security commitments from the outset of the relationship as well as over the long term. A clause should allow these requirements to be adapted based on the results of checks, changes in the service provided, and the development of threats.

In addition, it is worth emphasising that for this type of relationship an accurate mapping (partner relationships; type of relationship, including security, etc.) should be drawn up, and regularly updated with reinforced monitoring (CERT, SOC).

4.3.1. From company premises

Regarding the internal information system (on premises), in sum we can differentiate between two types of access:

- Access via devices provided by the company, in which case company security policy and security solutions apply. Special attention should nevertheless be paid to the services (applications, functions) which the partner will need to provide its service or guarantee its relationship. In other words, the partner is not a company employee and as such their access rights must be limited to the strict minimum. In terms of solutions, network access control (NAC), authentication – preferably multi-factor – (at application level), and role-based access control (RBAC) will be implemented
- Access via partners' devices, for which safety must nevertheless be ensured. A state-of-the-art level of compliance and integration of these devices is highly recommended or even required in some cases. "Guest" access solutions (such as guest wi-fi) can also be set up.

Regarding access to company IS in the cloud, a similar approach (company or partner workstation) must be applied. The monitoring possibilities offered by the cloud service subscribed to must of course be taken into account. Special attention should be paid to authorisation and authentication in order to be able to distinguish between employee and service provider access.

For certain interactions or relationships, specific systems (internal or in the cloud) could be implemented to give read and write access to shared information. One example might be the case of peers within the Forum des Compétences and its working groups. Here again, an authorisation process and level of authentication in line with the level of risk should be implemented.

4.3.2. From secure premises

The relationship or interaction between the partner and company can be conducted between the clearly identified, secure premises of both parties. The workstation-type approach specified in section 4.3.1 continues to apply, together with the related security requirements (permissions, authentication, workstation integration, monitoring, etc). Detailed mapping of this type of relationship should be defined and updated (particularly the type of relationship via the internet or specialised link, level of security of the relationship and link, etc.)

4.3.3. From home

Once again, the type of workstation must be taken into account (company or partner, even personal or BYOD) as this will condition the level of authorised access allowed to the resources. However, in theory this type of access poses greater risks, in a similar way to employee access. Ideally, authentication should be stricter and access to certain resources restricted or even forbidden in some cases.

4.3.4. Nomadic

We find the same type of issue as in section 4.3.3, but with stricter requirements and prohibitions which in certain cases will depend on partners' behaviour (e.g.: ban on using public wi-fi and carrying out certain actions from certain locations: risks of spying or improper influence).

4.3.5. Chaining

This is the most complex case as it will be difficult to map accurately. In addition, the principle of the weakest link is fully applicable by contagion. If certain partners in direct contact with the company do not apply sufficient checks and safeguarding policies with their partners, a safety breach by one of these partners could impact us.

Furthermore, there are more or less direct dependencies (e.g. security or IT solution suppliers) which increasingly present a proven risk for the company. This is known as a "supply chain attack". If these partners are compromised (e.g. by introduction of malware or a "backdoor" in their software), the end client will be vulnerable to a potential attack with a multiplying factor based on the "success" of the software.

4.4. Supervision by regulators

A new, previously uncommon concept emerged in 2020: checks carried out remotely. In this way checks became more declarative, with potential loss of quality. What will happen with long-term widespread use of this type of practice?

New communication and remote data gathering tools have become necessary. As data handled by controllers is often confidential, should we move towards dedicated, sovereign tools at the request of regulators in order to mitigate any confidentiality breach in the data processed?

Lastly, controller spoofing is a new risk that also needs to be taken into account. Measures already exist to safeguard against it, such as the requirement to have an engagement letter before carrying out checks for example. But it is also becoming necessary to ensure the identity of controllers during checks, using techniques such as strong authentication. This also supports the idea of establishing shared video conference tools where the identity of each person can be verified during the checking process.

4.5. Concept of trust/sensitivity

The level of trust assigned must be determined for all the use cases identified, depending on:

- Type of stakeholder: partners, clients, employees
- Context of use: nomadic, remote, or on company premises
- Type of resource accessed: public data, restricted data, confidential data or secret data

This is in order to determine the checks required for this access.

