
Problem

Privileged user credentials continue to be the top target by attackers. Whether through phishing or malware, a privileged user constantly needs to protect their credentials and identity. OverWatchID is committed developing and delivering technology that protects privileged users. The number one problem with legacy privilege access management systems is that the implementation ends in partially or failed deployments due to the legacy vendors leaving it up to customers to solve how to deploy to all the targets they want to protect. That very heavy manual burden is the primary focus of what OverWatchID solves. OverWatchID calls this a “plumbing problem”. Only by deploying privilege security, can a company protect itself against the identity breach vector. Most privilege security solutions only work with on-premise resources that have a shell or RDP interface. Current support for modern web-based user interfaces are error-prone and difficult to configure and maintain.

Solution

OverWatchID is a Denver, CO based company with a goal to “Solve the Identity Security Crisis for Everyone” at a fraction of the cost. OverWatchID is a SaaS company that delivers Privilege Anywhere for companies in medium to larger size enterprise with cloud first initiatives, applications and cloud infrastructure running in Amazon AWS, Azure and Google Cloud. This allows enterprise to easily protect and secure privilege users from any cloud application to on-premise infrastructure.

OverWatchID’s Identity Automation capability solves this problem that takes months or years for deployment into days and hours, resulting full in a PAM solution deployment, not partial or shelved. OverWatchID deploys anywhere to defend cloud applications, cloud computing resources, and on-premise infrastructure. OverWatchID supports modern web user interfaces in addition to shell and RDP. OverWatchID stops privilege attacks and protects against insider threats for organizations actively pursuing cloud first initiatives. The modern architecture means privilege user access to any application, server or on-premise infrastructure is one-click away. With active monitoring and recording, OverWatchID can demonstrate access compliance for PCI DSS, HIPAA, SOX, SOC 2, and ISO 27002.

OverWatchID is architected as a 100% software solution that deploys with a gateway on a jump server in the DMZ and an agent on the privilege user workstation. OverWatchID automation reaches out into the network to detect and identify critical IT resources. The resources are then provisioned into OverWatchID in seconds to immediately provide privilege security.

Privilege Anywhere™ secures all IT resources wherever they are deployed, completely implements in days, strengthens IT security, and costs less to own. As a result, information security teams work less and pay less for better IT protection from insider threats and external attacks.
OVERVIEW

Fueled by the adoption of cloud applications, cloud computing, and hybrid IT environments, privilege security continues to be a major issue for organizations. Even with robust identity and access management deployments, companies are still vulnerable to external attacks and insider threats. Only by deploying privilege security, can a company protect itself against the identity breach vector. Unfortunately, most privilege security solutions only work with on-premise resources that have a shell or RDP interface. Current support for modern web-based user interfaces are error-prone and difficult to configure and maintain.

OverWatchID, a privileged security service, deploys anywhere to defend cloud applications, cloud computing resources, and on-premise infrastructure. OverWatchID supports modern web user interfaces in addition to shell and RDP.

OverWatchID stops privilege attacks and protects against insider threats for organizations actively pursuing cloud first initiatives. The modern architecture means privilege user access to any application, server or on-premise infrastructure is one-click away. With active monitoring and recording, OverWatchID can demonstrate access compliance for PCI DSS, HIPAA, SOX, SOC 2, and ISO 27002

PRIVILEGE ANYWHERE

Built from the ground up to provide privilege security for cloud applications, cloud computing and on-premise infrastructure, OverWatchID extends and strengthens existing identity and access management infrastructure to secure against external privilege attacks and insider threats.

PRIVILEGE SECURITY
- Manage Privilege Credentials
- Prevent Spread of Malware
- Lock Down 3rd Party Access
- Connect with Web UIs, shell, and RDP
- Secure and manage Service Account credentials

IDENTITY SECURITY AUTOMATION
- Deploy and configure privilege security for hundreds of servers per day
- Discover and provision new targets and services
- Respond in real-time to emerging threat activities

INTEGRATIONS
- Single Sign-On – Okta, Ping Identity, Microsoft, OneLogin
- Multi-Factor Authentication – Duo Security, Google Authenticator, Microsoft
- Identity Governance – SailPoint
- IT Service Management – ServiceNow, JIRA, Zendesk, BMC Remedy

IT deployments have evolved away from on-premise deployments into a blend of cloud applications, cloud computing services and on-premise infrastructure. OverWatchID is the only privilege security platform that secures privilege users and defends critical resources wherever they are deployed.
OverWatchID is architected as a 100% software solution that deploys with a gateway on a jump server in the DMZ and an agent on the privilege user workstation. OverWatchID automation reaches out into the network to detect and identify critical IT resources. The resources are then provisioned into OverWatchID in seconds to immediately provide privilege security.

**FEATURES**

**Privileged Security**
- Session brokering for web UIs, shell, RDP – Connects users in seconds to target resources without revealing privilege credentials.
- Session recording and key logging – Demonstrate access control compliance and monitor changes to shell, RDP and web UI resources.
- Privilege credential management – Automatically updates privilege credentials after each use. Credentials are available for check out to support native clients.
- Credential vault – Securely encrypts and stores credentials to prevent credential theft.
- Break-glass support – Checkout/check-in credentials with available out of band approval for situations when connection brokering cannot be used.
- Analytics – Gather, analyze and alert on privilege user activities. Feed privilege user event activity through Syslog to log analytics or SIEM.
- Reporting – Review activities and exceptions generated by users within OverWatchID.

**Identity Security Automation**
- Auto_Discovery – Scans and monitors a network for new targets and resources to provision into OverWatchID. Gathers resource information to aid in provisioning.
- Auto_Orchestration – Preps and provisions target resources into OverWatchID. Hundreds of targets per day can be provisioned into OverWatchID.

**Integrations**
- IAM – Leverage deployed IAM infrastructure and services for user information, SSO support and multi-factor authentication. (Active Directory, LDAP, Okta, One Identity, Ping Identity, Duo Security, RSA SecurID)
- IT Service Management – Provide governance, approvals and change management. (ServiceNow, Zendesk, Jira, BMC Remedy, ConnectWise)

**Administration**
- Multitenant – Native support for complex organization control. Configure and manage business units, 3rd parties, and customers separately with multitenant support.
- Auto-update – All software components update automatically (or on a schedule within a configured change window) so that administrators don’t have to worry about patching and updates.

With OverWatchID Identity Orchestration, organizations streamline configuration, maintenance and administration of privilege security using the latest DevOps technologies. Privileged users are easily protected with Privilege Anywhere in a Zero Trust environment from the cloud to on-premise, wherever they are working.