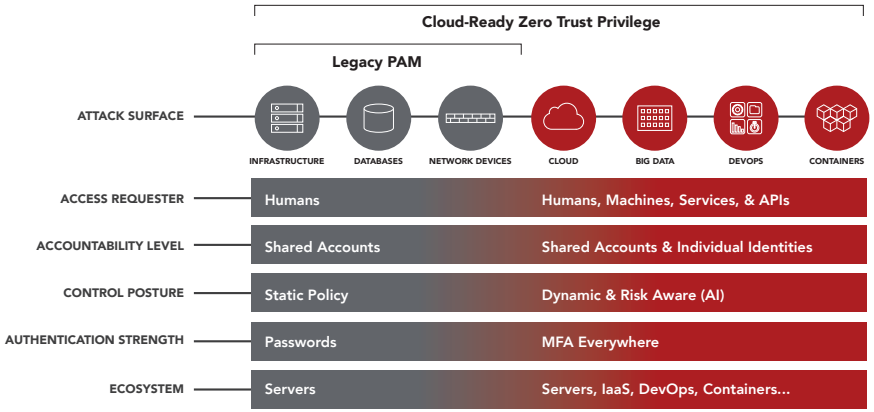
ZERO TRUST PRIVILEGE

Legacy PAM Is Not Enough for the Modern Attack Surface

Legacy Privilege Access Management (PAM) has been around for decades and was designed back in the day when ALL of your privileged access was constrained to systems and resources INSIDE your network. The environment was Systems Admins with a shared "root" account that they would check out of a password vault, to access a server, a database or network device. Legacy PAM served its purpose.

However, today's environment is different, privileged access not only covers infrastructure, databases and network devices but is extended to cloud environments, it includes big data projects, it must be automated for DevOps, and it now needs to cover hundreds of containers or microservices to represent what used to be a single server. In addition, Advanced Persistent Threats (APTs) create a growing and changing risk to organizations' financial assets, intellectual property and reputations. Expanding access and obtaining credentials is an essential part of most APTs, with privileged access being the crown jewels. Forrester stated that "80% of security breaches involve privilege credentials."[1]



Cloud-ready Zero Trust Privilege is designed to handle requesters that are not only human but also machines, services, and APIs. There will still be shared accounts, but for increased assurance, best practices now recommend individual identities, not shared accounts, where least privilege can be applied. All controls must be dynamic and risk-aware, which requires modern machine learning and user behavior analytics. Today PAM must integrate and interoperate with a much broader ecosystem including IaaS providers like AWS and Azure, with DevOps CI/CD Pipeline tools such as HashiCorp and Ansible, and with Container solutions such as Docker and CoreOS.

1 The Forrester Wave: Privileged Identity Management, Q3 2016

Centrify
ZERO TRUST PRIVILEGE

"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

LEGACY PAM NO LONGER MEETS THE DEMANDS OF THE MODERN THREATSCAPE... THE TIME IS NOW FOR ZERO TRUST PRIVILEGE.

$137 Billion

expected spending on IT security and risk management in 2019

Source: Gartner, Forecast: Information Security and Risk Management, Worldwide, 2016-2011, 3Q18 Update

2/3

of companies breached 5 times or more

Source: Forrester, January 2017

80%

of breaches involve a privileged identity

Source: Forrester Wave™: Privileged Identity Management, Q3

GARTNER ON PRIVILEGED ACCESS MANAGEMENT (PAM)

Top 10 list

of new projects for security teams to explore in 2019

Source: Smarter with Gartner, Gartner Top 10 Security Projects for 2019, February 2109