5. Is Zero Trust the answer?

5.1. What is Zero Trust?

5.1.1. Origins

To answer all the issues presented above, new concepts have emerged including the "Zero Trust" concept which it seems worthwhile to present here and explain in detail.

The concept was invented in 2010 by a Forrester analyst,[1] who published a report showing that the concept was able to increase company security levels based on some simple principles:

- Consider all traffic as a threat
- Grant the least amount of privileges
- Monitor technical and user access

5.1.2. The NIST perspective

In order to avoid "Zero Trust" becoming a catch-all expression, the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce, issued in August 2020 the Special Publication "800-207 Zero Trust Architecture"[2] which details the concept, and explains the principles for implementing it.

In this publication, the NIST defines seven tenets on which Zero Trust architecture is based:

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioural and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6. All resource authentication and authorisation are dynamic and strictly enforced before access is allowed
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

In a nutshell, **all access to a resource** (1) **must be secure** (2), **checked** (3), **dynamic** (4 & 5), **monitored** (6) **and supervised** (7) **in real time.**

[1] John Kindervag (2010), Build Security Into Your Network's DNA: The Zero Trust Network Architecture
[2] https://csrc.nist.gov/publications/detail/sp/800-207/final

5.1.3. ANSSI' technical and scientific opinion

ANSSI also issued a scientific and technical opinion in April 2021[3], the principles of which are listed and explained below:

- Access requests should be checked in the same way, whatever their origin ("inside" or "outside" perimeters of the entity)
- Access to resources should be granted on a need-to-know basis
- Access should be granted based on the lowest level of privilege required to perform the task
- Resource access policy should be dynamic and take into account a wide range of attributes (identities of the person accessing and the resource accessed, sensitivity of resources requested, behavioural analysis of the user, access times, etc.)
- The entity must ensure the security of all assets when access is requested, and on a recurring basis during use
- Authentications and authorisations to access resources must be regularly re-evaluated

Below are the priorities to focus on:

- Improved identity governance
- More granular and dynamic segmentation of resources
- Use of state-of-the-art authentication tools
- Enhanced detection capabilities
- State-of-the-art configuration

[3] Zero Trust model | French National Agency for the Security of Information Systems (ssi.gouv.fr)

5.2. Why is this concept interesting?

The explanations of NIST and ANSSI clarify:

- The requirement to control all human or technical resources that want to access the information system "*whatever their origin*" (ANSSI)
- The requirement to systematically and continuously monitor access to resources with regular re-evaluations
- The requirement to segment or even silo resources accessed according to their role, use, sensitivity, or business scope

Thus, if we take another look at the diagram of today's information system presented in section 3.2, we can superimpose a few major areas of interest onto it:

- Global and systematic identity management to control all human resources
- Global and systematic management of devices (managed or not) to control technical resources accessing the information system
- Conditional access taking into account the context (user/terminal/resource accessed/conditions) to dynamically determine whether the request is in line with access policy
- A siloed information system so that an authorisation only allows access to the resource concerned

All this must be:

