Centrify Cloud Suite

Govern and Control Access to your Cloud- or Multi Cloud-Hosted IT Infrastructure

Digital transformation is changing the enterprise landscape, creating increased complexity as organizations leverage emerging technologies such as the cloud, big data, DevOps tools, containers, microservices, and more. As organizations modernize their IT estates and expand infrastructure from the data center to the cloud, they are faced with an exponential increase in identities and attack surfaces that challenges their ability to modernize their Privileged Access Management in response.

Cloud Migration is Forcing a Security Rethink

Leading up to 2020, many organizations were already seeing the cost, flexibility, scalability, and availability benefits of the public cloud as a transformative game-changer. As a result of the COVID-19 pandemic that shifted entire workforces remote, the cloud has, more than ever, become a must-have.

But this rapid transition to the cloud has also resulted in confusion. Whose responsibility is it to secure workloads in the cloud? How do we centrally manage siloed, fragmented identities across hybrid and multi-cloud enterprise infrastructures? How do we manage the risks associated with an exponential increase in identities and attack surfaces?

The short answer for most organizations is, not easily without a Privileged Access Management (PAM) solution that is purpose-built to address these concerns.

Why Not Retrofit Legacy PAM Solutions?

Designed for on-premises infrastructure, where policy management and policy enforcement controls are on the same network, traditional PAM solutions can't easily accommodate a decentralized architecture with control points in multiple VPCs/VNets and across multiple cloud providers.

Being ephemeral in nature, cloud infrastructure exposes new attack surfaces, as the number of machine identities explodes.

It may be attractive to try to retrofit the PAM solution you've used for years. Unfortunately, the pain of the consequences of that decision can be significant:

- **Security impact:** having two separate PAM stacks, one for on-premises, the other for cloud; new attack surfaces; an explosion of identities for machines and workloads vs. human admins; inability to enforce multi-factor authentication (MFA) for all administrative access control points; and having to use local accounts for the login to cloud instances.
- **Cost impact:** replicating infrastructure to the cloud (e.g., PAM stack and Active Directory domain controllers); licenses and education for new tools to fill security gaps; CapEx vs. OpEx.
- **Productivity impact:** managing new identity silos; re-architecting PAM to handle distributed workloads; expanding the PAM footprint and replicating PAM infrastructure in the cloud; managing and operating PAM software and supporting infrastructure; extending on-premises directories to the cloud for enterprise account login; automation and integrating into development pipeline

Modern PAM-as-a-Service

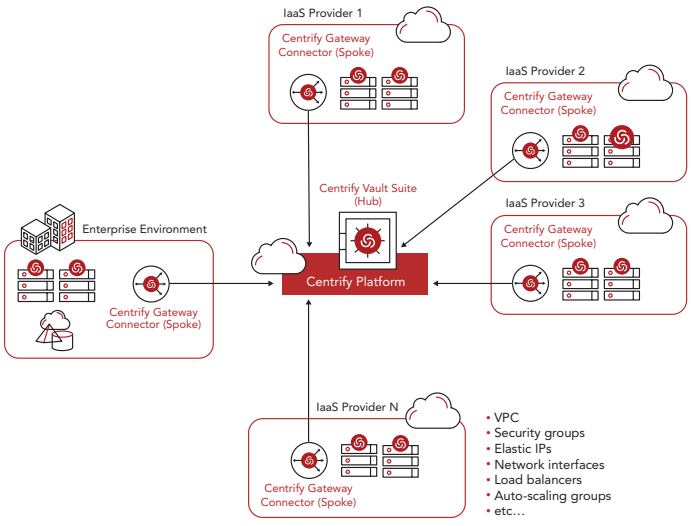
When migrating IT environments and workloads, it is essential to enforce a consistent privileged access security model across public cloud and on-premises infrastructure. Built for the cloud from the ground up, Centrify Cloud Suite achieves this goal, leveraging key benefits of the cloud economy such as elasticity and multi-tenancy. It can easily accommodate the most demanding and complicated multi-cloud architectures, delivering on simplicity, flexibility, and efficiency.

By offering PAM-as-a-Service, our cloud-ready solution can be up and running in under an hour. Customers avoid a complicated and protracted IT project to deploy PAM software and supporting infrastructure on-premises and the ongoing cost to operate and routinely update it.

Hub-and-Spoke SaaS Architecture Designed for Hybrid IT

Centrify Cloud Suite's hub-and-spoke architecture makes scaling out your PAM infrastructure simple and quick. A Centrify Platform SaaS tenant acts as your hub for shared services and centralized policy management. Lightweight Gateway Connector spokes deploy in minutes into your infrastructure, linking it to the Centrify Platform.

For example, if you spin up a new development project in its own VPC or VNet in AWS or Azure, simply drop in a Centrify Gateway Connector, enroll it in the Centrify Platform, and you can now centrally manage and control access to new virtual instances and containers. You avoid the hassles of a traditional PAM product that requires you to obtain and build-out supporting infrastructure and that depends on complicated vault synchronizations, failover, and disaster recovery.