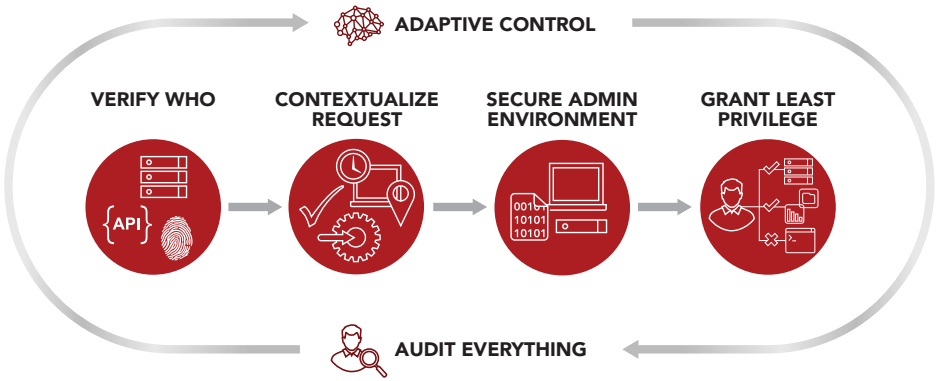
#2

in estimated information security spending growth for 2019

Source: Gartner, Forecast: Information Security and Risk Management, Worldwide, 2016-2011, 3Q18 Update

Centrify Delivers Cloud-ready Zero Trust Privilege

A Zero Trust Privilege approach helps enterprises grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Zero Trust Privilege minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity, and costs for the modern, hybrid enterprise.



VERIFY WHO: Not just people but workloads, services, and machines. Verifying WHO means leveraging enterprise directory identities, eliminating local accounts and decreasing the overall number of accounts and passwords, reducing the attack surface.

CONTEXTUALIZE REQUEST: It is important to know WHY privileged access is needed. This includes associating the request with a certain trouble ticket and providing a reason as well as a timeframe. Once the request is contextualized then it must be routed for approval.

SECURE ADMIN ENVIRONMENT: To not expose malware to servers or introduce infections during our connection, we need to ensure access is only achieved through a clean source. Avoid access from user workstations that have Internet and email, which are too easily infected with malware.

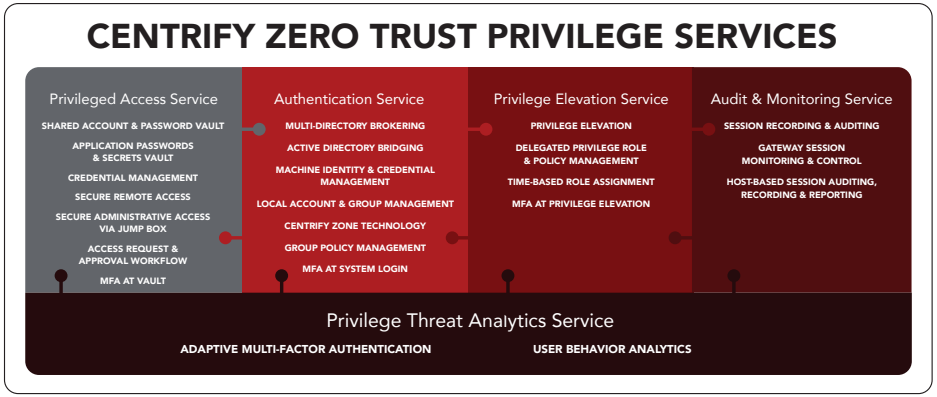
GRANT LEAST PRIVILEGE: Just enough privilege to get the job done. Just in time privilege based on temporary access through a simple request process and limiting lateral movement by only granting access to the target resources needed and no more.

AUDIT EVERYTHING: Audit logs are critical for evidence of compliance and are used in forensic analysis. Best practice for privileged sessions is also to 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 requires 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 alerting as well as active response to incidents by killing sessions, adding additional monitoring or flagging for forensic follow up.

Centrify Zero Trust Privilege Services

Centrify delivers Zero Trust Privilege through a set of integrated services:



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

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

A LEADER IN THE 2017 KUPPINGERCOLE LEADERSHIP COMPASS: PAM

Centrify ZERO TRUST PRIVILEGE

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