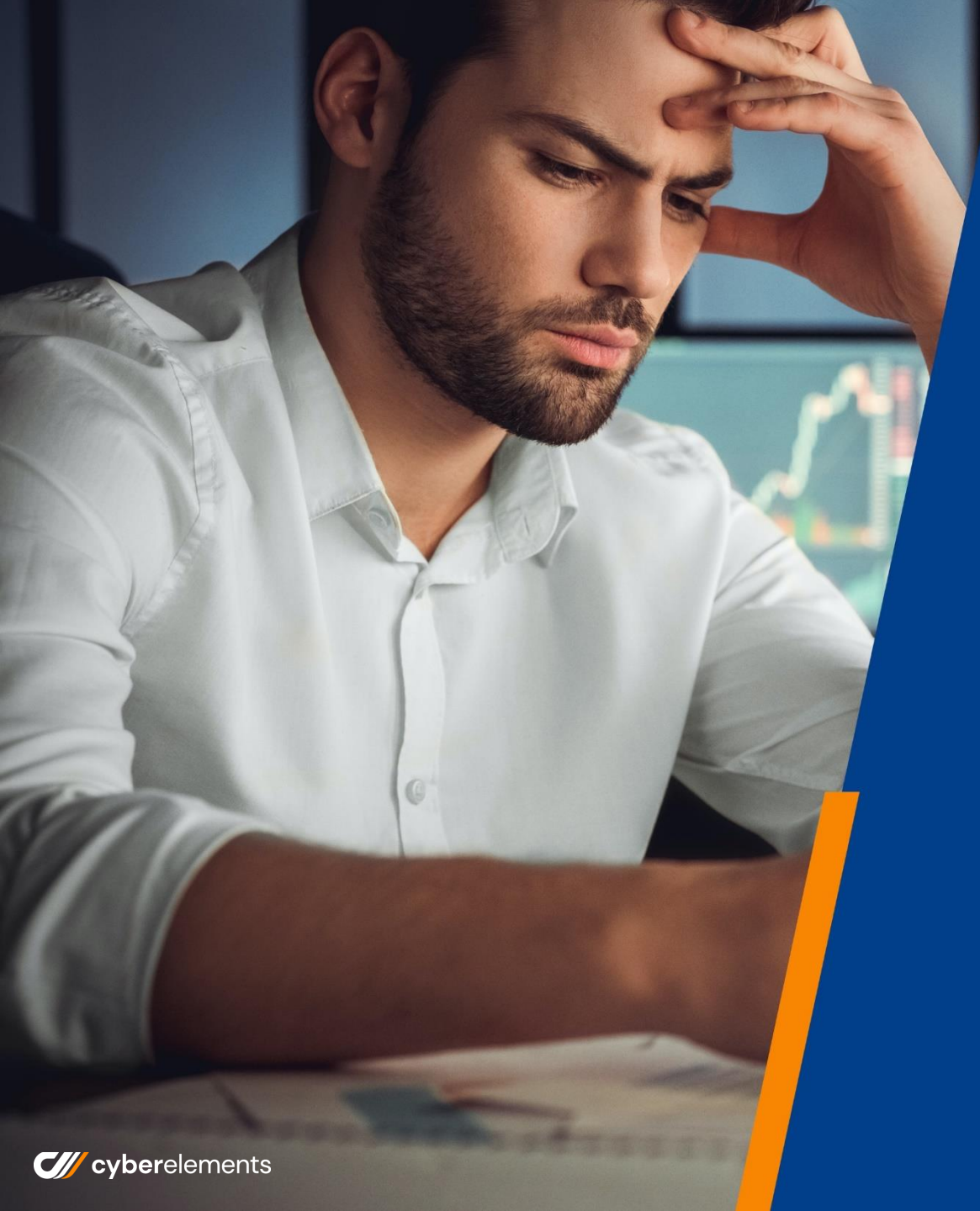

cyberelements

PAM : The 4 Main Issues of Service Provider Access

1

Do Not Trust your Service Providers Blindly

For several years we have been witnessing an increase in organizations outsourcing their IT management and providing service providers remote access to their IT resources.

