



CLOUD INFRASTRUCTURE ARCHITECTURE AND THE ZERO TRUST MODEL AS A CYBERSECURITY STRATEGY

ORIGINAL ARTICLE

TEODORO, Douglas Diego Rocha¹

TEODORO, Douglas Diego Rocha. **Cloud infrastructure architecture and the zero trust model as a cybersecurity strategy**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Year. 07, Ed. 11, Vol. 13, pp. 204-232. November 2022.

ISSN: 2448-0959, Access link:
<https://www.nucleodoconhecimento.com.br/technology-en/zero-trust-model>, DOI:
10.32749/nucleodoconhecimento.com.br/technology-en/zero-trust-model

ABSTRACT

Since the emergence of the internet, the vertiginous growth in the use of electronic media has grown in the same proportion as cyber crimes, applied in an increasingly sophisticated way. In addition to these two factors that impact the use of the internet, the speed with which the resources and tools inherent in the area of Information and Communication Technology (ICTs) evolve, which enhance the need to continuously develop and improve the means for the protection of sensitive data of people and public and private organizations. In this perspective, Cloud Computing emerges, which allows the storage of data, networks and applications, and other resources through integrated environments through the internet, from collective providers, as opposed to the on-premise system, which is based on the custody and access through local servers, including mainframes, which are still maintained in most large organizations, such as the banking system, for example. Added to Cloud Computing are Zero Trust practices, whose main innovation is the adoption of several layers of access verification. This article was prepared using bibliographical research as a methodology. The question that arises on the subject is: how does Zero Trust provide greater security to network users? The objective is to demonstrate the advantages of security provided by Zero Trust, combined with Cloud Computing. In view of the analyzed literature, it was possible to conclude the existence of two main aspects brought by Zero Trust: internet user access only from 7 layers of verification, and the mitigation of vulnerabilities, including the idea of responsible browsing by different users.



Keywords: Cybercrime, IT Security, Mainframes, Cloud Computing, Zero Trust.

1. INTRODUCTION

Since the emergence of Information Technologies (IT), the issue of data security has always been at the top of the experts' agenda. Protecting users' sensitive data is a priority, given the recurrent malicious activities, including ransomware and phishing, which compromise user data, as well as internal networks, even affecting organizations' digital assets (IBM, 2022).

The fact is that over time companies have developed internal computing systems, resulting in the implementation of complex and costly information processes, which required investments in equipment, installation and maintenance of programs and teams of specialists to take care of their IT infrastructure, system known as onpremise.

It was the phase in which market requirements conflicted with each other, demanding from infrastructure professionals strong efforts in the search for the preservation of the necessary secure controls, while development professionals were led to act in the identification of “new functionalities for increasingly faster applications ” (CASTRO, 2019, p.1). Such movements kept many difficulties for the effective implantation of integrated solutions that could promote the homogeneity of the platforms.

In this sense, Cloud Computing emerges as a redefinition of ICT practices, both from the perspective of the individual use of networks and systems accessed by citizens, and within organizations (CASTRO, 2019). Recording a document, replying to an email or listening to a song on streaming are actions that are already done naturally nowadays, and that are possible from the evolution of ICTs, since all of this is done through Cloud Computing.



Allied to the security offered by the cloud, the Zero Trust concept appears, to improve the protection of users' sensitive data, as opposed to standard network security, which acts to stop possible threats coming from outside the network, which may occasionally leave data vulnerable, allowing data to be eventually stolen within that network. The basic principle of Zero Trust is to reinforce user authentication through the use of several layers of advanced access control, both for network devices and for servers that support such resources (ORACLE, 2022).

This scientific article was prepared based on extensive bibliographical research, aiming to answer the following question: how does Zero Trust provide greater security to network users? The objective of this study is to demonstrate the security advantages provided by Zero Trust, combined with Cloud Computing.

2. ON-PREMISE ENVIRONMENTS

Local environment or on-premise system is one that requires the acquisition and maintenance of licenses for its installation. It can be managed by the organization's internal team, requiring “upgrades and changes to the internal system without requiring internet access” (BRESSANIN, 2021).

Its operation requires the installation of a program on the company's servers and, depending on the format of the application, it must also be installed on each machine on an internal network. Such needs make its installation more timeconsuming, requiring the configuration of each of its modules on each machine on the company's internal network. Its installation is carried out by contracting service packages, which can be defined in advance, and tuned to each segment. Despite being a laborious and time-consuming process, the use of an on-premise system allows for several customization possibilities, an attractive aspect when the company “requires integration and development” (BRESSANIN, 2021).



When talking about corporate environments, with regard to the investments required for the installation and maintenance of the on-premise environment, and, considering the complexity and delay for its implementation, one of the possibilities is to adopt a model of computerized solution known as ERP System - Enterprise Resource Planning, which allows the optimization of all operational processes of the organization, allowing greater efficiency and productivity, in addition to cost reduction (BRESSANIN, 2021).

The ERP system was developed to support the management of organizational processes, including the areas of planning, sales, issuing invoices and financial controls (SALESFORCE, 2016). In addition to these functionalities, there are improvements in internal processes and the integration of activities in the various sectors, such as inventory and human resources. The use of ERP allows the integration of information on a single platform, making it more easily shareable, as well as all organizational communication that becomes lighter and more agile (TOTVS, 2022).

With regard to the costs required to implement an on-premise system supported by a management ERP, the initial investment is massive, as the following are required: specific equipment; acquisition of licenses for hardware and software, necessary for this system; hardware maintenance costs, in addition to the complexity and delay in its implementation (BRESSANIN, 2021).

In summary, Table 1 shows the evolution of the On-Premise system to Cloud Computing.

