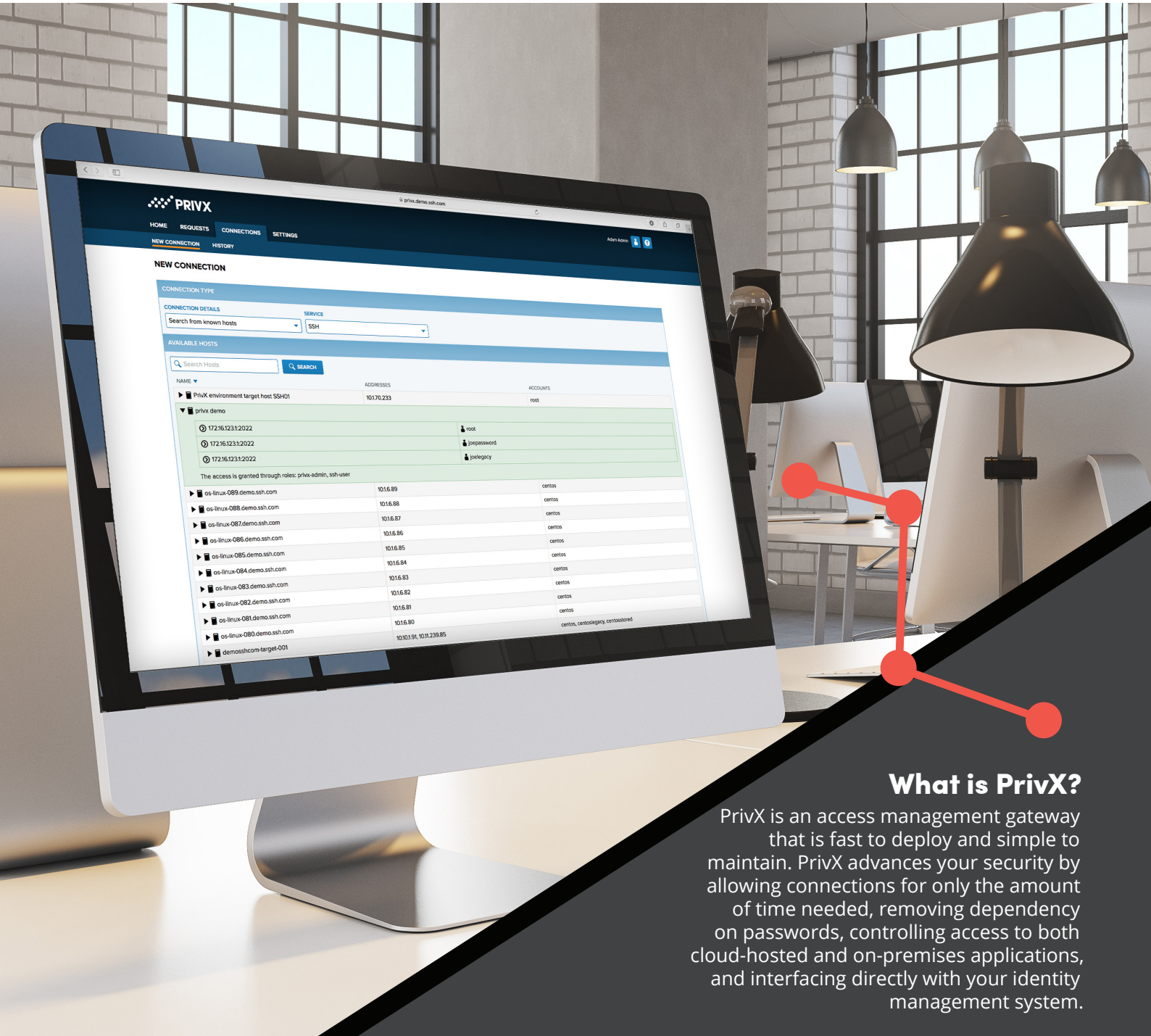
SSH.COM

PrivX® Datasheet

Zero Trust Access Management



What is PrivX?

PrivX is an access management gateway that is fast to deploy and simple to maintain. PrivX advances your security by allowing connections for only the amount of time needed, removing dependency on passwords, controlling access to both cloud-hosted and on-premises applications, and interfacing directly with your identity management system.

Your gateway from ground to cloud

Lean, fast and highly scalable

Light on its feet, PrivX provisions administrative access for just the duration needed – no permanent access and no passwords to handle. Quick integration with ID management systems, no agents to install, and nearly unlimited scalability.

- Integration with widely used ID data services
- No agents to install and maintain
- No passwords to vault, rotate and manage
- Scalable microservices architecture

Across hybrid and multi-cloud environments

Control and consolidate access to workloads in AWS, GCP, Azure, OpenStack and on-premises hosts from a single user interface.

