accops
Virtualize.Secure.Deliver

Secure Application Access

HYSECURE

Secure Remote Access to Applications and Data

Accops HySecure is an application access gateway that enables enterprise mobility and secure access to corporate applications, desktops and network services from any device working from any network. HySecure enables users working from any network be it trusted LAN or untrusted WAN or Internet or mobile network to securely access corporate resources. HySecure's SPAN technology makes secure access a simple, fast deployment without requiring any complex network configurations. User can get onto a browser, desktop client or mobile application and start accessing the applications without requiring any configuration on the devices.

Accops HySecure brings together the performance, simplified management and functionality required for enterprise remote access and reduces complexity and costs traditionally associated with other VPN solutions.

- **Easily enable BYOD and give access of applications to users**
- **Easy secure remote access to implement strong authentication for applications.**
- **Deliver apps seamlessly to roaming users**
- **Replace legacy IPSEC/SSL VPN**
- **Create secure sandbox work space**

Enable, effortless enterprise mobility

Enable secure sandbox computing

Wrap & deliver applications with strong authentication

Integrated with application & desktop virtualization

SPAN Technology

Accops HySecure's Secure Private Application Network (SPAN) technology enables a high performance, simplified remote access deployment. Accops's SPAN technology makes remote and mobile users access business applications from any device without requiring any network adaptor installation or creating complex network routing changes. SPAN technology makes sure, user's get the fastest experience when on high latency and slow networks, while network security administrators can ensure full control on which applications are exposed to roaming users.

Authentication, Authorization Auditing

Before applications can be exposed to untrusted networks, it is required to secure applications with strong authentication layer. Accops HySecure includes strong multi-factor authentication features which ensures only authorized users can access the applications. Strong device identification features ensures that administrators can control which devices can connect to corporate network and access the applications. HySecure's flexible, multi-layered authorization framework enables organizations to control access to business applications based on more than 20 parameters. IT administrator can gain insights into who access what at what time through the management console.

Secure Enterprise Mobility

HySecure enables strong and latest TLS protocol base data security and integrity for application traffic. By deploying HySecure solution, organizations can secure any business application and make it available to end users without requiring any pre-configuration on end users machine. With HySecure, its easy for organizations to enable extranet users, vendors, consultants to bring their own device and get access to applications.

Strong Endpoint Control

Before an end user is allowed to access the applications, it is mandatory for organizations to detect, scan and evaluate the trust level of the device used by the user. Based on the trust level of the device, HySecure can control the endpoint and make sure the device is not compromised and can be compromised while user is accessing the applications. HySecure can control and restrict Internet access on end user machine. HySecure can also detect the device location and implement different policies based on the location of the device.

Anywhere, Anytime Computing

HySecure provides a single window access to end users which lists the applications that are available to end users, providing a seamless end user experience and reducing the number of support calls. End users can use the HySecure web portal to access business applications. When combined with HyLite access mode, HySecure can deliver any Microsoft Windows and Linux based virtual hosted applications & virtual desktops to end users in a secure sandbox environment. For Power users and locally installed applications, end users can use the HySecure client for desktops to access the applications. HySecure client does not require any pre-configuration and can work from machines without administrative rights and auto-upgrades when new version is available.