Table 1 - Evolution of Emerging Technologies, by company and business model

Decade	Emerging Technology	Company Paradigm (date of IPO*)	Business model



1960 - 1970	Mainframe	IBM	Vertical integration Hardware sales and leasing
1970 - 1980	Minicomputer	DEC HP	Sale of proprietary hardware and software, but incorporating third-party peripherals
1980 - 1990	Personal computer	Intel Apple (1980) Microsoft (1986)	Hardware as a commodity software licensing
1990 - 2000	Internet	Microsoft Netscape (1995)	Software licensing Access mechanisms (browser)
2000 - 2010	Web 2.0	Microsoft Amazon Google (2004)	Provision of search services, home banking, ecommerce, telecommunications, etc.
2010 -	Cloud computing	Google, Apple, Facebook	Advanced search services, social networks and targeted advertising
*IPO – Initial Public Offering			

Source: Tigre and Noronha (2013, p.116).

3. ARCHITECTURE FOR CLOUD COMPUTING

By definition, “cloud architecture is how individual technologies are integrated to create clouds. They are IT environments that abstract, pool and share scalable resources across a network” (REDHAT, 2019). Storing data in clouds means “migrating data, systems and applications to cloud architecture (...)”, and is currently considered a “major technological trend” (CLARANET, 1996-2002).

For Sousa, Moreira and Machado (2019, p.5) cloud computing basically offers three benefits to users of virtual networks: reducing infrastructure investments, which can be on demand or with heterogeneous resources; make this model more flexible in terms of hardware and software needs; provide ease and abstraction of access to its users.



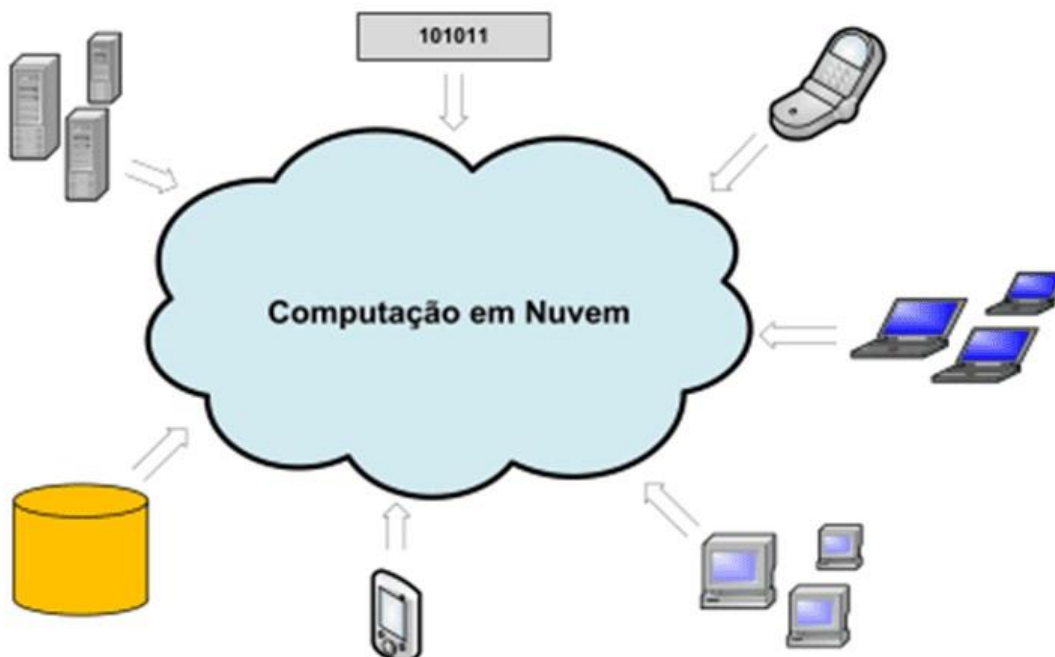
Pedrosa and Nogueira (2011) define cloud computing as an innovative model, allowing end users to access large amounts of content and solutions from anywhere, regardless of a specific platform.

In turn, Falcão e Silva (2021, p.101) refer that cloud computing emerged at the end of the 20th century, but became popular in the beginning of the 21st century, given the “evolution of virtualization technologies and wide availability through public cloud computing providers. In order to make IT systems viable, its proposal was to “facilitate and optimize the allocation of resources, generating financial savings and managerial efficiency of computational and human resources”. Thus, Cloud Computing also caused changes in the areas of Engineering and Software Architecture.

If in the previous phase numerous systems were developed with “monolithic architecture” deployed on a single server, the concept of cloud computing, reinforced by the subsequent evolution of different ICTs, allowed the creation of completely distributed systems, including the “architectural pattern of microservices”. With regard to “hosting systems in the cloud, due to the similarity of principles, such as ease and speed in the allocation and de-allocation of resources and services”, for example (FALCÃO and SILVA, 2021, p. 101-2)

Given the availability of all computing resources in the cloud, individuals now need to have only “an operating system, a browser and internet access” on their electronic devices (SOUSA et al., 2009, p.4). To this definition, we add the concept elaborated by TD Synnex (2022), when defining that “the researcher's objective was that the connection could be made from anywhere and that it was available at any time. Or, in another way, availability and accessibility”.

Figure 1 – Overview of a computing cloud



Source: Sousa, Moreira and Machado (2009, p.3).

