accops

Work From Home Solutions

Accops Systems Private Limited

ACCOPS CONFIDENTIAL

Need of Secure Work from Home

- Every business needs a cost-effective Business Continuity Plan
- Growing Concern of Global Pandemic like Coronavirus
- Natural disasters
- Traffic Crawls
- Business growth requirements

Concerns with Work from Home

- BYOD devices can not be trusted
  - Malware/Keyloggers on end user devices
- Provisioning laptops to users for work from home, is
  - Costly
  - Time consuming
  - Logistically complex
- How to provision applications to end users on new/personal devices
- User's Internet access can not be controlled
- End user's bandwidth won't be guaranteed
- How to address HR/attendance/productivity issues

Expected Solution for Work from Home

- Quick to setup
- Quick to rollout
- Zero end user device management
- BYOD capable
- Detailed auditing
- Employee attendance and timesheet management

- Security compliant
  - Protects data
  - Prevents data leakage
  - Role based access
  - Strong authentication
  - Device and user logon approval workflows
  - Device identity, monitoring and control
- Available on both on-premise as well as cloud offering
- Subscription licensing

Work from Home Technologies

- Traditional VPN
- Remote Desktop (Server-based) computing
  - Office PC access via VPN
  - Temporary Session-based Desktop via VPN
  - Virtual Apps & Virtual Desktop Infrastructure

Concerns with Traditional VPN

- Provide Secure connectivity but
  - Does not solve the endpoint security issues
  - Does not provision Applications on end user PC
  - Users can use any device
  - No advanced features like device entry control, data copy protection
  - End user bandwidth utilization can not be guaranteed
  - Malware on end user PC is big risk to corporate network
  - End point configuration is required
  - User’s Internet can not be controlled
  - Data copy possible by user

Solution: Accops HySecure Advanced

- App Tunnel based technology. No network bridging
  - Prevent any potential malware spread from user PC to corporate network
  - Lightweight and works faster on mobile networks
- Device entry control
  - Only allow authorized devices based on device fingerprinting
  - Check compliance status and only allow compliant devices
- Can work in Stealth mode with full control on end user device to
  - Restrict Internet
  - Restrict USB ports
  - Block printing
  - Block data download and copy-paste
  - Block printing screen, screen recording software
- Strong 2FA included in the product

Remote Desktop-based Work From Home Options

Office PC Access from Home

- Allow users to connect to their personal PC in office
- User uses their home/personal PC to connect
- Accops provides html5 based clientless access to office PC
- Product used: Accops HySecure Advanced
- Configuration: "My Desktop & Files Access"
- Printing, file download, clipboard can be restricted
- Optional: Enable MFA, force use of approved devices only, use HySecure client to access

Limited RDS Desktop Access

- Allow users to connect to temporary virtual desktop
- User uses their home/personal PC to connect
- Setup Microsoft RDS Servers and allow users to connect to RDS server
- Publish RDS servers via Accops HySecure
- Accops provides html5 based clientless access to office PC
- Product used: Accops HySecure Advanced
- Configuration: Publish RDS server as cluster for load balancing and session persistence
- Printing, file download, clipboard can be restricted
- Optional: Enable MFA, force use of approved devices only, use hySecure client to access

Virtual Apps/Desktop Access

- Allow users to connect to published Apps or session/virtual desktops
- Setup Virtual apps , session-based desktops or dedicated virtual desktops using Accops HyWorks
- Publish Accops HyWorks via Accops HySecure
- Accops provides html5 based clientless access to office PC
- Product used: Accops HyWorks Enterprise
- Configuration: Publish Accops HyWorks
- Printing, file download, clipboard, other USB devices and peripherals can be allowed or blocked based on policies
- Optional: Enable MFA, force use of approved devices only, use Accops HyWorks client
- Must for large deployments

Deployment Options

On-Premise

- Use existing virtual infrastructure
- No network change needed
- Same security stack can be used
- New hardware delivery can take time
- New Capex investment may not be useful after emergency WFH requirement is gone
- Microsoft licenses are also big Capex cost