Automated administrative access

Reduce errors and save time by connecting with existing AD/LDAP infrastructure, unifying user/role management and enabling SSO (single sign-on) logins. Set it and forget it – PrivX stays in sync and automatically discovers new hosts.

- Connect and stay in sync with existing AD/LDAPs and other ID data services
- SSO logins with multi-factor authentication (MFA)
- Automatic cloud host discovery

Privileged access re-imagined

PrivX stands apart from traditional privileged access management (PAM) tools by delivering a lean, cost effective solution. Compared to legacy PAMs, PrivX helps you to:

Cut the costs of password lifecycle management and vaulting by granting short-lived authentication to users only when they need it.

Economize on deployment and maintenance efforts by avoiding the use of agents on your client workstations and hosts.

Fortify your cost-saving cloud deployments by controlling access to your AWS, GCP and Azure-host servers, on-premises – or any combination.

How does PrivX work?

1. Identities automatically mapped from directory services. PrivX integrates with Microsoft AD, Azure AD, LDAP, Google G Suite, AWS Cognito and other OpenID Connect providers. User/group ID data is automatically updated as people join, move or leave. When you set up PrivX you define access to target hosts for each appropriate role (e.g. quality engineer, developer, sysadmin etc.) and map the roles to existing AD/LDAP user groups. Any change in your user directory is updated immediately in PrivX, so there's no separate privileged user directory.

2. Privileged access via ephemeral certificates. Users log in to PrivX via their browser using SSO/MFA and can see all their available hosts. They can then access their hosts in one click. It's "credentialess" because access is not granted by user passwords. This is possible because PrivX validates each secure SSH/RDP connection in real time with unique, short-lived certificates that are invisible to the user and automatically expire unless authorized by PrivX. There are no agents required on the client or host. PrivX acts as the only centralized certification authority for the target hosts. If required, native Mac and Linux SSH clients can be configured with PrivX Agent software.

3. Access elevation and 3rd parties. Privileged access elevations and access for non-directory users is managed via request/approval workflows with the option of 4-eyes authorization. Access for 3rd parties can be managed according to policies defined in PrivX and access can be granted or revoked instantly.

4. Monitor and audit connections. PrivX administrators can monitor and control the access lifecycle, including revocation and modification, down to granular access per host. SSH/RDP sessions can be recorded and played back with full audit log. Additionally, PrivX collects audit events which can be sent to SIEMs for behavioral, anomaly detection and other analysis.

5. Multi-cloud, private cloud or hybrid. PrivX admins have control over access to all on-premise and global cloud assets in one view. PrivX auto-discovers changes in your host environments. To integrate with standard software provisioning tools, like Chef and Ansible, PrivX provides deployment scripts. Users can then make SSH connections to target hosts according to your Ansible playbook via PrivX without the need for passwords. PrivX Extender software is also available to manage privileged access to VPCs (Virtual Private Clouds) via PrivX.

The problems that today's IT security professionals face

IT environments are increasingly complex and they require security tools that can be both expensive to deploy and burdensome to use and maintain. Below are a few examples.

Security is costly

Today's complex environments require enhanced security

Security tools can be a hurdle

PAMs are expensive to deploy and maintain

Traditional PAMs require heavy resources to deploy and manage. Tasks include installing and updating agents on workstations as well as vaulting and rotating passwords. PAMs can take months and even years to install, and some are abandoned before full deployment.

As workloads move to the cloud, security concerns rise

As organizations take advantage of the economy that cloud hosting offers, security concerns also mount. Chief among these is managing access to sensitive data that reside in the cloud.

People will find ways to avoid difficult systems

You need your access management tool to be easy so people will use it. Astute users can find ways to bypass heavier tools, like traditional PAMs.

Compliance can be burdensome

Meeting internal and regulatory requirements can be onerous. You need to demonstrate that your systems are under control and that unwarranted users are kept out of your servers.

Need to control access inside the network

Not only are insider attacks a threat, but the clever hacker who does gain access to your network can move among your systems if un-checked at access points. It's not enough to control your perimeter; you need to control access inside network.

Need to conserve resources

Your administrators have a lot on their plates. They need easy-to-use security tools so they can spend their time on more productive activities.

PrivX: A modern solution for modern problems

PrivX helps you solve your access management problems cost effectively, securely, and in a package that your administrators will find easy to use.

Ephemeral certificate-based authorization

Leave passwords in the dust by using just-in-time, temporary access to target hosts. Reduce your threat surface, and the money you spend on credential lifecycle management.

Agentless*

Benefit from fast deployment by avoiding the need to install traditional agents on client workstations and/or host servers.

