Omada

Omada and CyberArk Extend Strong Identity Security and Governance to All Identities

Highlights

- Gain complete visibility of all identities and access permissions across the organization to reduce risks, defend against attacks and satisfy audit and compliance
- Effectively manage, govern and provision access for both privileged and workforce identities and their corresponding access entitlements through their entire lifecycles
- Enforce unified access policies and consistent governance, provisioning and authorization processes for privileged and non-privileged identities to ensure regulatory compliance
- Extend Single Sign-on and Multi-factor authentication to all workforce users
- Implement out-of-the-box governance workflows for automated and ongoing attestation of all types of users and their access entitlements from a single portal for improved efficiency
- Demonstrate compliance and accountability for authorities via advanced reporting and analytics options for both privileged and workforce user data and access rights
- Improve business efficiencies by instituting self-service access request workflows with tight approvals processes and automated audit capabilities

Omada and CyberArk partner to deliver enhanced Identity Security solution for strong identity governance, administration and access management.

This joint solution unifies authentication, identity and access governance and privileged access management controls, giving organizations the power to centrally manage and govern all types of identities — including privileged users and their entitlements. Together, CyberArk and Omada position organizations to — to ensure enforcement of strong access policies and regulatory compliance.

Many organizations use disparate solutions to manage the identity lifecycle and access policies for privileged and workforce identities. However, standalone solutions lack the ability to enforce consistent governance, provisioning, and authorization policies . processes. Without a unified platform, this can lead to access policy violations, security gaps, or failed audits—not to mention the inefficiencies created by stitching these separate processes together.

The collaboration between CyberArk and Omada means organizations can achieve strong privileged access management, workforce access management and identity governance in a unified platform. The integration enhances and enriches Omada's native governance functionality with data about privileged and workforce user access from CyberArk's Privileged Access Management (PAM) and Identity and Access Management (IAM) solutions. This allows organizations to create workflows and business processes across all identities and enables continuous governance and access recertifications.

Omada helps organizations define and enforce access policies based on identity attributes and organizational relationships. Omada centrally manages and governs the lifecycle of all types of identities and entitlements from one integrated platform, providing organizations with the ability to manage access, roles and entitlements for all identities

as they join, move and leave the organization. This ensures all identities have the right levels of access on day one and conversely, access is removed upon leaving the organization. The integration between CyberArk and Omada's certification and reporting capabilities means that organizations are continuously positioned to ensure the right security level and governance of privileged accounts while also optimizing business efficiencies and processes.

Omada Products:

- Omada's Identity Cloud, IGA as a Service
- Omada Identity, for organizations deploying on-premises

CyberArk Products:

- Privileged Access Manager
- CyberArk Identity

Provide Complete Governance and Secure Administration of all Identities

The CyberArk Identity Security Platform is an integrated, enterprise-class solution that includes both Privileged Access Manager (PAM) and Workforce Identity. CyberArk PAM solutions securely manage all accounts and credentials used by human and machine identities. manages and secures all privileged accounts used by individuals and applications. The solution securely manages credentials including passwords and SSH keys, controls account access, and isolates and records privileged sessions for auditing and forensics analysis. CyberArk PAM centralizes all privileged account information and activities, and provides data about privileged access directly into Omada.

CyberArk's Workforce Identity solution provides workers with simple and secure access to all enterprise resources — on-premises, in the cloud or hybrid — from any location, using any device. Workforce Identity includes both Single Sign-On (SSO), which gives workers convenient one-click access to all of their enterprise applications using a single set of credentials, and AI- powered Adaptive Multi-factor Authentication.