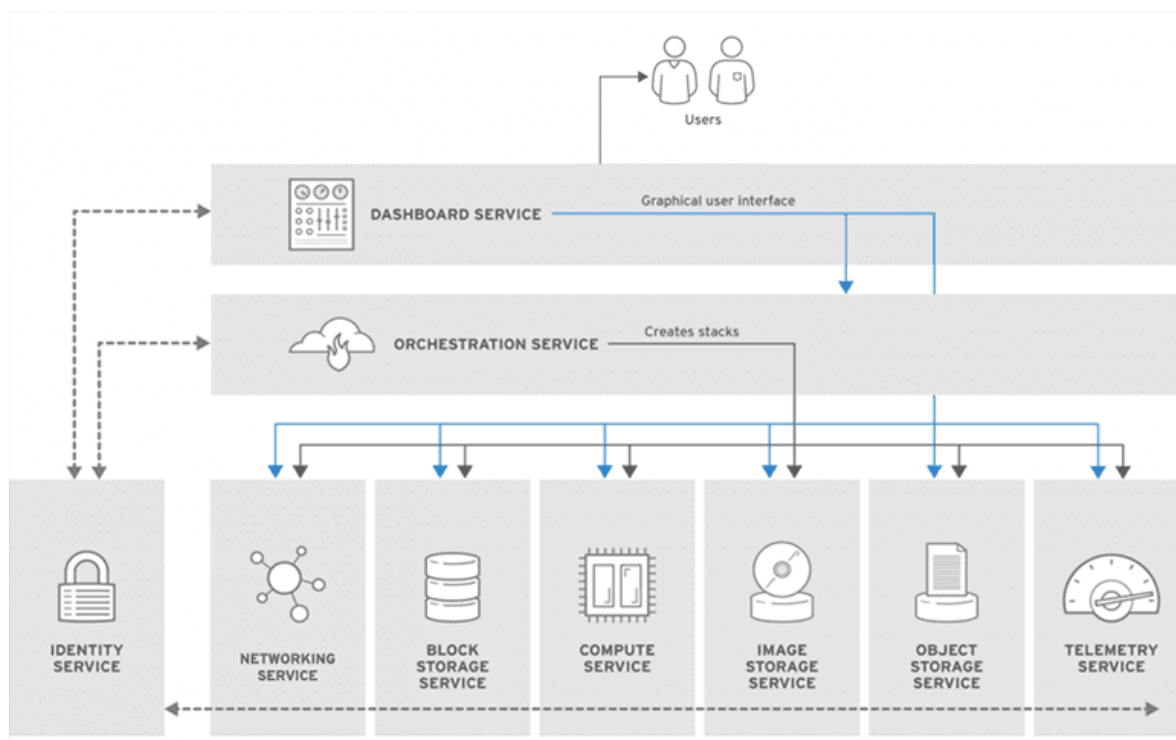
By analogy, one can mention the example given by Redhat (2019), when he says that thinking about security infrastructure is something similar to building a house, whose structure includes the necessary materials, such as bricks, sand, lime, cement, wood, brushes, paint, etc.; in this perspective, the structure of architecture would be the plan of the property under construction.

The above comparison allows us to state that the effective development of the cloud architecture requires the existence of “the necessary components and resources, which must be connected in order to allow the construction of an online platform on which the applications must be executed” (REDHAT, 2019).

It means that the cloud architecture can vary according to the needs to be developed; however, whatever the purpose of its installation, “automation, management, middleware and hardware software” will be required (REDHAT, 2019).

Another important aspect to highlight is the speed with which computational resources become obsolete, making the use of Cloud Computing an intelligent solution, as it uses third-party platforms; moreover, it is a more functional and economical solution, leading different users to the accesses of interest, without having greater technical knowledge in IT. It should also be said that such accesses are carried out on demand by interested parties (SOUSA et al., 2009).

Figure 2 - Composition of a basic cloud architecture



Source: Redhat (2019).

Cloud computing was developed to meet the demands of the IT area, also aiming to be a global resource in meeting the virtual needs of different types of users, that is, from “the end user who hosts his personal documents on the Internet to companies



that outsource the entire IT infrastructure to other companies” (SOUSA et al., 2009, p. 3)

Virtualization to abstract hardware resources into centrally managed data lakes is also used by cloud infrastructure. Other clouds known as bare-metal connect customers directly to hardware (REDHAT, 2019).

From a strategic and commercial point of view, there are important competitive advantages for organizations in adopting cloud architecture, including cost reduction and greater security of existing electronic data. In addition, “it allows workloads to be executed remotely over the internet, through the use of a commercial data center that uses the public cloud model” (CLARANET, 1996 - 2022).

By way of illustration, there are currently large public cloud providers, including Amazon Web Services (AWS), Microsoft Azure and Google Cloud. The most used in 2020 were: Alibaba Cloud / Oracle / IBM / Tencent Cloud / Amazon Web Services / Microsoft / Google (MONTEIRO and BORGES, 2021).

In a brief timeline obtained from the TD Synners portal (2022), one can observe the evolution of Cloud Computing in the interval between 1950 and 2000, which is similar to that already presented by Tigre and Noronha (2013):

- **1950:** The operating systems of organizations were developed on mainframes. They were expensive machines, and as such, there were only a few in each company;
- **1960:** The conception of the cloud concept begins. John McCarthy, considered the father of Artificial Intelligence (AI) launches the idea of Utility Computing, also creating Lisp programming;
- **1960:** Joseph C.R. Licklider collaborates with the development of the Advanced Research Projects and Agencies Network (ARPANET);



- **1990:** Part of the telecommunications companies create quality virtualized networks at low cost. The provision of shared access on the same physical infrastructure begins. In the same phase, access to technologies was popularized;
- **1997:** Professor Ramnath Chellapa uses the expression “cloud computing” for the first time in an academic lecture. This expression was inspired by the idea of “something that is in the air”, as is the case with the internet;
- **2000:** Cloud Computing technology gains strength when it starts to be offered for commercial use. At this stage, opportunities arise for companies and individuals offering their virtual computers for lease and streaming platforms, such as Amazon, Google, Microsoft Azure and Netflix. It is the provision of subscriptions to a set of services for storage, computing and human intelligence, based on the cloud.