You'll also be more likely to stay current with PrivX's version updates when you only need to centrally update your software.

Integration with existing IMS/IAM

Economizing on time and effort, PrivX stays in sync with the role-based users in your identity management system. Employees come and go and change roles, while PrivX stays up to date.

Expedite access to target hosts with SSO; users log in once and gain one-click entry.

Recorded sessions with playback

Make easy work of preparing for audits, as well as post-event forensics. All access traffic is recorded and stored for review. PrivX collects audit events which can be sent to SIEMs for user and entity behavior analytics (UEBA). and other analysis.

Hybrid and multi-cloud support

PrivX manages access to target hosts whether they're in AWS, Azure, GCP cloud environments, or all three as well as private cloud and on-premises.

Microservices architecture for scalability and high availability

PrivX lets you easily add instances as your needs grow, while also providing high availability for disaster recovery. Your multiple, distributed PrivX instances can be dispatched through a common load balancer and connected to a backend database to run as a unified, highly available system.

*Available as agentless or with agents.

FEATURES	
Role-based access control to target hosts	Short-lived certificate-based authentication Users can be dynamically mapped to roles View hosts that are accessible by specific roles
Directory service integration	Users and groups synced with Microsoft AD, Azure AD via Graph API, Google G Suite, LDAP and OpenID Connect providers (e.g. AWS Cognito, Okta, Ubisecure)
Sign-in and access control to PrivX	• Single sign on (SSO) through directory services applications via Kerberos • Username & password for local users • Multi-factor authentication (MFA), time-based one-time password (TOTP) • OAuth2 over TLS
Authentication to target hosts	• OpenSSH certificate • Virtual Smart Card for RDP • Stored, vaulted credentials • Username & password
Supported protocols	SSH (v2), RDP, HTTP(S) and SFTP
Fast and responsive user experience	HTML5 single page UI over REST APIs
Complete HTTP REST API	Anything the UI does can be executed via the API
Host and user searches	Capable of indexing tens of thousands of hosts and users from multiple sources
Support for cloud providers	Automatically scan and add tagged cloud hosts: AWS, Google Cloud, OpenStack, Azure
Support for virtual private clouds (VPCs)	Connect to VPC using PrivX Extender (reverse proxy)
Standalone product	Includes internal user & host directories Includes a mechanism for requesting roles & approving them with email notifications

PERFORMANCE	
Capacity	100 000 users mapped to roles 10 000 target hosts
Concurrent connections	10 000 SSH, 60 new RSA connections per second 200 RDP connections Tested on a 3.6GHz 8-core server with 16 GB of RAM, scales horizontally as needed

TARGET HOST REQUIREMENTS	
Certificate-based authentication	OpenSSH 5.6 or later
Certificate-based authentication with AuthorizedPrincipalsCommand script	OpenSSH 6.9 or later

PRIVX INSTANCE	
Compatible operating systems	Red Hat Enterprise Linux 7.4 or later CentOS 7.4 or later

HARDWARE REQUIREMENTS

Evaluation/trial license (<10k users)	Recommended minimum: 4GB RAM, 2 core CPU, 15GB disk space
Production license (<100k users)	Recommended minimum: 8GB RAM, 8 core CPU, 100GB disk space

DEPLOYMENT

High availability and scaling	• High availability through active-active cluster nodes • Horizontal scaling by adding nodes • Load balancing with sticky-session support
Installation	Download and upgrade PrivX from GPG-signed RPM repositories
Management	• Web-based admin UI • HTTP REST API • API end point status and service status page
SSH target host configuration	All OpenSSH compatible hosts supported. Automated deployment scripts provided: CentOS, RedHat, Ubuntu, Debian, Amazon Linux.
Automated deployment	Compatible with Ansible and Chef automated deployment tools

For detailed information on deployment and requirements, please refer to the Administrator Manual here.

AUDITING

Audit events persisted to log files	All user and admin actions are persisted to log files and can be automatically directed to SIEM
Connection manager	View past and ongoing connections Terminate ongoing connections
Record and playback sessions	Record browser-based SSH and RDP connections. Store encrypted audit trails in your preferred location.

SECURITY

System security	• Communication between service components and PrivX secured via TLS • Information stored in the vault encrypted with AES128 or AES256 GCM • PrivX secrets can be secured using hardware security modules (HSMs)
Alerts and reports	System and connection-based alerts collected and sent to SIEMs (e.g., Splunk, IBM Qradar), AWS CloudWatch or Azure Event Hubs

SSH Communications Security Oyj

Kornetintie 3, 00380 Helsinki

www.ssh.com

+358 20 500 7000

info.fi@ssh.com