Centrify
ZERO TRUST SECURITY

ZERO TRUST SECURITY

Through the Power of Next-Gen Access

Centrify delivers Zero Trust Security through the power of Next-Gen Access. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience.

Today's Security is Not Secure

Traditional Security Doesn't Work. And Never Will.

Traditional perimeter security depends on firewalls, VPNs and Web gateways to separate trusted from untrusted users. But as mobile employees increasingly access the network remotely via their own devices, perimeters blurred. And they have virtually disappeared with the rise of cloud computing and IoT devices.

Never Trust, Always Verify

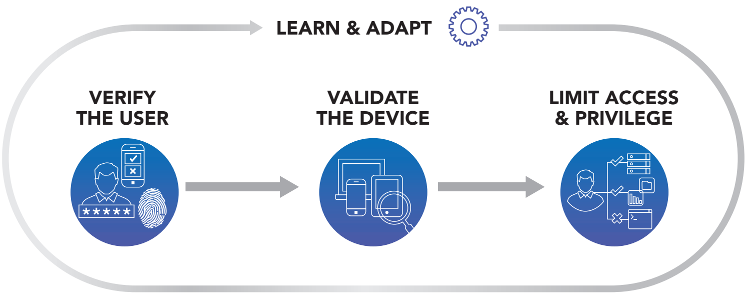
As traditional network perimeters dissolve, organizations must discard the old model of "trust but verify" which relied on well-defined boundaries. Instead, organizations must strengthen security by implementing an "always verify" approach for everything — including users, endpoints, networks, servers and applications.

Zero Trust Mandate

Following the highly-publicized breach of the U.S. Office of Personnel Management (OPM), which exposed the personal data of millions of Americans, the U.S. House of Representatives' Committee on Oversight and Government Reform issued a report recommending that federal information security efforts move toward a Zero Trust model. Stating that, "The Zero Trust model centers on the concept that users inside a network are no more trustworthy than users outside a network," the 2016 report triggered a discussion of Zero Trust across the public and private sectors.

The New Threatscape Requires Zero Trust Security

Zero Trust Security assumes that untrusted actors already exist both inside and outside the network. Trust must therefore be entirely removed from the equation. Centrify Zero Trust Security presumes that users and endpoints are not trustworthy and must be verified first so that security is not compromised.



Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience.

The end result is Zero Trust Security through the power of Next-Gen Access. This mature and proven approach unifies single sign-on (SSO), multi-factor authentication (MFA), mobility management, privilege management and behavior analytics.

VERIFY THE USER

Ensure authenticity of every user before access to a resource is ever granted

- Simplify Access through Single Sign-On
- Authenticate Everywhere with MFA
- Enhance Security and User Convenience with Behavior-Based Access

VALIDATE THE DEVICE

Enable secure access only from trusted devices

- Ensure Secure Access Through Trusted Endpoints
- Minimize Endpoint Threat Vectors through Device Security Management
- Increase Endpoint Security Posture with Endpoint Privilege Management

LIMIT ACCESS & PRIVILEGE

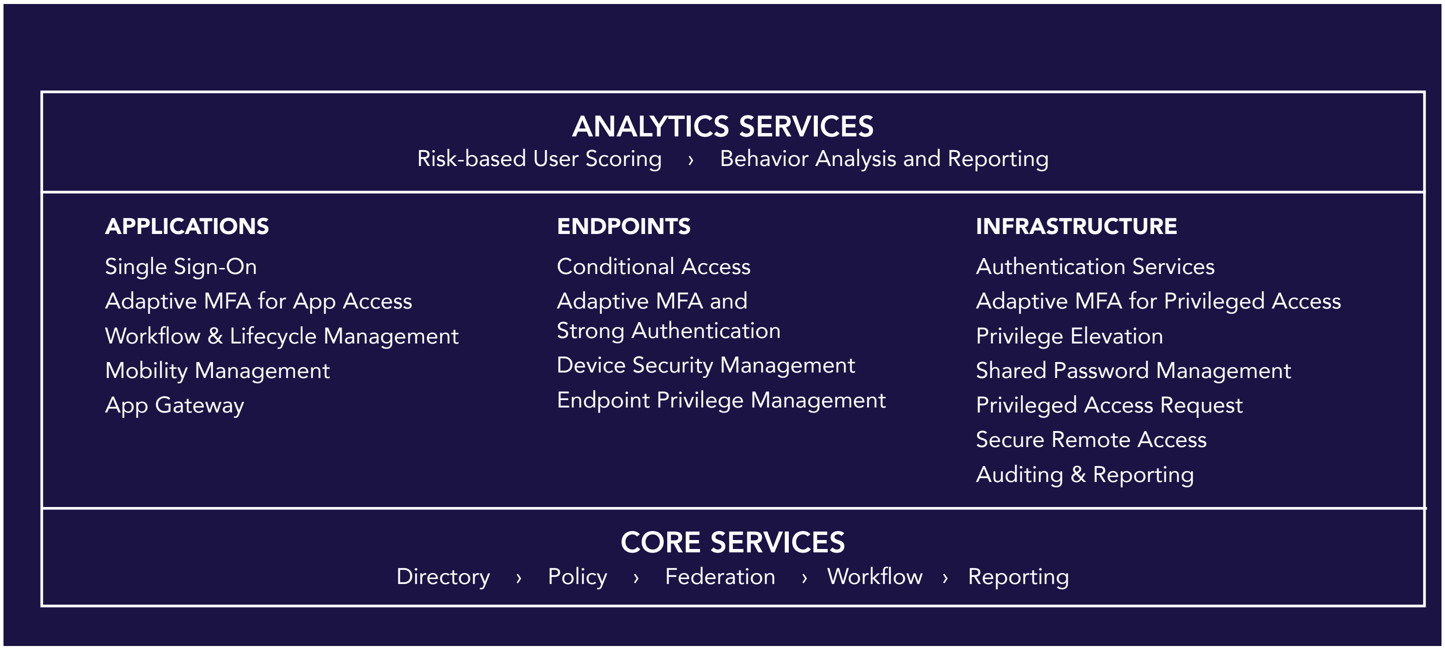
Grant just enough access and privilege to perform task

