WHITEPAPER

Domum

Access Anywhere

senhasegura®

Document Classification: Public

Índice

Introduction

In a service-outsourcing process or mass migration to remote work, employees and third parties need to have access to the internal resources of a corporate network in which they are providing services remotely. These working models brought new challenges to the security department of companies.

Zero Trust Environment

In the traditional security model, the architecture is based on the idea of a security perimeter in the organization, which must be protected by a firewall and VPN software like a castle surrounded by a moat. The purpose of this moat is to prevent unauthorized people and applications from gaining access to company resources by keeping them outside the castle. However, all users and applications that are inside the castle are considered “trusted” by default. Unfortunately, with so many users working remotely and so many assets, software, and hardware being placed in the cloud, relying on the perimeter approach alone is becoming less effective and riskier.

Excessive network access rights can be mistakenly granted via VPN, making them a top target for attackers

To get around this new dilemma, companies started to adopt the **Zero Trust** security model. The basic premise of this model is that no one should be trusted or given permission to access assets until the user or application is validated as legitimate and authorized; another basic premise is the least privilege principle. In addition, it selectively grants access to resources only as needed. And those who are granted access to the network, data, and other assets are constantly required to authenticate their identities.

The basic principles of Zero Trust are:

- **Grant the Least Possible Privileges.** First of all, everyone should have as few privileges as possible and gain new ones as needed.

- **Do not Trust, Always Check.** Within the Zero Trust security model, no user and device is trusted. Every new access to a system or request to access new data needs to come with some form of authentication so that the identity of the user and the device can be verified.

- **Always Monitor.** Finally, a Zero Trust security model requires constant monitoring and assessment of user activity, data access, network changes, and data changes. It is always best to check all actions taken within the organization's network infrastructure.

senhasegura Domum

senhasegura Domum is designed to provide privileged, fast, easy, and secure access for external vendors and privileged remote employees who need to access critical internal systems, which are managed by senhasegura.

senhasegura Domum is a cloud-based service that grants secure and temporary access to devices on a corporate network. It eliminates the need for VPNs, agents, or passwords, avoiding risks of lateral movement, configuration errors, and excessive exposure of the private network. Once authenticated, all privileged sessions are automatically logged for full auditing and monitored in real-time.

Features

Domum combines Zero Trust access, multi-factor authentication, just-in-time provisioning for external providers, and full integration with senhasegura PAM (Privileged Access Manager), for full visibility and auditing for administrators, in a single SaaS solution.

Highlights		
Zero Trust	No Agents	Least Privilege
Compromised user machines will not be a risk	Time-to-Value Reduction	Frictionless encryption

By requiring remote users to authenticate their identities, organizations are able to introduce a Zero Trust framework for remote users seeking access to critical assets being managed by senhasegura.

Security administrators can **grant** access to external providers for a specific amount of time and/or a specific number of sessions. This procedure **gives** external providers the minimum amount of access they need, while automatically de-provisioning access when it is no longer needed. This is a cornerstone of the new just-in-time concept.

Direct integration with senhasegura PAM ensures that all remote users, whether vendors or employees, are automatically using the secure point of control that isolates and logs their sessions whenever they need access.

Any information generated and used by the senhasegura Domum tool, such as logs and records referring to remote sessions used in the audit, are stored on the senhasegura server located in the client's environment and nothing is stored in the cloud environment

Below is a list of the main benefits of using the senhasegura Domum tool.

