Privileged Access Management
REMOTE ACCESS

wallix one

Secure access without VPN, without shared passwords, and without compromising security!

Most businesses rely on external service providers to perform remote tasks that require privileged access to their IT or OT network. Half of them do not have an inventory of third-party access to their network, have little or no visibility and control over their remote digital access. WALLIX One Remote Access helps meet the new access requirements for provisioning and enabling secure access to external service providers who need to access critical infrastructure managed by WALLIX One.

Features

End-to-end security

- Total segregation of the directory for external providers (Just-In-Time provisioning without adding identities to the corporate AD)
- Continued application of the corporate security policies
- Delegation of administration to business owners
- Self-service password reset (SSPR)
- No VPN to install and manage, no additional tickets for IT staff

Full visibility of external remote access

- Full visibility of external remote access
- Real-time creation of authorized access
- Unified web portal with integrated RDP & SSH web clients
- Control and transparency of third-party activity
- Compliance with the standards & recommendations of the French National Agency for Security and Information Technology (ANSSI) and business standards, security hygiene
- No shared passwords

wallix

Technical Characteristics

> **Federation Protocol**

- OpenID

> **Multi-Factor Authentication (MFA)**

- Authentication application OTP (WALLIX Authenticator, Google Authenticator, ...)
- Security Key FIDO (Yubikey, ...)

> **Self-service user portal**

- Registration of MFA authentication methods
- Self-Service Password Reset (SSPR)

How it Works

Step 1: the business manager, who has delegation of the WALLIX PAM admin, registers his third-party (Just-In-Time provisioning).

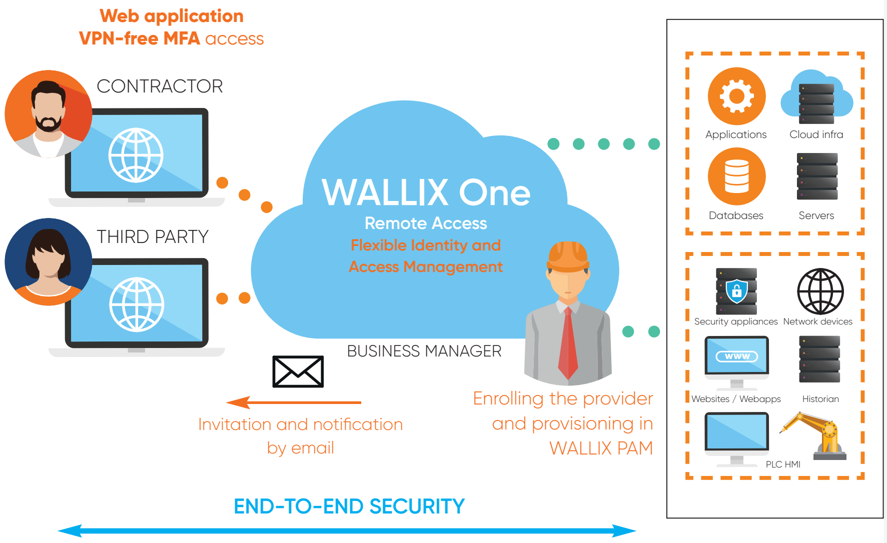
Step 2: the contractor is invited by e-mail and notified of his authorisation to access the company's internal infrastructure (IT or OT).

Step 3: the contractor registers the device he will use to provide his second authentication factor (TOTP, Yubikey) and then initiates his password.

Step 4: the contractor authenticates himself using his password and his second authentication factor.

Step 5: The contractor accesses a unified web portal to connect to corporate resources (RDP and SSH sessions) to perform the tasks assigned to him. Depending on the configuration of authorisations, access to resources can be subject to a request for approval and the approver can define the duration of the work assignment.

Step 6: From WALLIX PAM, it is then possible to replay and audit all external contractor sessions.



Benefits of SaaS

- Rapid Deployment
- Operational Efficiency
- Effective Scalability
- Automatic Updates and Maintenance
- Lower TCO

About WALLIX

WALLIX protects identities and access to IT infrastructure, applications, and data. Specializing in Privileged Access Management, WALLIX solutions ensure compliance with the latest IT security standards and protect against cyber-attacks, theft and data leaks linked to stolen credentials and elevated privileges.

Benefits

OPERATIONAL EFFICIENCY

- Optimisation of IT resources, and replacement of costly VPN solutions.
- Control over TCO (Total Cost of Ownership).
- Autonomy of the business teams without impact on their activity.

SECURE DIGITAL TRANSFORMATION

- Remotely launching sessions for third parties.
- Seamless user experience.

CONTRIBUTES TO ZERO TRUST ARCHITECTURE

- Provides Zero Trust Architecture compliant remote access: protects resources, assigns granular access rights and creates an audit trail.

WWW.WALLIX.COM

wallix