- Monitored in real time
- Monitored automatically

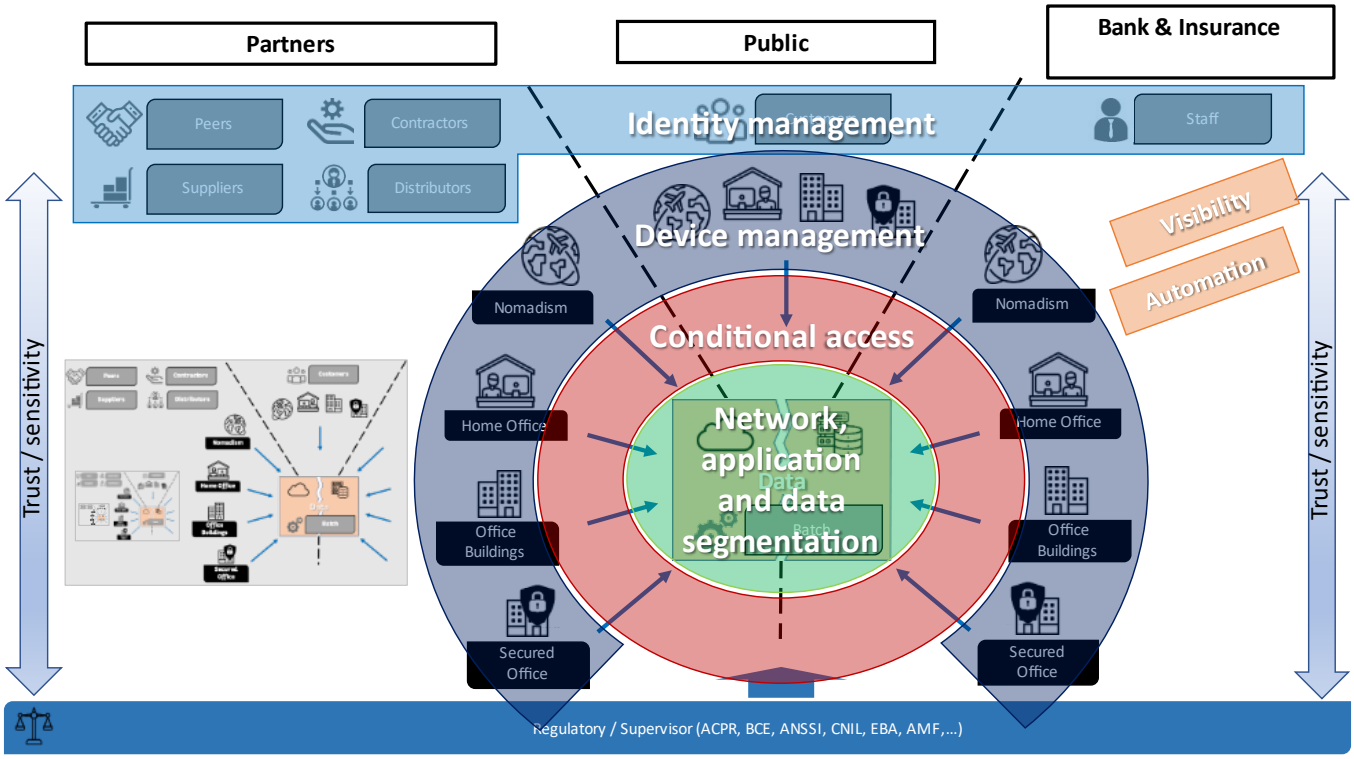
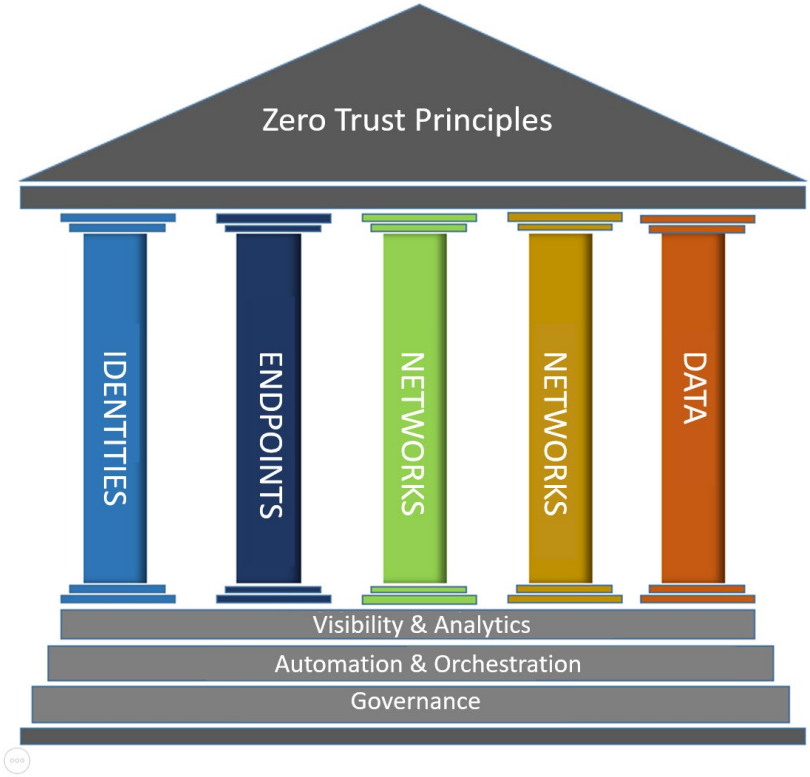


Figure 3 - Link between representation of the company and Zero Trust concepts

This concept is interesting because it allows us to generalise access and interaction within an information system that has become complex and diverse. In some respects, it challenges the access and interaction rationale within an information system in order to make it easier to understand and monitor. In addition, the segmentation resulting from the security model provides protection against lateral movements.