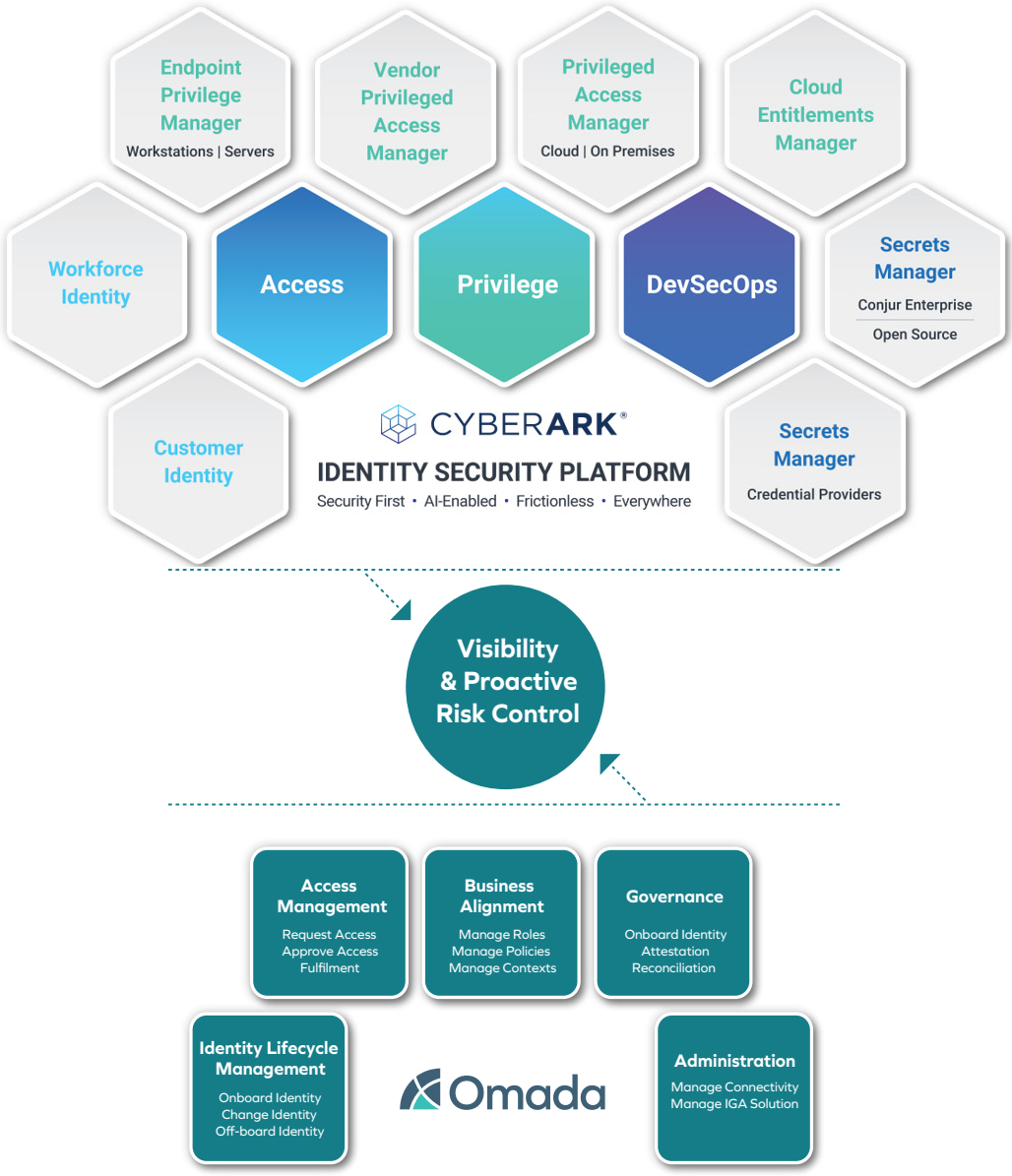
Omada collects granular entitlement data from CyberArk to enable governance, certification and reporting for all identities. Fine-grained access reporting allows an organization to see exactly which privileged accounts can be accessed by which users or applications, removing the need to correlate reports from multiple solutions to demonstrate compliance. Omada can automatically provision user entitlements to CyberArk via Microsoft Active Directory and/or Azure Active Directory groups based on access and segregation of duty policies, approval workflows and certification status.

The integration enables organizations to:

- Provide all users with secure access to applications and resources using modern Single Sign-On and Adaptive Multi-factor Authentication
- Manage privileged, workforce and third-party vendor identity access and entitlements via the Omada Portal
  - Provide self-service, yet highly secure access requests to accounts including secure configurable approval chains so that admins can see who requested access and why
  - Delegate privileged access rights or request privileged access rights be provisioned to other users
- Monitor entitlement reviews and reporting in the Omada Portal
  - Use Omada attestation feature for certification of privileged access entitlements and permissions
  - Audit and analyze privileged user access permissions
  - Access Review Surveys for privileged user access entitlements
  - Report on privileged users access entitlements
- Define privileged user access policies
  - Create assignment policies to automatically grant access to privileged accounts based on roles, rule and policies
  - Manage entitlements for contractors based on business context. Provision privileged third-party access to applications or infrastructure just-in-time.
  - Create Segregation of Duty (SoD) policies, to eliminate toxic combinations of access rights and maintain least privileged access

Joint Omada and CyberArk Solution Benefits:

- Create standardized, automated processes for managing access and entitlements for all identities within the organization, throughout their entire lifecycle
- Control and govern identities and access rights holistically across all types of users
- Drive operational efficiencies by automating provisioning of privileged access rights based on organizational rules and policies or via self-service portal including implementation of review/approval automated access controls
- Allow organizations to provide in-depth reporting on all types of identities and their access permissions from a single pane of glass showing accountability for compliance and improving security posture



Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.

For more information, go to www.omadaidentity.com | info@omadaidentity.com

Omada