This remote access is not without risks for companies: an Opus & Ponemon Institute study revealed that **59% of organizations have suffered a data leak caused by one of their providers.**

In order to counter these risks, which are becoming more and more prevalent for companies, the **deployment of solutions adapted to the challenges of provider access** is becoming an **imperative for the global security of information systems**.

Organizations must be able to control all remote access and not only that of their employees.

Control and Monitor Access to Service Providers with PAM (Privileged Access Management) **Solutions**

Monitoring Access and Administration Actions

PAM solutions allow organizations to **control and monitor the access and actions of privileged users** (including IT service providers), i.e., users with specific rights allowing them to access critical resources of the information system and to perform actions on these critical resources.

In concrete terms, PAM solutions allow monitoring the actions of all IT service providers when they connect (by name) to the administered network. These connections benefit from the **Zero Trust approach**, which provides only the strict access and network rights necessary to strongly limit the risks induced by this type of access. Any solution that avoids opening network ports and that is located at the application level (layer 7 of the OSI model) should therefore be preferred.

Session Recording

The actions of IT service providers are then **recorded in video format**, which allows the IT department of the outsourced company to **see in real-time** or to **review an intervention later**. To simplify the search for a specific action among all the recorded videos, the **advanced search** allows you to define the type of action to be found and thus display all the videos as well as the precise moment when this action is performed. The goal is to be able to quickly find the source of a compromise, an error, or a proof of action on the outsourced information system.

Moreover, to guide the IT manager in his review of sessions, a **vigilance score** is applied to each video so that he can identify at a glance the sessions containing sensitive actions that he will be able to control and watch with high priority.

2

Cyber Threat Is Strongest at the Perimeter

IT service providers need to access critical resources of outsourced companies.

This broad access to resources represents a threat of **malware propagation** if it is done via solutions that are not adapted to the criticality of the actions performed.

When the right solution is deployed, certain features or product specifications can **further reduce the cyber risks for the outsourced information system**.

Use a Solution Natively Designed for Remote Access

Native Connection Security

Since service provider access is essentially remote accesses, the PAM solution chosen must be capable of **natively securing connections**. This can be done, for example, via a **ZTNA** (Zero Trust Network Access) connection that only gives access to the resource being administered and not to the entire IS, and only when the resource is accessed, which limits the attack surface area from outside the organization.

Moreover, it is essential to **make the resources invisible from the Internet network while allowing access to them**: this is possible thanks to the URL rewriting technology. This architecture allows a **protocol break** via a double barrier mechanism with a component in the cloud and a component in the LAN of the organization: there is only one outgoing connection that is created without opening an incoming network port. Two secure tunnels are opened for the operation : a tunnel between the user endpoint and the cloud service and a tunnel between the cloud service and the gateway located in the LAN of the organization. The only component exposed externally is the component located in the cloud that does not allow access to administered resources on its own.

Agentless Access

This external access should not require the deployment of an agent on the workstation, not only to **simplify** secure access for service providers, but also to meet the need for **scalability** given the increase in remote access that companies must regularly deal with.

cyberelements

3

Is PAM too Technical and too Expensive?

Once a solution has been identified, the challenge is to **quickly deploy it** to protect an information system that is still at risk of data leakage or malware propagation resulting from provider access.

The use of a PAM solution as a public cloud service (**PAM as a Service**) responds to this imperative by allowing the solution to be **deployed in a few clicks.** This is done with minimal impact in terms of human resource allocation, both during the deployment and the administration of the solution, thanks to regular and automatic updates that are totally transparent for the IT department.

Benefit From the Flexibility of the Cloud

Simplicity and Speed of Deployment

PAM as a Service is the best approach to dealing with provider access monitoring for most organizations that do not have a PAM solution yet. The first advantage of PAM as a Service is its **simplicity and speed of deployment** as well as the **time savings** it provides **over the long term**. Most of the service is hosted as a cloud service, particularly for the user access portal, in order to guarantee access in complete security, including in external access situations.

