accops
Virtualize.Secure.Deliver

Multi-Factor Authentication

HYID

Strong Authentication & Auditing

Accops HyId is multi-factor authentication and privileged access auditing solution, available as an add-on license to Accops HySecure gateway. HyID provides flexible, simplified and integrated multi-factor authentication services for user authentication, including One Time Password, Digital Certificates and Biometrics based authentication.

HyID can be integrated with HySecure gateway login, any third party network device login via RADIUS and TACACS, Microsoft Windows desktop login, Microsoft Windows server login and Linux server login.

HyID can deliver a One-Time-Password to User via SMS or Email or user can generate it using HyID software token available for mobile phones and PC. HyID biometric plug-in enables seamless login to desktops.

With a flexible authentication, authorization and policy structure, HyID can fit into any organization, integrates with existing infrastructure and provide user friendly authentication services. With HyID REST based API, any application can be protected with strong multi-factor authentication.

HyID Protects

- **Microsoft Windows Desktop Login**
- **Microsoft Windows Server Login**
- **RDP into Windows Desktops & Servers**
- **Linux Server Console and Remote Shell Access**
- **Remote Access Gateways**
- **SSL VPN, Firewalls, Managed Switches**
- **Any corporate application via REST API**

Secure Corporate resources with multi-factor authentication

Track, Audit and Control Privilege Access by Power Users

Reduce Identity Theft and Phishing attacks on Internet Facing Applications

Protect Desktop, Server & Network device remote logins with strong authentication & Auditing

SMS Token

Email Token

Mobile App Token

PC Software Token

FEATURES

Multi-Factor Authentication

HyID secures corporate resources with multiple factor authentication techniques. HyID can enable One-Time-Password based protection on top standard username and password based authentication. HyID can also use Biometrics authentication to secure corporate resources. HyID can calculate the risk of the access incidence and based on that require the user to authenticate using strong authentication. Risk is calculated based on user's location, device used, browser used, access time and more parameters. HyID also ensures a smooth experience for the end users with flexible but secure policy framework. Administrators can customize the level of security to be enforced on end users.

Protect Desktop Logins

As the entry point to any corporate work space access is the Desktop or the Shell access, HyID can protect the Microsoft Windows Login, Linux Console login and Shell login using multi-factor authentication. When installed, HyID client for Windows OS, secures the Windows Desktop OS as well as Windows Server OS with strong authentication. If a user is remotely logging into a Windows Desktop or Server using RDP, the user must pass through two factor authentication. Linux desktop & server console as well as shell access also can be secured with HyID

Flexible Token Support

HyID provides One-Time-Password via multiple tokens including SMS, Email, PC Software and Mobile Application. HyID can also integrate with any OATH compliant hardware token.

Availability

HyID is available as part of HySecure gateway. HyID can be bought as a standalone product (no HySecure functions) or as an add-on license to HySecure. HyID supports high availability and failover.

Privilege Access Audit & Control

Using HyID, organizations can track, control and audit privilege access by the IT teams, support teams, developers and consultants who needs administrative privilege to systems for their regular work. The challenge arrives when the organization cannot track exactly who used the privilege user accounts like local and domain Administrator accounts. This can lead to grave security issues and leave the organization without any tracking of the security breach. HyID ensures that power users must present their personal domain accounts to use the privilege user accounts. Based on dynamic risk based policies, the users might be required to enter additional authentication methods like OTP and Biometric.

Protect Network Logins

HyID has built-in RADIUS and TACACS based interface to integrate with any managed network equipment that supports two factor authentication via RADIUS and TACACS protocol. Almost all Firewalls, NAC devices, Managed routers and switches enables two factor authentication for administrator user logins. HyID can ensure strong authentication for such privilege user access to these network devices.

Integrate with Any Application

HyID provides REST based API to be integrated with any Application. The REST based API are very simple and provides a workflow for any developer to integrate in any application that needs to be protected by multi-factor authentication.

Detailed Auditing & Monitoring

With HyID, Organizations can track and audit who accessed the corporate resources, when and from where and if the access had certain risk associated with it. HyID reports the endpoint details which can help track the location of access.

new era
REDEFINING IT SOLUTIONS

NEW ERA INFORMATIQUE PVT. LTD.
CIN No.: U74140MH2006PTC162912
Locations: Mumbai | Delhi
We Provide Solutions PAN India

Email: teamfocus@newera-technologies.com
URL: www.newera-technologies.com
/company/newerainformatiquepvtltd
/NewEraInfo2001