5.3. Details of prerequisites

Zero Trust can be seen as a strategic initiative that allows management to implement pragmatic and effective security measures. To do that, six pillars are fundamental for Zero Trust.



5.3.1. Identities

Identity and Access Management (IAM) is the crucial security building block of the Zero Trust pillars. In a Zero Trust strategy, the **main functions** of an identity and access management solution should make it possible to:

- Define an access rights management policy (defining profiles, life cycle, monitoring)
- Allocate access rights by following the **principle of least privilege**
- **Continuously check** the identity of an individual, process, or machine using one or more **authentication credentials** (2FA, FIDO, certificate, etc.)
- Integrate **behavioural analysis** into the authentication process (device fingerprinting, geoprofiling, time range, etc.)
- Protect privileged accounts by storing the secret in a virtual safe
- Apply single sign-on and identity federation to access cloud applications.

5.3.2. Devices

The security posture of devices from which users connect to company resources must be **continuously** evaluated for each access request:

- Compromise status
- Vulnerabilities
- Software version
- Protection status
- Encryption
- etc.

Changing the status of a device to a higher risk security posture must modify the access rights assigned to the identity dynamically.

Here are some practical use cases on assessing device security posture:

- On **managed devices**, the management of known or unknown threats via various technological approaches such as EPP and EDR will enable at-risk devices to be detected, and access rights can be adapted dynamically to company resources. The security logs from these solutions should be leveraged to manage access dynamically at infrastructure level.

- Assessment of security posture is very limited for **non-managed devices (BYOD)**.

As well as evaluating the security posture on devices, which is the key element of this "Devices" key area, it is obviously recommended to have good asset management: inventory, vulnerability and patch management, etc. (ANSSI Reference Guide)

5.3.3. Networks

Although a Zero Trust strategy is primarily based on identity (Data Centre, IaaS), generally speaking the network remains a fundamental step *towards guaranteeing access to resources while applying a level of control with Zero Trust*.

At network level a Zero Trust model is a real revolution, and aims to:

- Microsegment resources at network level (data centre, cloud) in order to limit the spread of malware and prevent lateral movements
- Protect communications via various encryption systems: IPsec, TLS, etc.
- Protect against advanced threats by increasing detection of malicious behaviour within the network and the appropriate response.

From a practical point of view, two technological approaches have launched recently in order to address Zero Trust needs at network level:

- **Microsegmentation software,** various types of technology (via virtualisation or an agent) to create increasingly granular security zones within data centres and cloud deployments to isolate each individual workload and secure it independently of the others, thereby limiting an attacker's ability to move laterally. In other words, microsegmentation software eliminates

server-to-server threats within the Data Centre, securely isolating networks from each other and reducing the total attack surface of a security incident affecting the network.

- **"Network Detection and Response"** is a cybersecurity solution that continuously monitors a network's organisation by collecting all network traffic for better visibility, and by using behavioural analysis, machine learning, and artificial intelligence to detect and respond to cyber threats and abnormal behaviour through native capabilities or by incorporating other cybersecurity tools/solutions.

5.3.4. Applications

In order to align security measures with the Zero Trust model, functions are required to guarantee a level of security at application level while also improving accessibility. These functions hinge on four main areas:

- Access management of cloud/on premises applications is based on identities and strong authentication.
    - An identity provider (IdP) is highly recommended. This IdP will enable identity federation, whether internal or external, from various sources such as the active directory.
    - Strong, context-based authentication should be applied to each access request.

- Protection against advanced threats by analysing all application flows using **web application firewall** (WAF) type tools deployed in the cloud and/or on the premises.

- Access to applications subject to users' location and type of device (managed or not managed), while ensuring secure communication via an SDP approach.
    - **The "Software Defined Perimeter" (SDP)**, a cloud network that provides access to applications by connecting different types of site (SaaS, IaaS and data centres), and offering various access modes (agent or web portal) for managed or non-managed devices
    - SDP includes the principle of least privilege, and takes the device's security posture into account on an ongoing basis
    - Communications are encrypted via IPsec and TLS systems.

- Security tests (e.g. pentests) during all application development phases.