Then, a gateway is deployed closer to the resources to secure the end-to-end connection. The gateway is then automatically referenced on the centralized server. Once the gateway or gateways are in place, no additional installation is required. **Updates** are then **automatic** and **totally transparent for the IT department**, which means that no human resources are required for tasks related to the management of the solution.

Financial Gain

PAM as a Service also has a financial benefit: **costs are distributed over time** according to the actual usage, whereas on-premise PAM requires a significant initial investment, sometimes incompatible with the budget allocated for IT. The maintenance and management of updates to the solution will also be a cost vector in the on-premise model. PAM as a Service ultimately allows a **better predictability of costs** and **spreads them over time**.

In order to optimize this financial benefit, it may also be wise to subscribe to a PAM solution offering **simultaneous user licensing**. For example, if a company has 10 privileged users (internal or external) but in practice no more than 5 of them are connected at the same time, only 5 licenses will be necessary, which limits the cost of the subscription.

4

Is PAM a Counter-Productive Constraint?

For companies, it is sometimes tempting to multiply cybersecurity tools to ensure that they are able to counter all threats. **However, this multiplication of cybersecurity solutions is counter-productive:** a study by IBM Security revealed that for organizations with more than 50 cybersecurity tools, the opportunity to detect cyberattacks drops by 8% and the opportunity to respond by 7% compared to companies with less than 50 cybersecurity solutions.

Another study by Trend Micro corroborates these observations, revealing that for employees working in cybersecurity operation centers, the excess of solutions leads instead to a series of negative effects. It includes a decrease of trust in the ability to prioritize and respond to numerous alerts and an increase in the time spent dealing with false positives.

To optimize the security of service provider access, and if the tool(s) chosen are adapted to these specific access, **the use of a reduced number of solutions is therefore essential** to guarantee the cyber resilience of the outsourced organization.

Offer Service Providers a Unified and Secure end-to-end Experience

Consolidate a Set of Functionalities

In order to improve operational efficiency, securing provider access must be achieved through the deployment of a **single solution** capable of consolidating a set of functionalities dedicated to the security of external access and the monitoring of privileged users. The chosen solution must therefore be able to authenticate providers by name via **MFA** and offer a **password vault** to protect the organization against password leaks from these providers and prevent non-identified connections.

The remote access of these providers must be secured, by applying the **principle of least privilege**, which consists of limiting their rights and authorizations on the information system to only those applications and data that are necessary within the framework and for the duration of their missions. The native integration of secure remote access such as **ZTNA** within the PAM solution is even essential when it comes to remote access by IT service providers.

The solution must be able to **trace and record all the actions of service providers** and allow the IT department to interrupt any action in real-time (automatically or via human intervention) if necessary. This means having total control over all the administration actions, which is the only way to truly control the security of the company's information system.

Ergonomics and Control of the Entire Provider Life Cycle

Since security often goes hand in hand with the ease of use, the use of an **HTML5 access portal** that does not require the deployment of an agent on the provider's workstation, as well as the provision of an intuitive administration platform for the IT department, are just as important as the features inherent in the PAM solution.

Finally, to ensure that former service providers who no longer operate on the IS no longer have any access to it, the PAM solution must offer an **account discovery** feature. This functionality allows, by scanning the administration network at regular intervals, to detect all administration accounts including **shadow admin** accounts and either to reintegrate them into the list of official accounts (and provide control and traceability mechanisms) or to delete them.

Monitor and Secure Administration actions on the IS

cyberelements

Cyberlements.io is the Zero-Trust and Identity-First access platform for business performance, allowing organizations to be better insured against cyberattacks without compromising workforce productivity.

It provides secure access and identity management capabilities, for both remote and on-site employees, third-party providers and industrial operators to access the business applications and privileged systems of the organization.

Start Free