On-Cloud

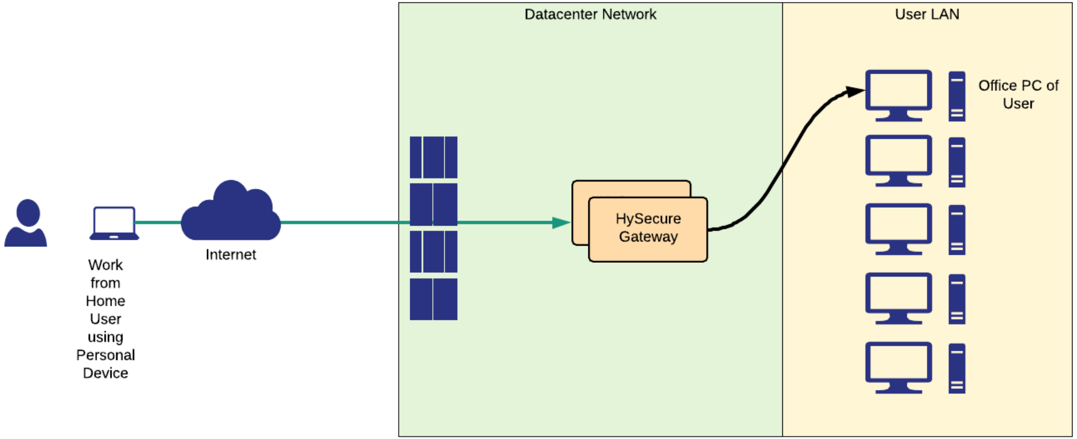
- Instantly Rollout new work from home service using virtual desktop in cloud
- Connect cloud tenant to on-prem datacenter
- Work from home users uses Internet to connect to cloud
- Flexibility to scale up or scale down
- Turn-off whenever need is over
- Microsoft licenses are also Opex cost for limited duration

Accops Solution: Meeting the Needs

Solution Requirement	Accops HyWorks Enterprise Solution
Quick to setup	Go live in few hours
Quick to rollout	HTML5 browser-based access is quick to rollout to users
Zero end user device management	No client software needed for instant access
BYOD capable	No device pre-configuration needed, user BYOD for access
Security compliant Protects data Prevents data leakage Role based access Strong authentication Device and user logon approval workflows Device identity, monitoring and control	Provides features to: Block file download and/or upload Block data copy, clipboard, printing, Block printscreen, screen recording Built-in Multi-factor authentication Allow only approved devices to login Flexible access policies to check compliance on device
Detailed auditing	Detailed audit log of what accesses what
Available on both on-premise as well as cloud offering	Install anywhere, Accops DaaS service available
Subscription licensing	Flexible pricing model to reduce Capex
Platform Support	On-Premise (any hardware, any hypervisor), Azure, AWS
Employee attendance and productivity reports	Provides granular customization reports &dashboarding

Office PC Access from Home

- User can use personal device to connect to office PC
- User can use web browser with no agent or download agent for compliance
- Endpoint control
  - Blocked Internet when accessing office apps
  - Block data download
  - Block clipboard, print screen, screen recording
- Enable MFA
- Enable device restrictions based on identity & health
- Lock down user to specific device

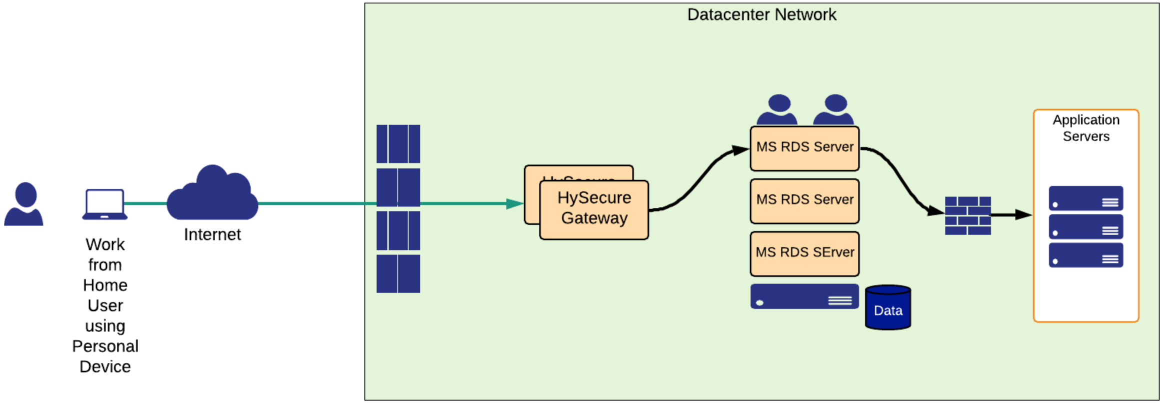


Product used: Accops HySecure Gateway Advanced with HyLite

Microsoft Licenses:
Even though user’s office PC is licensed, check with Microsoft about roaming rights.