5.3.5. Data

Migrating to the Zero Trust model also requires a data-centric approach in terms of cybersecurity throughout the data life-cycle, in transit or at rest on the company's assets (devices, applications, networks). An information protection strategy will be based on several components:

- Identifying data within the organisation
- Categorising data according to content, criticality, and level of exposure
- Protecting data with an encryption system using key management solutions
- Monitoring access rights to data based on identity
- Detecting and protecting against information leakage
- Analysing data access from a behavioural perspective

5.3.6. Real-time visibility

The Zero Trust programme is based on an advanced monitoring and detection service (new generation SOC, CERT, etc.) with advanced skills (analysts, SOC managers). This service relies especially on tools such as SIEM to manage security events, advanced security analysis platforms, user behaviour analysis, and other online analytical systems to help security experts monitor what is happening in real time and adjust their response intelligently. These increasingly automated real-time solutions should allow experts to focus on the most urgent cases likely to have a major impact on the company. The emphasis on analysing cyber event data can also help establish proactive security measures before an actual incident occurs.

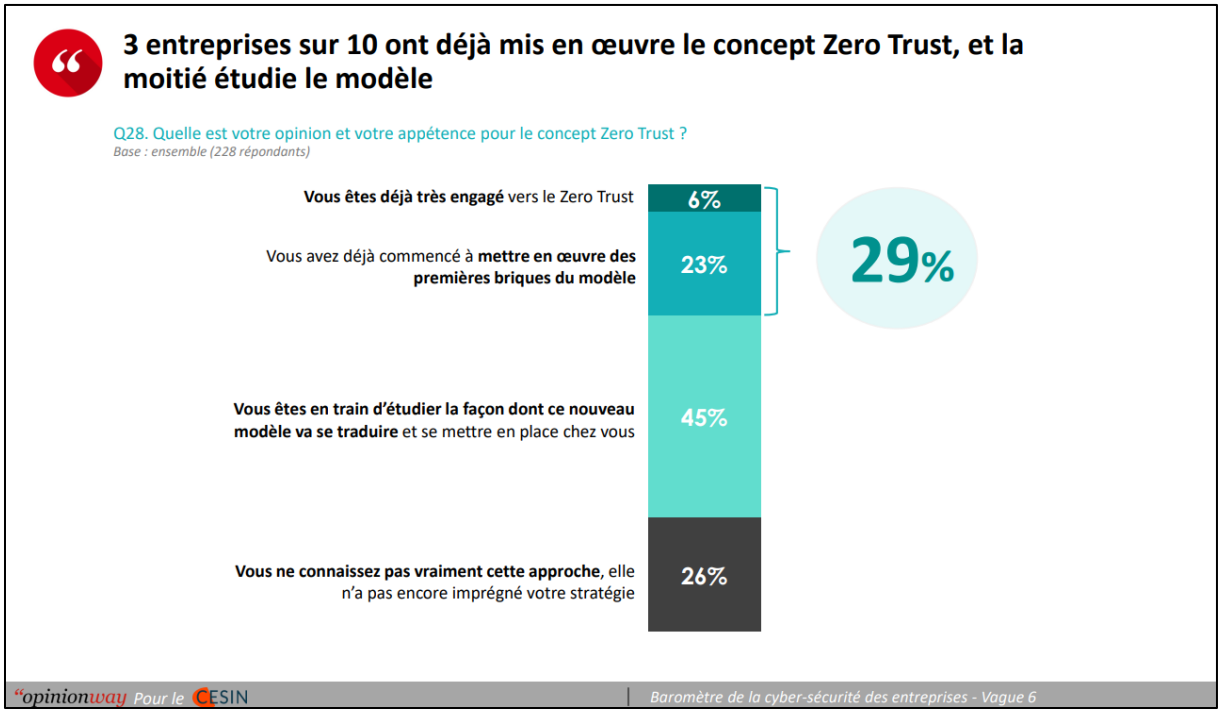
5.3.7. Automation and Orchestration

The Zero Trust model makes full use of security response automation tools that automate tasks across products through workflows, while allowing monitoring and end-user interaction. SOCs generally use other automated tools to manage security information and events, and to analyse user and entity behaviour. Orchestration of security connects these security tools, and helps manage disparate security systems. By working in an integrated manner, these tools can considerably reduce costs as well as manual efforts and event response times. This is a paradigm shift for many companies, a new approach that entails trusting tools with minimal human intervention. The goal is to focus on the essential, and improve response times and anticipation capacity.