- Reduce risk when sharing privileged accounts
- Grant just enough privilege, just-in-time
- Enforce accountability across all privileged activity

LEARN & ADAPT

Leverage machine learning to automatically define and enforce access policies

- Block access or enforce additional authentication
- Improve user experience with adaptable policies based on user behavior
- Gain visibility and understand risk across applications, endpoints and infrastructure.



ANALYTICS SERVICES

Risk-based User Scoring › Behavior Analysis and Reporting

APPLICATIONS

- Single Sign-On
- Adaptive MFA for App Access
- Workflow & Lifecycle Management
- Mobility Management
- App Gateway

ENDPOINTS

- Conditional Access
- Adaptive MFA and Strong Authentication
- Device Security Management
- Endpoint Privilege Management

INFRASTRUCTURE

- Authentication Services
- Adaptive MFA for Privileged Access
- Privilege Elevation
- Shared Password Management
- Privileged Access Request
- Secure Remote Access
- Auditing & Reporting

CORE SERVICES

Directory › Policy › Federation › Workflow › Reporting

Next-Gen Access Platform

Centrify's Next-Gen Access platform delivers an industry-leading solution that uniquely converges Identity as a Service (IDaaS), Multi Factor Authentication (MFA), Enterprise Mobility Management (EMM) and Privileged Access Management (PAM). This seamless integration secures access across applications, endpoints and infrastructure for all users, without sacrificing best-of-breed features.

Verify the User: Centrify Application Services

Centrify Application Services combine IDaaS and MFA so that organizations can evaluate user attributes and behavior to determine the amount of verification needed to securely authenticate that user — and require additional actions (MFA) as needed to ensure authenticity. Once authenticated, users gain access to all pre-approved resources. Additional verification may be required to elevate privilege or to access the most sensitive data.

Validate their Devices: Centrify Endpoint Services

Centrify Endpoint Services ensures secure access from only known and trusted devices. With Zero Trust, it's essential that information about not only the user's identity and information, but also about the endpoint come together to assign a risk score. If risk is low, friction decreases. As risk increases, the appropriate controls kick in, requiring additional factors of authentication or more restricted access.

Limit Access & Privilege: Centrify Infrastructure Services

Centrify's host-enforced Privileged Access Management (PAM) restricts access to just the systems and resources associated with a user's specific job. By granting just enough privilege and easing the process for privilege elevation, risk is reduced and security increased. If user credentials are compromised, the amount of damage that can be done is limited.

Learn & Adapt: Centrify Analytics Services

Centrify Analytics Service leverages behavioral data to stop compromised credential-based attacks. Through machine learning, Centrify Analytics Service assesses risk based on constantly-evolving user behavior patterns. It assigns a risk score and enforces an appropriate access decision, all while simplifying risk monitoring and analysis.

Zero Trust — The Only Security That Works

What the Analysts Say

Forrester has long been an advocate of a Zero Trust strategy, stating that "CIOs must move toward a Zero Trust approach to security that is data- and identity-centric — and in our view is the only approach to security that works."

Google BeyondCorp

It's not only theory espoused by analysts, Google has put Zero Trust into action with their BeyondCorp project. Google's BeyondCorp model entirely removes trust from the network, securely identifies the device and the user, and applies dynamic access controls, least privilege and context aware policies.

Think Zero Trust Security. Think Centrify.
Learn more at www.centrify.com/zero-trust-security.

Centrify
ZERO TRUST SECURITY

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organizations, including over half the Fortune 100, trust Centrify to proactively secure their businesses. To learn more visit www.centrify.com.

US Headquarters +1 (669) 444 5200 | EMEA +44 (0) 1344 317950 | Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876 | Latin America +1 305 900 5354 | sales@centrify.com