DISCOVER IDENTITY-CENTRIC PAM

Emerging technologies are reshaping our world. A good example is the cloud. Organizations are increasingly moving their workloads to the cloud to achieve greater agility, flexibility, and cost savings. Spending on cloud infrastructure services is projected to grow from an estimated $50 billion in 2020 to $74.1 billion through 2022 according to Gartner[1].

Many describe this overall trend as digital transformation — to rethink old operating models, to experiment more, to become more agile in your ability to respond to customers and rivals — with new, modern technologies.

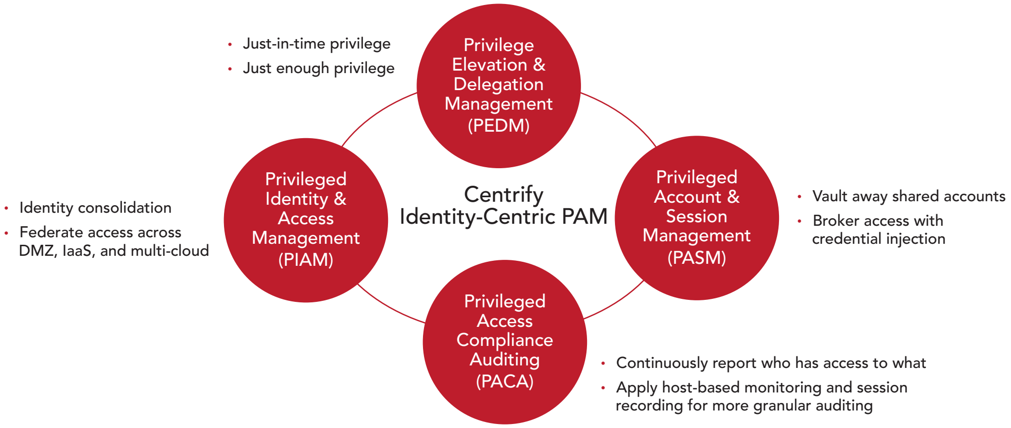
Underlying the foundation of digital transformation are privileged identities, as they're meant to assure that only authorized individuals, machines, or services are permitted access to the right resources at the right times and for the right reasons. Establishing a proper mechanism to do this in the most efficient and secure manner is therefore essential, and has become the Achilles heel to the success of many digital transformation projects.

As organizations continue their digital transformation journeys, they struggle to manage an infrastructure that is fragmented across hybrid- and multi-cloud environments, resulting in data breaches, audit findings, and unnecessary overhead costs.

Centrify enables digital transformation at scale, modernizing how organizations secure privileged access across hybrid and multi-cloud environments by enforcing Identity-Centric Privileged Access Management (PAM) based on Zero Trust principles.

Ultimately, leveraging Centrify Identity-Centric PAM helps organizations protect against breaches, enables cloud transformation, simplifies infrastructure management, and improves compliance postures.

Modernizing How Organizations Secure, Orchestrate, and Analyze Privileged Identities



Centrify Identity-Centric PAM

Privilege Elevation & Delegation Management (PEDM)
- Just-in-time privilege
- Just enough privilege

Privileged Account & Session Management (PASM)
- Vault away shared accounts
- Broker access with credential injection

Privileged Access Compliance Auditing (PACA)
- Continuously report who has access to what
- Apply host-based monitoring and session recording for more granular auditing

Privileged Identity & Access Management (PIAM)
- Identity consolidation
- Federate access across DMZ, IaaS, and multi-cloud

[1] Gartner Press Release, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020, November 13, 2019

"Centrify was one of the easiest technologies to justify return on investment. It's been a tremendous technology, it made our job a lot easier from a security and operational standpoint."

Sasan Hamidi, Former CISO, Interval International

"Success requires first-class software, reliable services, and outstanding support. The Centrify team provides us with all three."

Allessandro Rodrigues De Figueiredo, Chief Information Security Officer, SulAmérica

"Centrify has saved many man-hours for our sysadmin staff. Centrify also allows us to use Group Policies and manage Linux systems just like we do with Windows. Truly great product."

IT Manager, Government Agency

HUMAN OR MACHINE, IN THE CLOUD OR ON-PREM — PRIVILEGED ACCESS IS SECURE WITH IDENTITY-CENTRIC PAM

80%

of breaches involve a privileged identity

Source: The Forrester Wave™: Privileged Identity Management, Q4 2018

GARTNER ON PRIVILEGED ACCESS MANAGEMENT (PAM)

$131 Billion

expected spending on IT security and risk management in 2020

Source: Gartner, Forecast: Information Security and Risk Management, Worldwide. 2017 - 2023, Q419 Update

Top 10 List

of new projects for security teams to explore over the last 2 years

Source: Smarter with Gartner, Gartner Top 10 Security Projects for 2019, February 2019