6. Current state of play in companies

In January 2021 CESIN published its Company Cybersecurity Barometer, and one of the questions concerned companies' appetite for the Zero Trust concept.

Here are the answers from 228 respondents:



We can see that one-third of companies have decided to embrace this security model.

7. Conclusion

We have seen that the ecosystem surrounding companies has changed a great deal of late, with information system outsourcing, the advent of new working methods, deployment of new collaborative tools that are often outsourced and, more generally, the digitising of society.

To address this situation, in recent years our companies have been deploying information system security programmes that are each as ambitious, relevant and comprehensive as the next.

Having said that, ever more interactions are taking place with ever more parties, a fact that does not make this global securing of our information systems any easier. This is why new security models have appeared, aimed at facilitating adoption and deployment of security measures by simplifying understanding and automation of information system operations.

These new models, which are very attractive on paper, first require implementation and maintenance of the basics (often already deployed in our companies). Then the overall ecosystem also needs to be taken into consideration (employees, clients and partners). Lastly, implementation strategies must be carried out step-by-step to ensure the goal is always achieved, namely “increasing the company's general level of security”. The company should define a trajectory, and this trajectory must take its unique characteristics into account.

In addition, banking, insurance, and other regulatory authorities are there to require and monitor strengthening of these security levels, ultimately resulting in an obligation for continuous improvement and minimisation of risks.

8. Appendices

8.1. Legislation

Use of a service provider takes different names depending on the legislation referred to. The concept of "subcontractor" is defined differently in Article 1 of the Law of 31 December 1975 ("within the meaning of this law, subcontracting is the operation by which a contractor entrusts, by subcontracting and under their responsibility, to another person called a subcontractor, the performance of all or part of the company contract or part of the public contract entered into with the contracting authority", Article 1 of the Law of 31 December 1975 ("within the meaning of this law, subcontracting is the operation by which a contractor entrusts, by subcontracting and under their responsibility, to another person called a subcontractor, the performance of all or part of the company contract or part of the public contract entered into with the contracting authority"), and in GDPR Article 4 ("'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.")

Numerous anti-corruption regulations (Sapin II Law) helping to prevent risks to society (duty of care), money laundering and terrorist financing (AML – Anti Money Laundering / KYC – Know Your Customer, etc.), require companies to comply with the evaluation of external third parties (**clients**, **suppliers**, **intermediaries**).

More specifically, in France the Sapin II Law specifically addresses the fight against corruption, a subject which concerns more than 1,600 French companies. The scope of this law is expected to broaden following recommendations by the French Anti-Corruption Agency (AFA). In France, a company can be found guilty of corruption and sentenced for this offence to a criminal penalty, as well as a potential administrative sanction of €1 million (as laid down in the Sapin II Law).

For companies with capital, Ultimate Beneficial Owners (UBO) are natural persons who either directly or indirectly hold more than 25% of the capital or voting rights, or who exercise control over the company by any other means.

When no natural person has been identified according to the previous criteria, the Ultimate Beneficial Owner(s) is(are) the natural person(s) who legally represent the company. If the legal representative is a legal entity, the Ultimate Beneficial Owner(s) is(are) the natural person(s) who legally represent this legal entity.

Glossary

Acronym	
IAM	Identity and Access Management
IoT	Internet Of Things
DNS	Domain Name System
API	Application Programming Interface
DSP2	2nd European directive on payment services
MFA	Multi-Factor Authentication
CERT	Computer Emergency Response Team
SOC	Security Operation Centre
NAC	Network Access Control
RBAC	Role Based Access Control
ZT	Zero Trust
NIST	National Institute of Standards and Technology
ANSSI	National Agency for Information System Security
GIA	Identity and access management
2FA	Two-factor authentication
FIDO	Fast IDentity Online
EPP	Endpoint Protection Platform
EDR	Endpoint Detection and Response
BYOD	Bring Your Own Device
IaaS / Saas	Infrastructure as a Service / Software As a Service
IdP	Identity Provider
WAF	Web Application Firewall
SDP	Software Defined Perimeter
SIEM	Security Information and Event Management