Scalable, Reliable & Highly Available

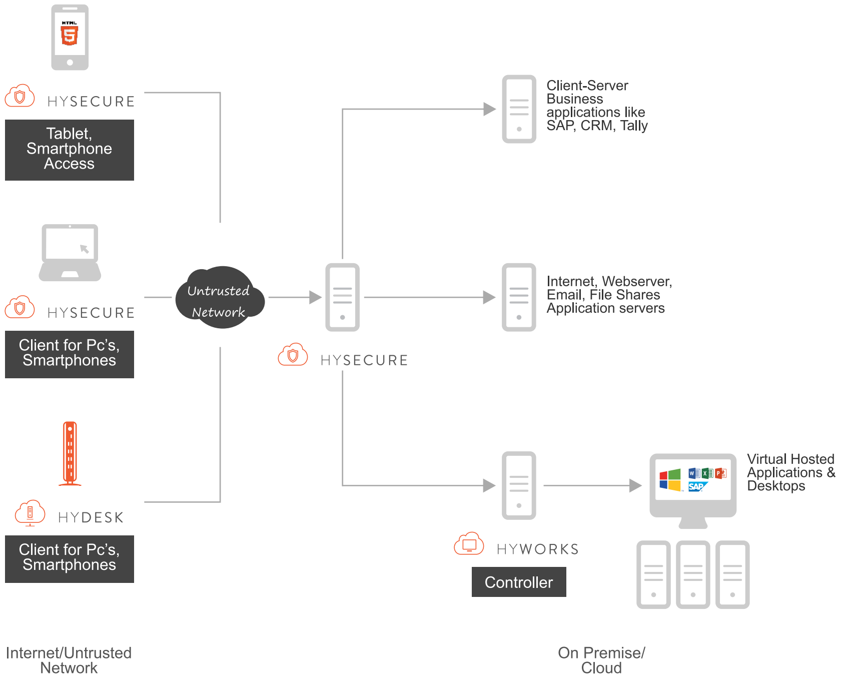
With built-in Load Balancing and high availability features, Accops HySecure can scale to thousands of users to ensure required uptime for business critical operations. HySecure has built-in load balancing for incoming users, as well as application traffic to ensure that the deployed hardware is effectively used. HySecure can be setup in DR mode with client side failover feature so that end users can always connect to a site.

Secure Sandbox Computing

HySecure, combined with HyWorks is used by organizations to create a secure sandbox for user computing. In the secure sandbox, the user can be restricted to run limited applications and user can be restricted from copying data from applications to local applications or take the data out of their machine. Secure sandbox can control clipboard, printing functions, desktop session recording, file saving, USB devices and more functions. Based on the user location, the sandbox can adjust itself releasing the restrictions if the user is working from a trust location.

Strong Two Factor Authentication

HyID, which comes along with HySecure for an additional license, can protect corporate resources with strong multi-factor authentication. HyID can enable two factor authentication based on One-Time-Password for HySecure login. User must login with a OTP received in SMS, Email or using the Accops HyID Mobile Application. HySecure can do SSO for applications like Microsoft RDP Connection, SSH to Linux Servers and HyWorks, along with presenting OTP for login into desktops, servers and network devices.


HYSECURE
Tablet, Smartphone Access
HYSECURE
Client for Pc's, Smartphones
HYDESK
Client for Pc's, Smartphones
Untrusted Network
HYSECURE
Client-Server Business applications like SAP, CRM, Tally
Internet, Webserver, Email, File Shares Application servers
Virtual Hosted Applications & Desktops
HYWORKS
Controller
Internet/Untrusted Network
On Premise/ Cloud

DATA SHEET

Application Support

- All web based, TCP and UDP based client-server applications
- Windows file shares and drive mapping
- Dynamic port based applications
- Publish Subnet or IP Range for network access
- Special support for RDP virtual channels
- Application server load balancing
- Session caching for load balanced applications
- Per application based compression switch
- MyDesktop for direct personal desktop access
- Terminal server application & VDI publishing via Propalms TSE, RDP & VNC, HyWorks
- HyWorks VDI & Hosted Application
- SAAS based Application support
- VoIP (voice over IP)
- FTP
- Fileshare
- SSO (SAML Support)
- O365 Support, GSuite, Salesforce (MFA is supported)

Access Security

- TLS 1.0, 1.1, 1.2 and above
- Encryption: Strongest available: DES, 3DES, AES
- Authentication: SHA-2, RSA 2048/4096
- 4096 bit RSA key CA certificate support
- Internet network masking and IP address/hostname mangling
- Application level gateway and not layer 2 bridging
- Hardened gateway operating system
- Split & Full tunnel modes
- Secure sandbox computing
- DDOS Protection
- Device based application access for O365, Salesforce & Outlook

Management

- Web based management console
- Dashboard with graphical reporting
- Menu driven console interface for system configuration
- Wizard driven installation procedure
- Self-signed certificate generation
- CLI
- Delegated administration
- Certificate based strong authentication for administrators
- Inline help
- Auto backup on E-mail/FTP
- Notification based on ser access
- Account lockout support
- Access control expiry
- Client auto-upgrade
- Broadcast customised messages
- Resource monitor and Alert