Leverage the Power of Centrify's Client

Installing a lightweight Centrify Client on managed systems gives you powerful, extended PAM capabilities. Centrify Clients enroll the machine into the Centrify Platform to take advantage of client-based shared services: multi-directory brokering, MFA at login, **Delegated Machine Credentials, and remote login via SSH and RDP clients.**

Multi-directory brokering will permit your admins to log in to IT servers, no matter where the servers or authoritative directories live.

Digital transformation projects often result in the enterprise directory (such as Active Directory or LDAP) remaining on-premises while IT or DevOps stands up new servers in private virtual clouds with no external Internet access. IT can bridge this separation with site-to-site VPNs for every VPC/VNet, in every IaaS cloud. Or perhaps standing up new LDAP servers or Active Directory domain controllers in the cloud, configuring trust relationships and new firewall ports for communication. These fixes are cost prohibitive, add complexity, reduce operational efficiency, and increase your risk.

Alternatively, the SaaS-based Centrify Platform has visibility into all managed resources as well as your enterprise directories — even cloud directories such as Google Cloud Directory. This brokered authentication service enables a Centrify Client on a host machine to validate the users' credentials with the Centrify Platform on its behalf. Net-net, as an administrator, you can now log in to any Windows, Linux, or UNIX server using your AD credentials and as IT manager, you don't have to directly join the server to a domain.

MFA at login is an essential layer of security to protect access to critical IT systems. More standards and regulations such as PCI-DSS are making this a requirement when logging in to systems that contain sensitive information, such as credit card data.

MFA at login is enforced by the Centrify Client, relying on the Centrify Platform to handle the various built-in and third-party authenticators (please see the Centrify Platform data sheet for more details).

Centrify designed **Delegated Machine Credentials** to address major challenges for DevOps. When applications and microservices need to retrieve configuration data and account passwords from an enterprise vault, they first need to log in to the vault. Thus, they each need a service account and password and a way to securely store them to avoid compromise. As the number of applications and microservices grows — often into the thousands — so does your attack surface due to the proliferation of these service accounts and passwords.

With Centrify, only the machine requires a service account — a machine identity. The machine can then authenticate to the vault on behalf of workloads running on the machine, obtaining a scoped OAuth2 bearer token for the workload to consume vault services. This essentially reduces the attack surface to zero.

Centrify Cloud Suite enables administrators to **log in to infrastructure servers using their familiar SSH or RDP client**, without needing a VPN connection. Even for hosted server instances in private virtual clouds with no public-facing IP address, the login process is familiar and streamlined. Centrify Cloud Suite achieves this because of its SaaS and hub-and-spoke architecture.

Centrify Server Suite or Centrify Cloud Suite?

Both solutions aim for feature parity, however, there are three common deployment scenarios to consider when deciding which — or both — to deploy.

If your IT infrastructure is on-premises, in a private cloud, or both; if you are heavily dependent on AD and comfortable using AD as a centralized policy management platform for Windows, Linux, and UNIX systems; then Centrify Server Suite is likely your best choice. Note that with infrastructure in both places, to enable admins to use their AD credentials to log in everywhere, you will need to ensure AD is visible to both, by (for example) installing a site-to-site VPN or replicating AD infrastructure such as a read-only domain controller (DC) with a 1-way trust.

If your infrastructure is cloud-hosted; If you're not AD-centric or use AD for enterprise user accounts but don't wish to use AD for centralized PAM policy management; then Centrify Cloud Suite is likely your best choice. It leverages the SaaS-based Centrify Platform to manage policies, with no AD dependence at all. Note that if your users are in AD, they can still log into any managed system with their AD account — multi-directory brokering has you covered without needing to set up a connection between the cloud instances and your DCs or replicating DCs in the cloud.

Finally, you may prefer both if, for example, you have separate teams managing each. Note that this results in policies in two places — AD and the Cloud Platform. However, since Cloud Suite roles can contain AD groups as members, you can manage role-based access for both environments from AD purely by manipulating AD group membership.

Note that Centrify's Systems Engineers will be happy to discuss this and explore the best option for you and your business.

Whether your IT infrastructure lives exclusively in the cloud, or whether you are migrating on-premises infrastructure for a hybrid approach, you need the most advanced, cloud-native PAM technologies to protect that infrastructure from identity-centric data breach.

Ready to Protect Against the #1 Attack Vector?

Register for a 30-day trial of Centrify's Privileged Access Management (PAM) software to minimize your attack surface and control privileged access to your hybrid environment.

Centrify enables digital transformation at scale, modernizing how organizations secure privileged access across hybrid- and multi-cloud environments by allowing human and machine identities to seamlessly log in and granting least privilege just-in-time, increasing accountability, and reducing administrative access risk.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +65 9788 2594
Brazil +55 11 3958 4876
Latin America +1 305 900 5354

sales@centrify.com

www.centrify.com