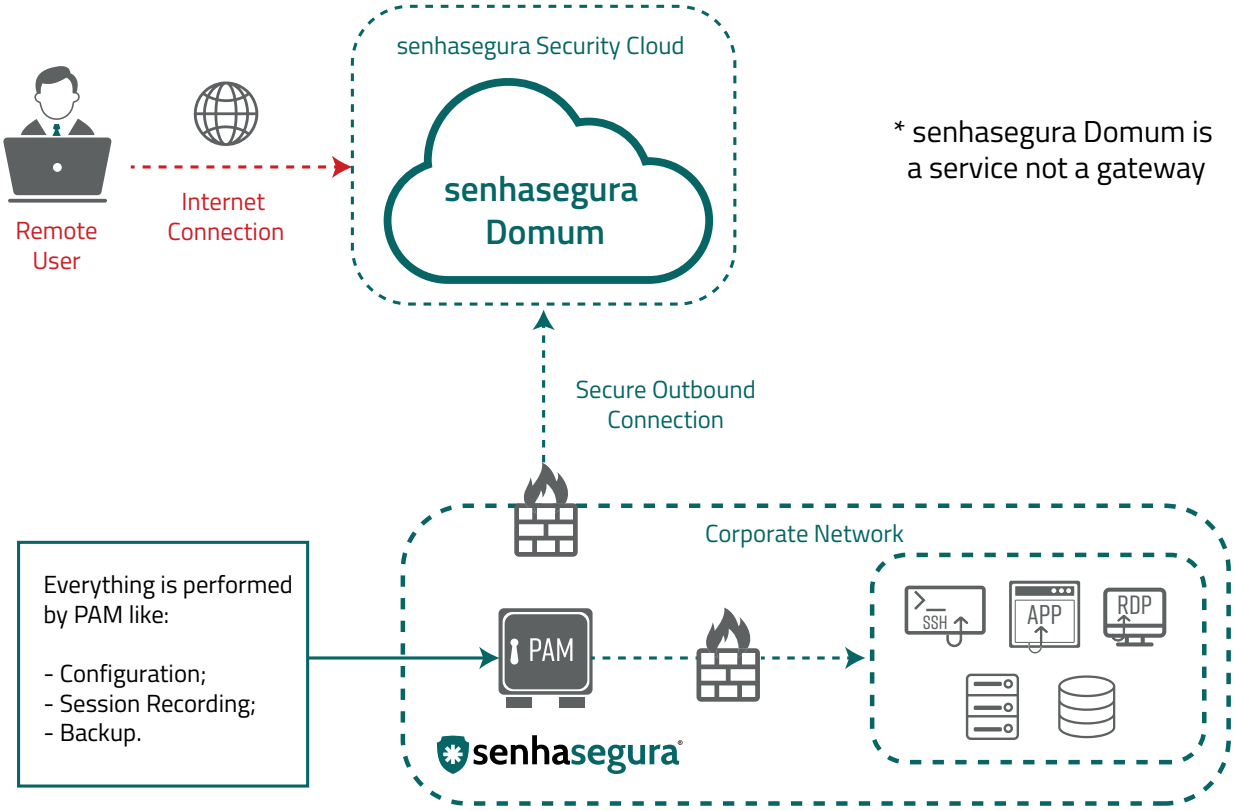
- **Full integration with senhasegura PAM.** The integration of senhasegura Domum with senhasegura PAM allows for centralized access management, in order to protect and control the use of impersonal and high-privilege credentials, providing secure storage, access segregation, and full traceability of the solution's use, as well as the possibility of giving access to remote devices temporarily.

- **Real-time Monitoring.** Every open session will be monitored and all information and logs generated by that session will be stored for future audits.

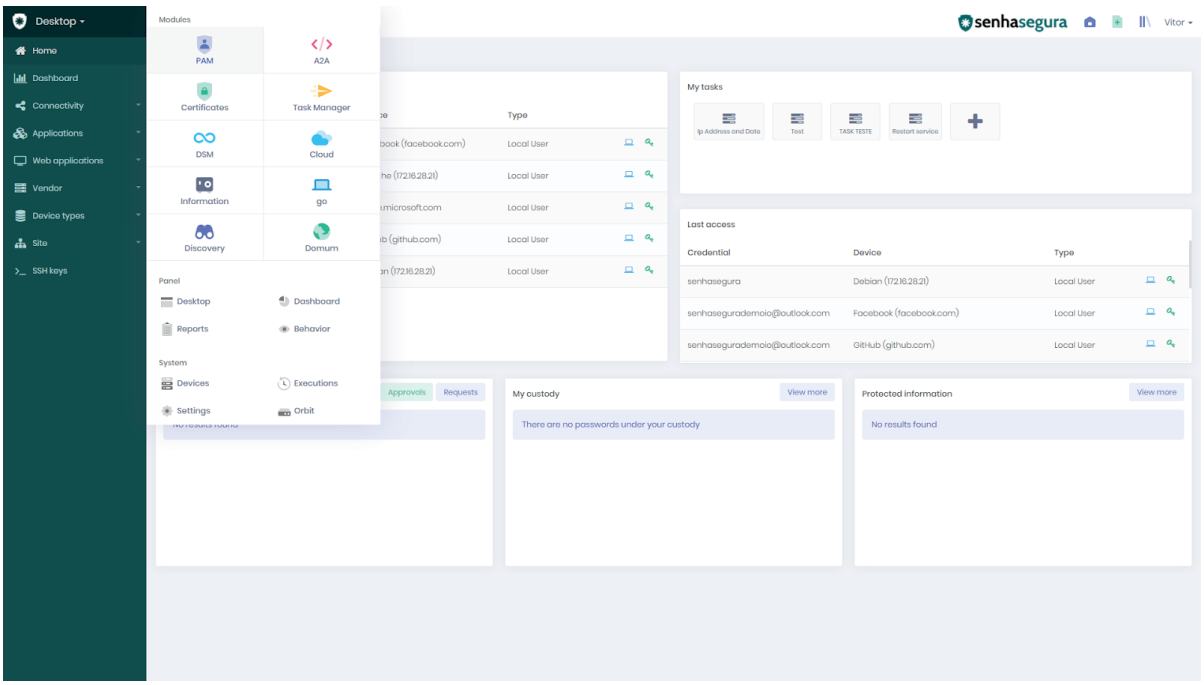
- **Defenses.** Use of Geolocation (Geofencing) and Behavioral Analysis (User Behavior) technologies to promote security in the client's environment.