Limited RDS Desktop Access

- User can use personal device to connect to a session based virtual desktop
- User can use web browser with no agent or download agent for compliance
- Endpoint control
  - Blocked Internet when accessing office apps
  - Block data download
  - Block clipboard, print screen, screen recording
- Enable MFA
- Enable device restrictions based on identity & health
- Lock down user to specific device
- Load balancing of RDS server taken care by HySecure

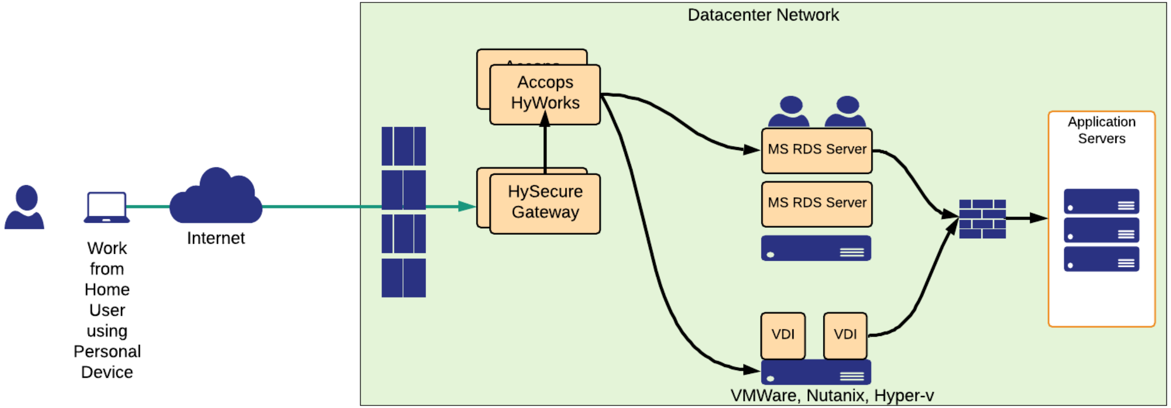


Product used: Accops HySecure Gateway Advanced with HyLite

Microsoft Licenses:
Windows RDS Server CALs: User based
Windows Server CALs (if does not existing: User based

Virtual Apps & Virtual Desktop Access

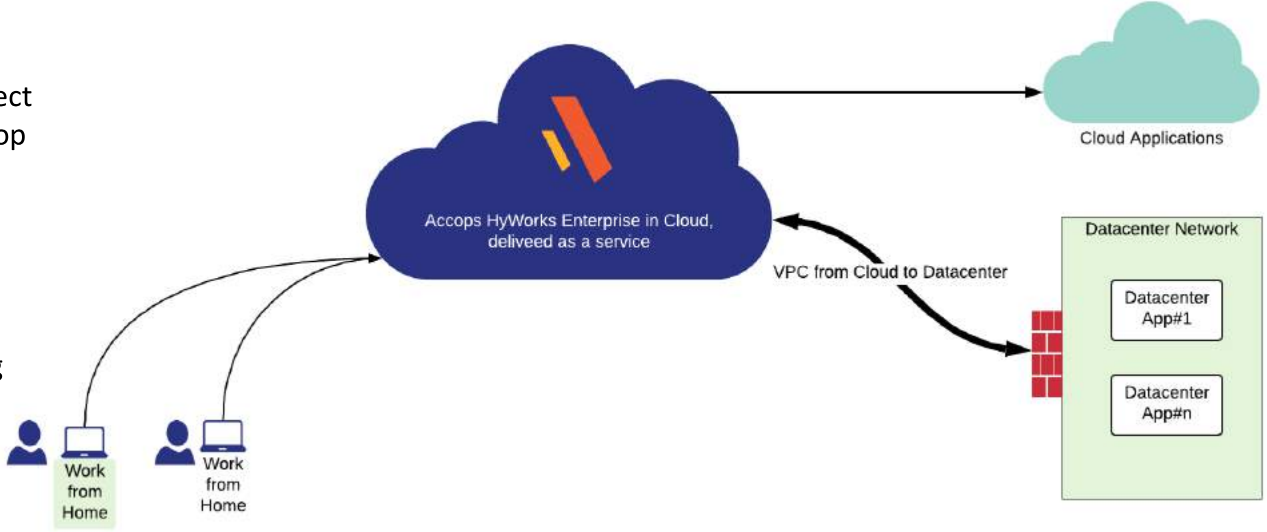
- User can use personal device to connect to a virtual apps, session-based desktop and personal virtual desktop
- User can use web browser with no agent or download agent for compliance
- Endpoint control
  - Blocked Internet when accessing office apps
  - Block data download
  - Block clipboard, print screen, screen recording
- Enable MFA
- Enable device restrictions based on identity & health
- Lock down user to specific device
- VM provisioning and life cycle can be managed from HyWorks
- User Session Recording