The design of a cloud platform comprises some pillars that allow the design of the structure of the cloud architecture, as well as the computational resources of the hardware components (REDHAT, 2019).

In this sense, the existence of three platforms or pillars that are commonly used for the creation of cloud architecture stands out, platforms that provide greater efficiency to organizations, in addition to reducing their investments in local infrastructure, to highlight: PaaS, SaaS, IaaS (REDHAT, 2019; CLARANET, 1996-2022).

The PaaS pillar consists of a platform focused on cloud architecture that offers its users a layered IT infrastructure (REDHAT, 2019). It is a platform model also called a service platform, as it offers its users a “set of services aimed at developers, specifically” PaaS provides “tools, processes and APIs, which, when shared, cause the acceleration of application development, testing and deployment” (CLARANET, 1996-2022).



It should be mentioned that the Application Programming Interfaces (APIs) promote the connection between systems, software and applications, require a more in-depth development of the cloud architecture, which allows “the incorporation and containerization, orchestration, application programming interfaces (APIs), routing, security, management and automation software” (REDHAT, 2019).

In turn, the SaaS pillar is a service software distribution model, which allows integrated access to software applications from a given provider, that is, instead of being downloaded from a given location, it is hosted at a third-party provider and accessed by its users from the interface of a web browser, from any machine (CLARANET, 1996-2022).

The IaaS pillar consists of being a service structure, that is, a form of cloud computing where the hardware is provided and managed by external providers. Otherwise, it is hardware that can include virtual servers and even network connections; it is a virtual machine that allows companies to better scale their technological solutions (CLARANET, 1996-2022).

IaaS provides important advantages to its users: 1. scalability, which can be achieved through a subscription; enables access to IT systems at any time, quickly and efficiently, while reducing downtime; 2. reduced maintenance with hardware that precedes IaaS, generating savings in maintenance for companies; 3. ondemand access, which allows the reduction of costs related to its use (CLARANET, 1996 - 2022).

There are two cloud networks available. The public cloud, which crosses the physical space of organizations, being provided and operated by third parties. The private network, on the other hand, is installed within a business environment, that is, it functions as an intranet or data center, which consists of the necessary equipment for the IT area (CLARANET, 1996 - 2022).



4. COMPARISONS BETWEEN ON-PREMISE VS CLOUD COMPUTING

Cloud Computing is a type of internet access that allows users to store, manage and share data, software, applications and services on the internet, with practicality, agility and security (TD SYNEX, 2022). For Sousa, Moreira and Machado (2009, p.3), "cloud computing is a recent technology trend whose objective is to provide Information Technology (IT) services on demand with payment based on usage".

It is observed that the migration from standard environments to Cloud Computing has become as natural as necessary. In this perspective, the TI Inside portal (2022) reports that in December 2021 the multinational Accenture, specializing in information technology management and outsourcing, carried out an online study entitled "The great cloud mainframe migration: what banks need to know", about the intention of bankers to migrate their data still kept in mainframes to the cloud.

This survey had the participation of 150 IT and innovation executives from banks from 16 countries across five continents, including: Germany, Australia, Saudi Arabia, Brazil, Canada, China, Spain, USA, France, India, Italy, Japan, Mexico, Singapore, Sweden and the United Kingdom. Some have been found to be planning to move their core functions to the cloud, while others have already begun that process.

In practice, the economic, managerial and optimization advantages of human and physical resources have led most bankers to migrate their business functionalities, new products and applications to the cloud system. However, dependence on mainframes still persists, being common in some large companies, such as banks, with regard to customer records, payments, investments, risk and compliance, still persist (IT INSIDE, 2022).



It should be noted that the migration to the cloud of mobile and online banking services is already a reality in several banks, as well as the tools necessary for their employees to operate, such as e-mails and videoconferences that already operate in the cloud system. (IT INSIDE, 2022).

Among the percentages in which bankers are interested in the different aspects related to the migration from the on-premise system to the cloud, the following are considered: “speed and agility (43%); security (41%); ability to add new features (37%)”. However, there are risks that have been considered relevant to such a migration, such as: “business interruption; lack of understanding of how the code works; ability to attract and retain professionals specialized in IT, and the regulation of security and compliance risks” (IT INSIDE, 2022).

Added to Cloud Computing is the protection provided by Zero Trust, which includes actions aimed at leveling all aspects of security for millions of Internet users, based on the assumption that “nobody is trusted by default from inside or outside the network”. It is a network security model based on the idea of “never trust, always verify”, that is, it is a system that strives for the secure authentication and verification of a user seeking access (ORACLE, 2022).

The adoption of Zero Trust implies preventing the various vulnerabilities allowed by standard security methods, which act to stop threats coming from outside the network, through the use of firewalls, Virtual Private Networks” (VPNs), access controls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), SIEMs and email gateways. As criminals become more and more specialized, their skills allow the “violation of websites, applications or any electronic devices connected to the internet” (ORACLE, 2022).

To better visualize the aspects with the greatest impact on organizations' decisionmaking, tables 2, 3 and 4 are reproduced below, based on the indications offered by the Mandic Cloud Platform (MCP), which is dedicated to the automation



and integration of flows of different services and products, aimed at different business models (MANDIC, undated).