#4

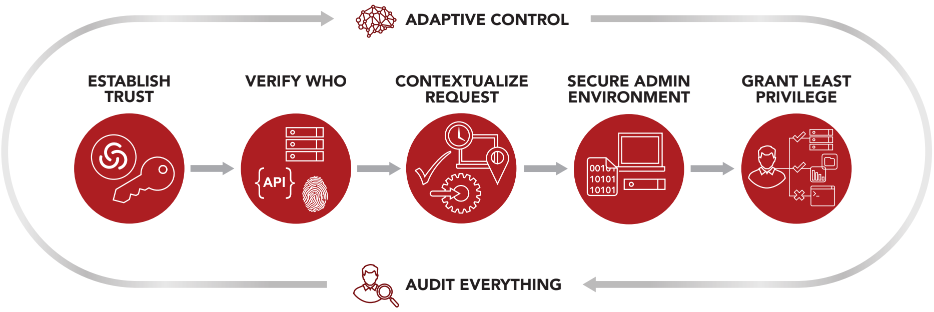
in estimated information security spending growth for 2020

Gartner, Forecast: Information Security and Risk Management, Worldwide, 2017 - 2023, 4Q19 Update

Centrify Redefines Legacy PAM

Identity-Centric PAM is founded on the Zero Trust principles of "never trust, always verify, and enforce least privilege." In the context of Privileged Access Management, Zero Trust requires establishing a root of trust, and then granting least privilege access just-in-time based on verifying who is requesting access, the context of the request, as well as the risk of the access environment. By implementing Identity-Centric PAM, organizations minimize the attack surface, improve audit and compliance visibility, and reduce risk, complexity, and costs for the modern, hybrid enterprise.

The Identity-Centric PAM Approach



ESTABLISH TRUST: For systems to enforce an authoritative access policy, each must have a securely-established unique identity with the authoritative security management platform. It is no longer acceptable in today's threatscape to allow management systems to use anonymous access accounts or injected credentials as often happens with vaulted, shared super user accounts, as they cannot be strongly verified for security operations.

VERIFY WHO: Today, identities include not just people but workloads, services, and machines. Properly verifying WHO means leveraging enterprise directory identities for the authentication and authorization process, eliminating local accounts and decreasing the overall number of accounts and passwords to reduce the attack surface.

CONTEXTUALIZE REQUEST: It is important to have zero standing privileges, and instead elevate privileges leveraging context to make just-in-time access decisions in order to prevent malicious lateral movement. In turn, associate the request with a relevant trouble ticket and provide a reason for access, as well as what is being requested and for how long. Once the request is contextualized then it must be routed for approval.

SECURE ADMIN ENVIRONMENT: By ensuring access is only achieved through a clean source, the risk of exposing servers to malware or introducing infections during a connection is reduced. Avoid access from user workstations that have Internet and email, which are too easily infected with malware.

GRANT LEAST PRIVILEGE: Just enough privilege, for just enough time to get the job done. Enable just-in-time privilege based on temporary access through a simple request process, and limit lateral movement by only granting access to the target resources needed and no more.

AUDIT EVERYTHING: Audit logs are critical for evidence of compliance and are used in forensic analysis. Best practice for privileged sessions is to also keep a video recording that can be reviewed or used as evidence for your most critical assets. Multiple regulations including PCI-DSS for payment card data specifically require this level of auditing.

ADAPTIVE CONTROL: Modern machine learning algorithms are now used to carefully analyze a privileged user's behavior and identify anomalous and therefore risky activities. Controls include alerts as well as active response to incidents by killing sessions, adding additional monitoring, or flagging for forensic follow up.

Modern. Agile. Hyper-Scalable. Modular.

PRIVILEGED ACCESS SERVICE

Shared Account & Password Vault
Application Passwords & Secrets Vault
Credential Management
Secure Administrative Access via Jump Box
Secure Remote Access
MFA at Vault

AUTHENTICATION SERVICE

Multi-Directory Brokering
Active Directory Bridging
Machine Identity & Credential Management
Local Account & Group Management
Centrify Zone Technology
Group Policy Management
MFA at System Login

PRIVILEGE ELEVATION SERVICE

Privilege Elevation
Delegated Privilege Role & Policy Management
Time-Based Role Assignment
MFA at Privilege Elevation

AUDIT & MONITORING SERVICE

Session Recording & Auditing
Gateway Session Monitoring & Control
Host-Based Session Auditing, Recording & Reporting

PRIVILEGE THREAT ANALYTICS SERVICE

Adaptive MFA
User Behavior Analytics
Command Activity Analysis

CENTRIFY PLATFORM

Access Request & Approval Workflow | Multi-factor Authentication Service | Unified Policy Management
Cloud Directory | Connector Gateways

Gartner

A LEADER IN THE 2018 GARTNER MAGIC QUADRANT: PAM, Q4 2018

FORRESTER®

A LEADER IN THE 2018 FORRESTER WAVE: PIM, Q4 2018

LeadershipCompass • KuppingerCole •

A LEADER IN THE 2019 KUPPINGERCOLE LEADERSHIP COMPASS: PAM

Centrify

Centrify Headquarters | 3300 Tannery Way, Santa Clara, CA 95054
+1 669 444 5200 | www.centrify.com