Authentication

Authentication based on

- User identity, OU/group/realm
- Static passwords, OTP – dynamic passwords
- Certificates
- Device signature: CPUID, HDDID, IMEI, more
- User location, MAC ID, IP Address
- Endpoint security trust level
- ADFS Support
- SAML Integration

Two Factor authentication

- Certificates, Device Signatures
- One Time Passwords (OTP) : SMS/ Email/ Hardware/Biometric/Software Token
- Local database with full customization per user, password policies & reset support
- RSA Secure ID or any 3rd party OTP server
- Integrates with AD/LDAP/RADIUS/SAML
- Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning
- Email based user provisioning
- Support for multiple authentication servers with cascading mode
- Realm based multi-organization support
- SSO based SAML
- Biometric authentication
- Consent (Push Notification)
- Consent with additional tokens (Push Notification)
- SSO NPLM based apps

Authorization

Access control based on

- Device identity and profile
- Endpoint Security trust level
- User Authentication method
- User Role
- User's organization
- User's location
- ACL (Access control List) expires automatically
- Application based access control
- Dynamic policy evaluation based on run time information about device, authentication method and user role
- Display of allowed applications and availability of the application server to users
- Time based restriction policies
- Scheduled account expiry
- Block specific groups
- Multiple VPN Domain based control
- Control User's Internet access
- Support for external authorization servers
- Automatic fetching of group information from AD/LDAP/RADIUS

Endpoint Control

Real time status check for

- Last update time
- Real time protection check

- Strong device identification based on 20 parameters includes CPUID, MBID, HDDID, MACID, IMEI No. and more
- Detect managed and unmanaged devices
- Login control from managed and unmanaged device
- Support for checking for antivirus, firewall and antispyware products
- Geo- fencing
- IP based access control
- Windows update based access control
- Application control based on device profile
- Mandatory profile for non-avoidable policy checks on all endpoints
- Quarantine profile for devices that fails all other profile
- Secure endpoints from attacks over Internet or becoming a proxy for attacks
- Restrict Internet access of the user based on policy
- Restricts users from leaking data using clipboard, printing, USB devices.
- Geolocation based restriction
- Windows update based restriction
- Profile based security policy

Auditing

- Information logged includes
- Time of access
- Username, domain
- MAC Address of endpoint
- IP address of endpoint
- Application accessed
- Device profile
- Productivity Logs
- User location Monitoring (Accops Reporting Server - ARS)
- Monitor users for Log monitoring
- Complete reporting of user logons and activity
- Detailed logging of endpoint security scans results
- Extract logs in CSV format for feeding to third part report generation
- Search logs
- Auto-archiving of logs
- Monitor and disconnect live users
- Alerts on new device registrations, user account lockouts
- Reporting on domain wise access, applications accessed, failed login attempts, concurrence graph
- Alert on Resource Utilization
- Sys log support

Access Modes

Multiple access modes

- HyLite portal for clientless access*
- Agent based access from any browser
- Full access client for desktops
- iOS & Android app
- Hybrid Portal Mode
- L3 Mode
- Reverse proxy Clientless VPN for web applications

Client platforms supported

- Windows 7/8/10
- Windows server 2003/2008R2/2012R2/2016
- Linux OS , MAC OS X
- iPad / iPhone / Android Access
- No configuration required on end user machines
- Site to site access
- HyLite: Access on any device with a HTML5 browser: Blackberry, Windows Mobile, iOS etc*

Deployment

- Scalable to thousands of users
- Active-Active N+1 cluster
- SSL connections load balancing, multiple algorithms
- Application connection load balancing
- Session persistence: Users do not need to re-authenticate
- ISP load balancing for incoming connections
- Client side failover using Alternate gateways
- Runs on hardened Linux based platform
- Menu driven console interface for easy configuration
- Can run on any standard or custom hardware
- Runs on virtualization platforms from VMware, XenServer, Hyper-V
- Runs on cloud platforms like AWS, Azure, Oracle Cloud, Google Cloud, Nutanix

* Requires additional license

accops
Virtualize.Secure.Deliver

Tel: +91-20-67190123 | Email: sales@accops.com | Web: www.accops.com