Table 2 – Comparison of Structural Aspects between the On-Premise Environment vs. cloud server

ON-PREMISE	CLOUD SERVER	MANAGED CLOUD SERVER
Customization and deployment on behalf of the company.	Possibility of increasing memory, processing, disk and bandwidth resources, when necessary.	Possibility of increasing memory, processing, disk and bandwidth resources, when necessary.
High-cost hardware that occupies a large space within the company.	Hardware outside the company.	Hardware outside the company.
Software license on behalf of the company.	Full control over server management and server root/admin access.	More time dedicated to the business, since you have a team of specialists working for your company.

Source: Mandic (no date).

Table 3 – Comparison of Operational Aspects between the On-Premise Environment vs. cloud server

ON-PREMISE	CLOUD SERVER	MANAGED CLOUD SERVER
Updating software and hardware on behalf of the company.	Constant updating of applications made available by the contractor; however, who does it is the operator of the contracting company.	Constant updating of applications, in terms of security operation.
The company has full control over the server. You can make changes and adjustments as you see fit.	Server control is the contracted company.	Server control is the contracted company.
Installation of applications and security strategies on behalf of the company.	You need technical knowledge to operate the server control panel.	With no need for technical knowledge, it facilitates the creation of websites and management of applications.
Personnel training on behalf of the company.	Provider's expert team.	Provider's expert team.
Bad downtime.	Guaranteed stability, with resources automatically reallocated in case of downtime.	Guaranteed stability, with resources automatically reallocated in case of downtime.
Support during business hours only.	Support 365x24x7	Support 365x24x7

Source: Mandic (no date).

Table 4 – Comparison of Financial Aspects between the On-Premise Environment vs. cloud server



ON-PREMISE	CLOUD SERVER	MANAGED CLOUD SERVER
<p>The company bears the costs of purchasing and licensing hardware and software.</p> <p>Cost also with the maintenance and updating of the same.</p> <p>Need to have specialized cloud technicians within the company or who can respond to any emergency, whatever the time of day.</p>	<p>The company pays for the hiring of a cloud provider and this one takes care of the maintenance of the infrastructure.</p> <p>The customer makes the necessary configurations in the cloud to run their applications and has to deal with possible problems at any time.</p>	<p>The company only pays for hiring a provider, which manages the infrastructure and necessary settings, being available at any time if there is a problem, without you having to worry.</p>
<p>Cost fluctuates according to monthly need.</p> <p>Software license and necessary licenses are also at the expense of the company.</p>	<p>Fixed monthly cost without the need to spend on software licenses.</p>	<p><i>Fixed monthly cost without the need to spend on software licenses. Fonte: Mandic (sem data).</i></p>

Source: Mandic (no date).

5. ZERO TRUST SECURITY MODEL

In 2010, John Kindervag, then vice president of Forrester Research, which is considered one of the world's leading cybersecurity experts, created the Zero Trust concept. Its objective was to put an end to the idea of a “trusted or unreliable network”, that is, that existing security models assumed that everything within a given network should be trusted, and that everyone who accessed it surfed responsibly (PALO ALTO, 2022).

It turns out that under the Zero Trust perspective, “trust is a vulnerability”. Another aspect that compromises the security of a network or system resides in the presumption about the fact that “a user's identity is not compromised and that all users act responsibly and are trustworthy”. Such aspects are related to the fact that



“once on the network, users – including threat actors and malicious insiders – are free to move laterally and access or transfer any data to which they have access” (PALO ALTO, 2022).

In turn, a definition obtained from the Oracle portal (2022) argues that Zero Trust is a network security model whose philosophy is based on the principle that no internet user and no device, inside or outside a company's network, can access a certain security system IT without being verified in several ways so that it can get your authentication.

Another way of conceptualizing Zero Trust is through another definition that is also known as security without a perimeter. It consists of “validating user identities, access rights associated with a specific system, and allows organizations to manage the digital identities of users, ensuring appropriate access” (ORACLE, 2022).

The adoption of several layers of advanced access control to access different network devices and/or servers allows the tracking of user activities, from the creation of reports on such activities, with the purpose of developing better policies of good practices (ORACLE, 2022).

According to the Palo Alto Networks Incorporation portal (2022), a multinational specialized in cybersecurity, some fragmented gateways can be related to Zero Trust, which will provide granular visibility of traffic, based on 7 layers of inspection and access control, that is, with granular Layer 7 policy.

This is the Kipling method, which covers the following aspects: “who”, “what”, “when”, “where”, “why” and “how” (PALO ALTO, 2022). This prevents unauthorized users from accessing the protected surface, which is only possible at Layer 7. This practice prevents unauthorized transfer of confidential data.



Among the factors covered by Zero Trust, there are several that deserve to be highlighted (PALO ALTO, 2022):

1. it does not mean making a system trustworthy, but rather removing the aspect of trust in the interactions between users and systems;
2. is a strategic initiative that helps prevent data breaches by removing the concept of trust from an organization's network architecture;
3. it is based on the principle of “never trust, always verify”;
4. aims to secure modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user access control;
5. this trust model continues to be related to misused credentials;
6. allows the identification of a “protection surface”. The protection surface is made up of the most important and valuable data, assets, applications and services on the network – DAAS (Desktop as a Service);
7. Protective surfaces are unique to each organization. Because it only contains what is most critical to an organization's operations, the protection surface is much smaller than the attack surface and can always be known;
8. once the protection surface is identified, you can identify how the traffic moves in the organization in relation to the protection surface, that is, understanding who the users are, what applications they are using and how they are connecting is the only way to determine and apply the policy that guarantees secure access to your data;
9. when understanding the interdependencies between DAAS, infrastructure, services and users, the controls must be placed as close as possible to the protection surface, creating a micro perimeter around the surface, which will move with the protection surface to where the user moves direct.