- **Agentless.** You do not need administrator privileges on your workstation, just have access to a browser and you are good to go.

Process



Through the Domum web management console, one can define users who will have temporary access to credentials for remote login or password use. All cases may respect approval workflows and validation of explanations provided by the requesting user.



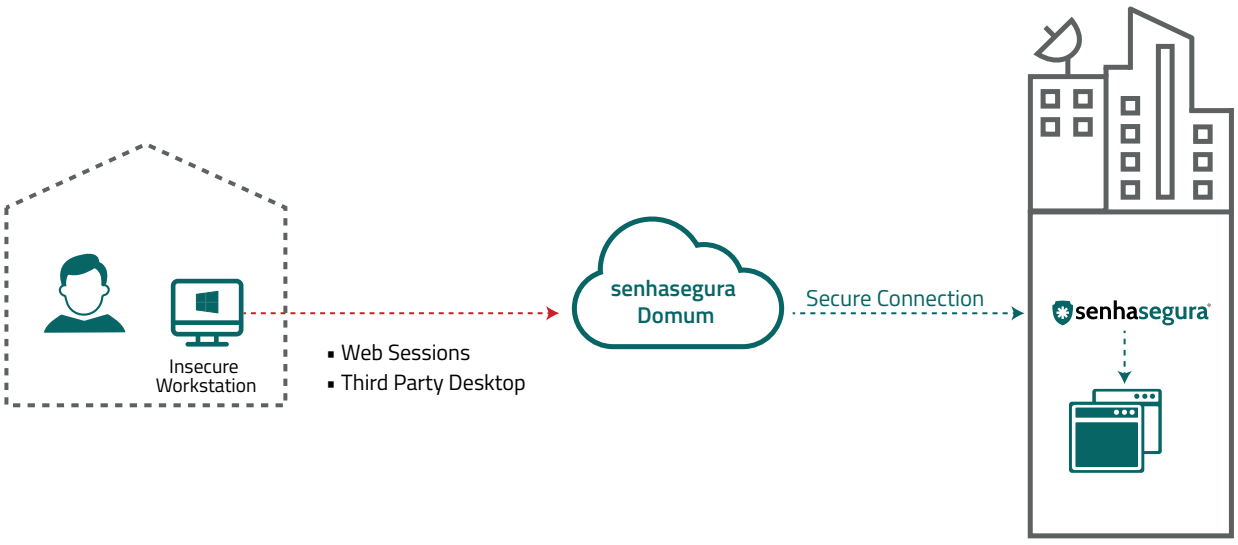
Remote User

The user will receive an invitation email sent by senhasegura Domum, containing a temporary personal link. When accessing the link for the first time, the user will receive a token via email or SMS to configure their authentication factor.

In a typical attack against a company's infrastructure, the end user's computer is the first to be exploited. From the moment the user's computer is compromised, all the trust relationships associated with it are explored - the so-called lateral movement. User IDs and passwords are the intended targets of attackers, as they will have access to other computers on the corporate network with this information.

The combination of the senhasegura Domum and senhasegura PAM tools prevent attackers from making this move, even if they somehow have access to improperly stored credentials in the location.

Domum Service



Connections are redirected to the Domum Service, whose main purpose is to encrypt the session between the user and the device on the corporate network. The Domum Service will translate the web protocol into RDP or web and secure protocol through the TLS protocol, TLS 1.2 - using ECC, RSA, or DSA encryption algorithms and SHA-2 hash algorithm.

In addition to encrypting connections, Domum Service has other features:

- **DDoS Prevention.** The Domum Service tool uses the Google GCP (Google Cloud Platform) cloud structure to prevent DDoS attacks.

- **senhasegura PAM.** Users will follow all security policies already present in senhasegura PAM, for example, restrictions, whether by day, time or location.

- **Single Point.** Only one connection will be opened between the Domum Service and senhasegura. With this, there is greater control and monitoring of traffic.

senhasegura PAM

The information entered by the user is validated in senhasegura PAM. Then the connection is redirected to the destination server.

With senhasegura PAM, administrators will be able to:

- Securely store device credentials and passwords;

- Segregate access based on user profile;
- Define groups for segregating access based on user profiles;
- Have flexibility in the approval process for access to privileged accounts;
- Have the possibility for more than one user to request access to the same privileged account;
- Have double custody of passwords to ensure more than one presence on access;
- Count on the integration with Help desk and Change Management tools;
- Change passwords by usage time or after viewing;
- Automatically change passwords on the main technological network platforms, servers, databases, web applications, and security equipment.

