Centrify brings Zero Trust to DevOps

Submitted by: Origin Comms Ltd
Monday, 16 April 2018

Centrify (https://www.centrify.com), a leading provider of Zero Trust Security through the power of Next-Gen Access, today announced it is extending its Zero Trust Security platform to DevOps environments. Centrify customers can now reduce their exposure to common security threats in their application development pipelines without compromising security, velocity, or scalability by leveraging Centrify Next-Gen Access (https://www.centrify.com/education/what-is-next-gen-access/).

The introduction of microservices, container-based architectures, and DevOps practices have led to a revolution in software development. However, as companies adopt these new technologies, tools, and methodologies, access management becomes increasingly complex. Security and operations teams must manage and audit permissions and credentials for a growing number of user and system accounts. Compounding the issue is that traditional methods of securing developer environments involve manual interventions and restrictive controls that significantly restrict the agility of development and operations.

“DevOps creates a challenge for many organisations because they need to maintain agility while also recognising that the DevOps process creates a broader attack surface,” said David McNeely, vice president of product strategy at Centrify.

“Prioritising functional requirements over security while building applications leaves organisations exposed to significant risk. Centrify Zero Trust Security reduces that risk by managing machine identities and access end-to-end across the entire corporate ecosystem, including DevOps environments and emerging tools and services.”

Centrify Zero Trust Security enables customers to scale adoption of secure DevOps by simplifying the integration of security into application development pipelines. This Zero Trust approach presumes that users, applications, and endpoints are not trustworthy and must be verified at every point of access so that security of the development pipeline is not compromised.

Centrify’s Next-Gen Access portfolio now enables:

Centralised management of Docker groups within Active Directory.
A Docker group is a permission group that allows non-privileged users to execute Docker commands. - Previously, non-root users had to be manually added to local Docker group on each container host. With the Centrify platform, customers can create a single Docker group in their Active Directory to grant non-root users the ability to create, modify, or delete container resources across container hosts. For fine-grained control over Docker command execution, customers can use Centrify’s Privilege Elevation service and grant users in a specific role the ability to execute specific Docker commands.

Centralised management of access rights and privileges for CoreOS Container Linux.
CoreOS Container Linux is a lightweight container-optimised operating system with pre-configured Docker Engine. Previously, customers needed to rely on shared root accounts or local administrator accounts to manage access to their container infrastructure. With the Centrify platform, customers can leverage Active Directory to control access to their container hosts running CoreOS Container Linux and further

secure user access with Multi-Factor Authentication (MFA) and Privilege Elevation services.

Access management for containerised applications.

Centrify's platform enables containerised applications to securely access other network resources by leveraging SAML or OAuth, and provides granular access controls to containers independent of the access to container hosts. With the Centrify platform, customers can protect access to containers and container hosts with MFA, and securely store account passwords or secrets such as configuration strings, encryption keys, and SSH keys in the Centrify Privileged Access Service.

The Centrify Zero Trust Security platform can now also be used to seamlessly authenticate to HashiCorp Vault, a tool for securely storing and accessing secrets. Centrify's authentication method grants users temporary access to Vault, eliminating long-lived credentials that can be compromised through malware attacks. With Centrify, user and service accounts can access Vault by authenticating against any connected directory source including Active Directory, LDAP, Google Directory, or the Centrify Cloud Directory. The Centrify Zero Trust Security platform authenticates users to HashiCorp Vault with their enterprise credentials, whether it is deployed on-premises, in a DMZ, or in the AWS cloud.

"With the strong growth of the HashiCorp community, having Vault integrate with Centrify Zero Trust Security is a valuable option for our users" said Burzin Patel, VP Worldwide Alliances at HashiCorp. "Centrify's platform empowers users to leverage the control and flexibility of using their existing corporate source for identity, while also increasing security and agility. That's huge for developers, who are usually required to sacrifice one over the other."

Centrify Zero Trust Security through the power of Next-Gen Access is a mature and proven approach that unifies single sign-on (SSO), MFA, mobility management, privilege management and behavior analytics. Zero Trust rethinks the "trust but verify" approach to security, replacing it with a stronger "never trust, always verify" approach to secure endpoints, networks, servers and applications.

To learn more about Centrify Zero Trust Security, visit www.centrify.com or booth 501 at RSA Conference 2018.

About Centrify

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, 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. 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.

Media contact:
Amanda Hassall

Consultant, Origin Comms
amanda@origincomms.com
+44 7855 359889/+44 1628 822741