In turn, the Oracle portal (2022) lists the principles of Zero Trust architecture as defined by the National Institute of Standards and Technology (NIST):



1. all data sources and computing services are considered resources;
2. all communication is secure regardless of network location; network location does not imply trust;
3. access to individual enterprise resources is granted on a per-connection basis; trust in the requestor is assessed before access is granted;
4. access to resources is determined by policy, including the observable state of the user's identity and the requesting system, and may include other behavioral attributes;
5. the company ensures that all owned and associated systems are in the safest possible state and monitors the systems to ensure they remain in the safest possible state;
6. user authentication is dynamic and strictly enforced before access is allowed; this is a constant cycle of access, scanning and threat assessment, adaptation and ongoing authentication.

6. IMPORTANCE OF ZERO TRUST SECURITY FOR THE UNITED STATES

The existing insecurities in the protection of sensitive data of users of different systems and virtual networks are not new. There are reports that viruses emerged in the late 1970s, initially infecting drives or floppy disks (SANTOS, 2022). However, ten years later, cybercrime has exponentially projected its levels of dangerousness, reaching the present moment with different modalities and groups of criminals specialized in the virtual world, as shown in Table I. Table 1 – Emergence of Viruses and Malware between 1980 and 2012

Date	Type of Virus/Malware	History/Creator	Source of query
1982	Elk Cloner	It was the first massively used virus. It hit computers with the Apple II system.	Pimentel (2021)
1984	Core Wars	It was created at Bell Computers Laboratories. Stronger than previous viruses, it compromised the machines' RAM memory.	Pimentel (2021)



1985	Brain and Bouncing	Considered the first virus capable of infecting personal computers.	Pimentel (2021)
1989-1990	Trojan or <i>Cavalo de Troia</i> . Considered the first ransomware.	It was developed by Joseph Frank Popp. Its purpose was to infect computers. At first, it only affected the Windows platform. As it evolved, it began to reach the Apple, Android and Linux platforms, and at present, even smartwatches.	Pimentel (2021, p.34); Formasier (2020); Lema and Freitas (2021)
1992	Michelangelo virus	Created to be inactive and undetectable until March 6th, the artist's birthday, and from that date, it corrupted the files, overwriting random characters.	Pimentel (2021, p.3-4)
1999	Melissa virus	Created by David L. Smith, considered the first to employ social engineering to be spread, which occurs via email, starting from one of the victim's contacts.	Pimentel (2021, p.3-4)
2000	I love you virus	It infected millions of Windows users, including the Pentagon and the CIA. It spread via email, containing an attachment called Love-letter-for-you, which, when executed, relayed the message to all the user's contacts.	Pimentel (2021, p.3-4)
2005-2006		The company Trend Micro, in Russia, discovers malware that compresses and overwrites some types of files, causing data hijacking. The goal was to ask for data rescue.	Brito (2016)
2012		Spread of cases across Europe and North America	Brito (2016)

Source: Santos (2022, p. 138-9).

The serious attacks that took place from the 1990s onwards, carried out through highly improved malware, were transformed into ransomware, that is, new malware that block, kidnap and scramble personal and financial data on electronic devices, with the aim of objective of obtaining the ransom payment (LEMA and FREITAS, 2021, apud SANTOS, 2022).



In this perspective, it is worth describing the most recent invasions made against large North American companies.

In an article published by the Spanish newspaper El País, Saiz (2014) reports that in 2013 the protection of government data was a priority agenda of the Obama Administration, due to the fact that “incursions by computer hackers caused damages of 24 to 120 billion dollars (57 .9 to 289.5 billion reais) to companies in 2013, according to a report by the Center for Strategic and International Studies (CSIC)”. At the time, the Chinese army was blamed for this attack, both by the US government and by the media and multinational companies.

On May 9, 2021, the Colonial Pipeline, the largest North American pipeline, which distributes more than 2.5 million barrels of oil daily - a volume equivalent to 45% of the supply of diesel, gasoline and jet fuel on the US East Coast - was the victim of one of the biggest cyberattacks in the history of that country (BBC NEWS, 2021).

Still according to the BBC News portal (2021), “a group of hackers completely disconnected the network and stole more than 100 GB of information from the pipeline of the Colonial company”. The coup was attributed to the DarkSide hacker group, which infiltrated the network. Upon detecting the problem and, to defend its data system, the company shut down part of the systems to contain the threat, an action that temporarily interrupted all operations of that pipeline.

The fact led the US government to “decree a state of emergency in 17 states, in addition to suspending restrictions on fuel transport by road” until that occurrence normalizes (BBC NEWS, 2021). In this sense, Stracqualursi (2021) claims that, once again, the vulnerabilities of the country's infrastructure are evident.

In turn, in June 2021 it was the turn of JBS, a giant in the food industry, which had all its factories and pig farms installed in the United States affected by a large cyber



attack, on a commemorative day in that country. As a result, the price of beef rose exponentially (INFOMONEY, 2021).

To prevent the attack from affecting its entire system and data leakage, and also, in order to solve the replenishment as quickly as possible, in an unprecedented decision, JBS opted for the payment of a millionaire ransom, in the order of US\$ 11 million, contrary to all legal guidelines (G1, 2021).

As a result, President Joe Biden signed a new Executive Order (GUGELMIN, 2021) on cybersecurity, which described some requirements for the creation of new solutions, including (BBC NEWS, 2021):

1. that all companies providing security solutions to that government adopt the same standards;
2. that suppliers inform contracting bodies of any flaws identified in their systems;
3. that encryption and authentication technologies be adopted for the government in a short period of time;
4. creating a list of rules on how to react to future attacks.