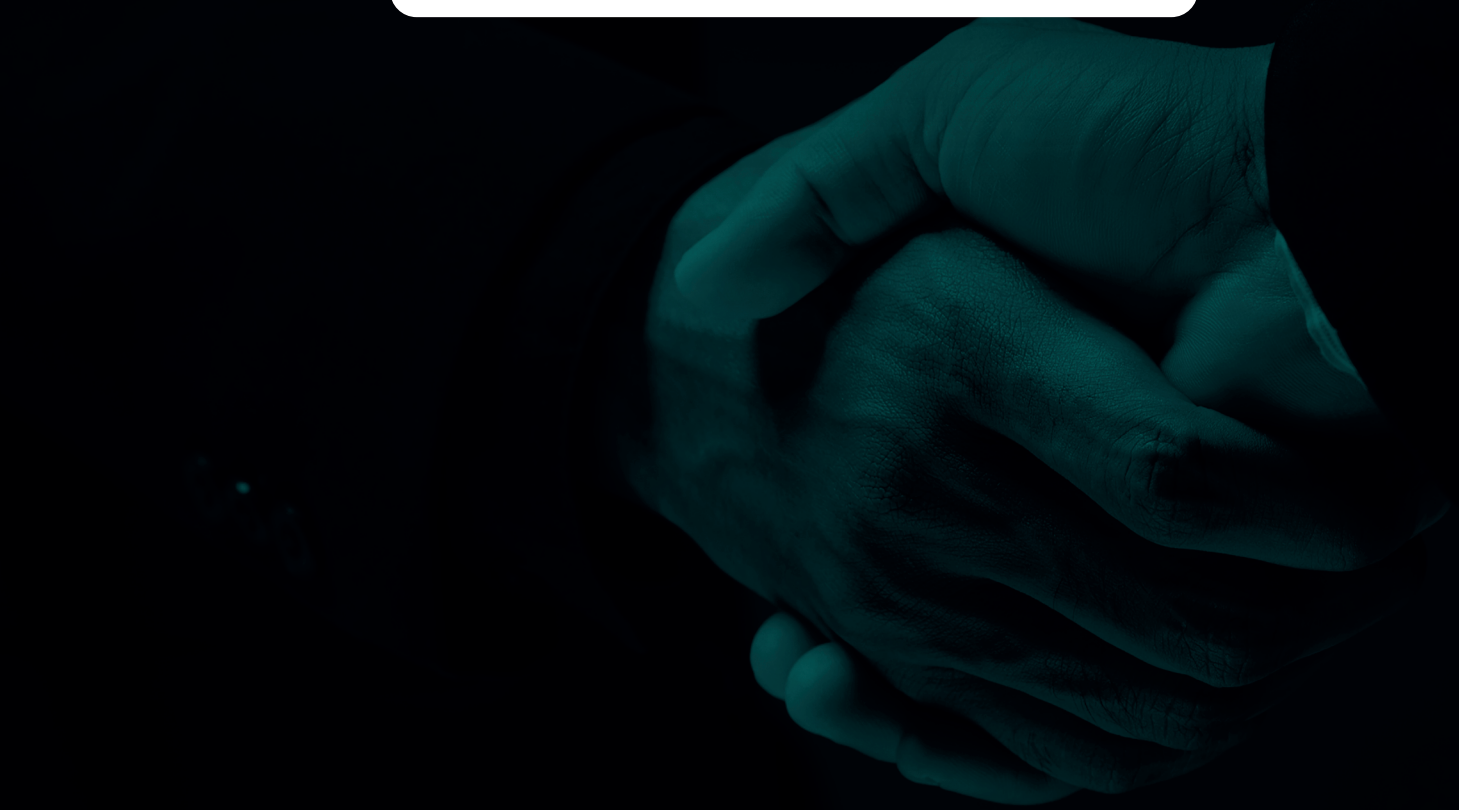
For greater integration between the environments, senhasegura PAM integrates with the main directory services for managing Access Groups and Profiles, and thus controls the use of credentials.

senhasegura PAM uses strong encryption standards (AES 256, SHA 256, RSA 2048 bits or higher, and FIPS 140-2), including the use of HSM devices.

We seek to ensure corporate sovereignty over-privileged actions and information. To do so, we work against data theft and through traceability of administrator actions on networks, servers, databases, and a multitude of devices. In addition, we seek compliance with auditing requirements and the most demanding standards, including PCI DSS, Sarbanes-Oxley, ISO 27001, and HIPAA.

For more information about senhasegura, visit the website: **www.senhasegura.com**

REQUEST A DEMO NOW



senhasegura®