With the recent war promoted by Russia against Ukraine, US authorities suggest that US companies and agencies remain vigilant against possible Russian cyberattacks (CNN BRASIL, 2022).

Gugelmin (2021) mentions some security specialists, consulted about the said Order, obtaining different opinions, shown in Table 2.

Table 2 – Expert Opinions on the New Executive Order for Data Security

Interviewed	Market Position	Evaluation	Suggestions
Several specialists	Not informed	They praised the decision for a new Executive Order; questioned its effectiveness.	-x-



Jeff Hudson	CEO of Venafi Inc., a private company specializing in cybersecurity, encrypted keys and digital certificates	He argues that preventive regulation of future attacks will be of no use, due to the fact that that government does not have the necessary speed to monitor software development.	Suggested that the security industry be encouraged to create more secure applications
Jyoti Bansal	CEO of Traceable and Harness	Agrees with Jeff Hudson.	Suggests that the application of new security decisions be adopted in the software creation cycle, and not when they are already being produced
Amit Yoran	CEO of Tenable and former officer at the Department of Homeland Security	Considers that a new Executive Order is a good start.	It reflects on the effectiveness of a single governmental or technological initiative having the power to prevent new attacks.

Source: Gugelmin (2021).

7. THE GOOD PRACTICES OF SAFETY ZERO TRUST

Among the best practices necessary for maximum confidence in security are aspects related to the evaluation, detection and means of preventing any type of fraud. The assessment is related to the existing system, allowing the implementation of correction plans; detection is related to access attempts outside the existing policy, and the identification of eventual anomalies when accessing data; preventing data access provides greater visibility of an organization's users and activities (ORACLE, 2022).

Thus, from the perspective of the Zero Trust model, the following model can be considered (ORACLE, 2020):

1. **Security as a priority design principles:** with security built in to reduce risk; isolated network virtualization; granular separation of responsibilities; least privilege access;



2. **Automated security:** to reduce complexity and avoid human error; automated threat mitigation and remediation;
3. **Continuous Security:** For seamless protection: ubiquitous encryption, enabled by default; continuous monitoring of user behaviors; context-aware adaptive authentication.

8. CONCLUSION

The reality of the facts obtained in the literature and presented throughout this article, combined with daily professional practices, allow me to issue some conclusions regarding evaluative aspects of data security.

There is a very significant evolution from the On-Premise environment to the Cloud Computing environment, both in terms of data accessibility, which is so necessary for users at any given time, and regardless of their physical location, as well as in terms of security measures. which aim to prevent the occurrence of criminal attacks and access to users' sensitive data.

This evolution arises with the advancement of information technology resources, combined with the high availability of data of interest to the user wherever and whenever needed.

Another way of analyzing the evolution of the On-Premise environment for Cloud Computing consists in the fact that such evolution takes place through new resource strategies, with the various possibilities for the file system architecture format and data access.

In addition to these specific aspects, there is another as important as those mentioned, which resides in the question regarding the investments necessary for cybersecurity, since Cloud Computing allows the optimization of the existing budget



for the IT area, in addition to guaranteeing business continuity, reconciled maintaining data privacy.

Finally, and no less relevant is the question of Zero Trust, whose objectives are pragmatic: to create real barriers to intruders regarding access to sensitive data of individuals, through the 7 layers of verification: “who, what, when, where, why and how”, beyond the seventh layer; eliminate the concept of responsible browsing by users, since its premise is “never trust, always verify”.

The adoption of Zero Trust also aims to prevent the occurrence of cyber attacks, instead of just stopping their occurrence; It also aims to prevent unauthorized access to and leakage of personal data, as well as to protect browsing environments and all systems involved.

REFERENCES

BBC NEWS BRASIL. **O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência**. Matéria publicada em 10 mai 2021. Disponível em: <https://www.bbc.com/portuguese/internacional-57055618>; acesso em 13 out 2022.

BRESSANIN, Lilian. **On Premises Vs Cloud**: a polarização no ambiente na nuvem. Artigo publicado em 03 ago 2021. Disponível em:

<https://www.selectsolucoes.com.br/2021/08/03/on-premises-vs-cloud-apolarizacao-do-ambiente-na-nuvem/>; acesso em 21 set 2022.

CASTRO, Klayton Rodrigues de. **Cloud.Jus**: Arquitetura de Nuvem Comunitária para Provisionamento de Infraestrutura como Serviço no Poder Judiciário da União. Dissertação de Mestrado Profissional em Computação Aplicada, apresentada à Universidade de Brasília (UnB). Brasília, 2019.

CLARANET. **Arquitetura em nuvem**: entenda o conceito do *cloud computing*. 1996-2022. Disponível em: <https://br.claranet.com/blog/arquitetura-em-nuvementenda-o-conceito-do-cloud-computing>; acesso em 14 set 2022.

CNN BRASIL. **FBI alerta para possíveis ataques de ransomware após sanções à Rússia**. Disponível em: <https://www.cnnbrasil.com.br/internacional/fbialerta-para>



possiveis-ataques-de-ransomware-apos-sancoes-a-russia/; acesso em 13 out 2022.

FALCÃO, Eduardo; SILVA, Matheus; SOUZA, Clenimar; BRITO, Andrey.

Autenticando aplicações nativas da nuvem com identidades. Capítulo 3. XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2021) p. 100-144. 2021. Disponível em: <https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/71/310/566-1?inline=1>; acesso em 14 set 2022.

GUGELMIN, Felipe. **Biden assina ordem executiva para combater ataques virtuais nos EUA.** Matéria publicada em 14 mai 2021. Disponível em: <https://canaltech.com.br/seguranca/biden-assina-ordem-executiva-para-combaterataques-virtuais-nos-eua-185034/>; acesso em 11 out 2022.

G1. **JBS diz que pagou US\$ 11 milhões em resgate a ataque hacker em operações nos EUA.** Matéria publicada em 09 jun 2021. Disponível em:

<https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoesem-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghhtml>; acesso em 13 out 2022.

IBM. **Soluções de segurança Zero Trust.** 2022. Disponível em: <https://www.ibm.com/br-pt/security/zero-trust>; acesso em 14 set 2022.

INFOMONEY. **Prejuízo do ataque hacker contra JBS se estendeu à indústria de alimentos dos EUA.** Matéria publicada em 11 jun 2021. Disponível em: <https://www.infomoney.com.br/mercados/prejuizo-do-ataque-hacker-contrajbs-seestendeu-a-industria-de-alimentos-dos-eua/>; acesso em 13 out 2022.

SANTOS, Levi Alves dos. **Os ataques ransomware e a camada de proteção em sistemas governamentais.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, Ed. 08, Vol. 04, pp. 132-161. Agosto de 2022. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware>, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/ataques-ransomware.

MANDIC – A Claranet Group Company. **On premise vs Cloud Computing.** Artigo sem data. Disponível em: <https://blog.mandic.com.br/artigos/on-premise-vs-cloudservers/>; acesso em 21 set 2022.

MONTEIRO, Matheus Antonio; BORGES, Leandro. **Viabilidade da arquitetura em nuvem para instituições educacionais.** Revista Eletrônica de Computação Aplicada, vol. 1, p.142-161.



ORACLE. **Modelo de segurança de confiança zero**. 2022. Disponível em: <https://www.oracle.com/br/security/what-is-zero-trust/>; acesso em 14 set 2022.

PALOALTO NETWORKS. **O que é arquitetura de Confiança Zero?** 2022. Disponível em: <https://www.paloaltonetworks.com.br/cyberpedia/what-is-a-zero-trust-architecture>; acesso em 14 set 2022.

PEDROSA, Paulo H. C.; NOGUEIRA, Tiago. **Computação em Nuvem**. Artigo publicado em 2011. Disponível em: <https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352120531-t2.pdf>

REDHAT. **O que é a arquitetura de nuvem?** Publicado em: 24 de junho de 2019. Disponível em: <https://www.redhat.com/pt-br/topics/cloud-computing/what-is-cloudarchitecture>; acesso em 14 set 2022.

SALESFORCE. **CRM ou ERP? CRM e ERP? Entenda a diferença**. Artigo publicado em 27 dez 2016. Disponível em: <https://www.salesforce.com/br/blog/2016/10/CRM-ou-ERP-Entenda-adiferenca.html>; acesso em 27 set 2022.

SAIZ, Eva. **Os EUA criam uma rede de segurança para proteger as empresas contra ataques cibernéticos**. Matéria publicada em 12 fev 2014. Disponível em: https://brasil.elpais.com/brasil/2014/02/12/internacional/1392230992_753620.html; acesso em 11 out 2022.

SANTOS, Levi Alves dos. **Os ataques ransomware e a camada de proteção em sistemas governamentais**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, ed. 08, vol. 04, pp. 132-161. Agosto de 2022. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware>, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/ataques-ransomware; acesso em 13 out 2022.

SOUSA, Flávio R. C.; MOREIRA, Leonardo O.; MACHADO, Javam C. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios. Cap. 7**. 1º Publicado no ERCEMAPI 2009. Todos os direitos reservados a EDUFPI. 2ª. versão. Setembro de 2010.

STRACQUALURSI, Verônica. **Ataque cibernético provoca fechamento de um dos principais oleodutos dos EUA**. Matéria publicada em 08 mai 2021. Disponível em: <https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-provoca-fechamento-de-um-dos-principais-oleodutos-dos-eua/>; acesso em 13 out 2022.



TD SYNnex. **Como surgiu a Cloud Computing?** 2022. Disponível em: <https://digital.br.synnex.com/bid/332223/como-surgiu-a-cloud-computing>; acesso em 30 set 2022.

TI INSIDE. **Cloud Computing. Em busca de velocidade, 4 em cada 5 bancos planejam ou já estão migrando mainframes para a nuvem.** 04 mai 2022. Disponível em: <https://tiinside.com.br/04/05/2022/em-busca-de-velocidade-4-em-cada-5-bancos-planejam-ou-ja-estao-migrando-mainframes-para-a-nuvem/>; acesso em 21 set 2022.

TIGRE, Paulo Bastos; NORONHA, Vitor Branco. **Do mainframe à nuvem: inovações, estrutura industrial e modelos de negócios nas tecnologias da informação e da comunicação.** R.Adm., São Paulo, vol.48, n.1, p.114-127, jan./fev./mar. 2013. Disponível em: <https://www.revistas.usp.br/rausp/article/view/55835>; acesso em 21 set 2022.

TOTVS. **O que é ERP?** Artigo publicado em 20 jul 2022. Disponível em: <https://www.totvs.com/blog/erp/o-que-e-erp/>; acesso em 27 set 2022.

Submitted: November, 2022.

Approved: November, 2022.

¹ Bachelor in Computer Science UNIB - Universidade Ibirapuera. Graduate: Specialization - Projects and Architectures in Cloud Computing - Anhanguera. Graduate: Specialization - Information Security and IT Management - Laureate – FMU. ORCID: 0000-0002-1645-6358.