Product used: Accops HyWorks Enterprise with HyID
Microsoft Licenses: Windows RDS Server CALs: User based Windows Server CALs (if does not existing: User based

Accops DaaS for Instant WFH Service Rollout

- Managed Desktops-as-a-Service from Accops
- User can use personal device to connect to a virtual apps, session-based desktop and personal virtual desktop
- User can use web browser with no agent or download agent for compliance
- Endpoint control
  - Blocked Internet when accessing office apps
  - Block data download
  - Block clipboard, print screen, screen recording
- Enable MFA
- Enable device restrictions based on identity & health
- User Session Recording
- Encrypted VM available



Product used: Accops DaaS

All inclusive of cloud cost, Microsoft licenses

Supporting Microsoft Azure Windows Virtual Desktop

End User Access

- Clientless Browser-based access
  - Any HTML5 capable browser is enough
- Client Software-based access
  - Client for Windows, MAC OSX, Linux
  - Mobile app for iOS, Android
- Accops Thinclient: Linux-based devices
- Accops HyDesk OS on USB stick

HyDesk HyOS: Secure Work from Home

1. A Secure Linux based OS for making live OS, running on a USB device
2. Use any standard USB 3.0 based USB storage device
3. User boots up their device with Secure USB
4. User boots into a new OS which connects the device with corporate network securely via HySecure or into VDI using HyWorks
5. 100% assured protection from Keyloggers & Endpoint originated threats from BYOD
6. Two options to connect
    1. Direct access via access gateway
    2. Secure access to virtual desktop
7. Protection from
    1. Keyloggers
    2. Endpoint issues
8. Fingerprint authentication enabled USB available from Accops

Accops Solution Key Features

- Virtual workspace features
  - Virtual Apps
  - Shared hosted desktop
  - Client OS based virtual desktops
- Persistent & non-persistent
- Floating virtual desktop and 1 to 1 assignment
- Secure Access Gateway
- Multi-factor authentication
- Load balancing
- High availability & Failover
- Horizontal Scale out architecture
- Granular User Level Reporting

- User Access Features
  - HTML5 clientless browser
  - Desktop clients for Windows, MAC OSX, Linux
  - Mobile Apps for iOS, Android
- Deployment Options
  - On-Premise
    - Runs on any VMWare, Hyper-v, Nutanix on any hardware
  - Deploy on any cloud: Azure, AWS
  - Desktop-as-a-Service
    - Accops provided DaaS service in Azure or AWS
- Licensing Options
  - Subscription license with annual contract
  - Perpetual license

Why Accops

Why Accops

Secure Application Tunnel

Strong & flexible policy set to force corporate policies

Integrated access gateway, MFA and Virtual desktop access

Clientless access with device entry control for high security with no endpoint management

Detailed reporting to monitor and audit user activities

Multiple WFH options available based on need of business

Flexibility: On-premise or Cloud, Capex or Opex Cost, 3 months or 3 years

Simplified, Cost Effective

Accops Solution: Meeting the Needs

Solution Requirement	Accops HyWorks Enterprise Solution
Quick to setup	Go live in few hours
Quick to rollout	HTML5 browser-based access is quick to rollout to users
Zero end user device management	No client software needed for instant access
BYOD capable	No device pre-configuration needed, user BYOD for access
Security compliant Protects data Prevents data leakage Role based access Strong authentication Device and user logon approval workflows Device identity, monitoring and control	Provides features to: Block file download and/or upload Block data copy, clipboard, printing, Block printscreen, screen recording Built-in Multi-factor authentication Allow only approved devices to login Flexible access policies to check compliance on device
Detailed auditing	Detailed audit log of what accesses what
Available on both on-premise as well as cloud offering	Install anywhere, Accops DaaS service available
Subscription licensing	Flexible pricing model to reduce Capex
Platform Support	On-Premise (any hardware, any hypervisor), Azure, AWS

Common Concerns with WFH Addressed by Accops

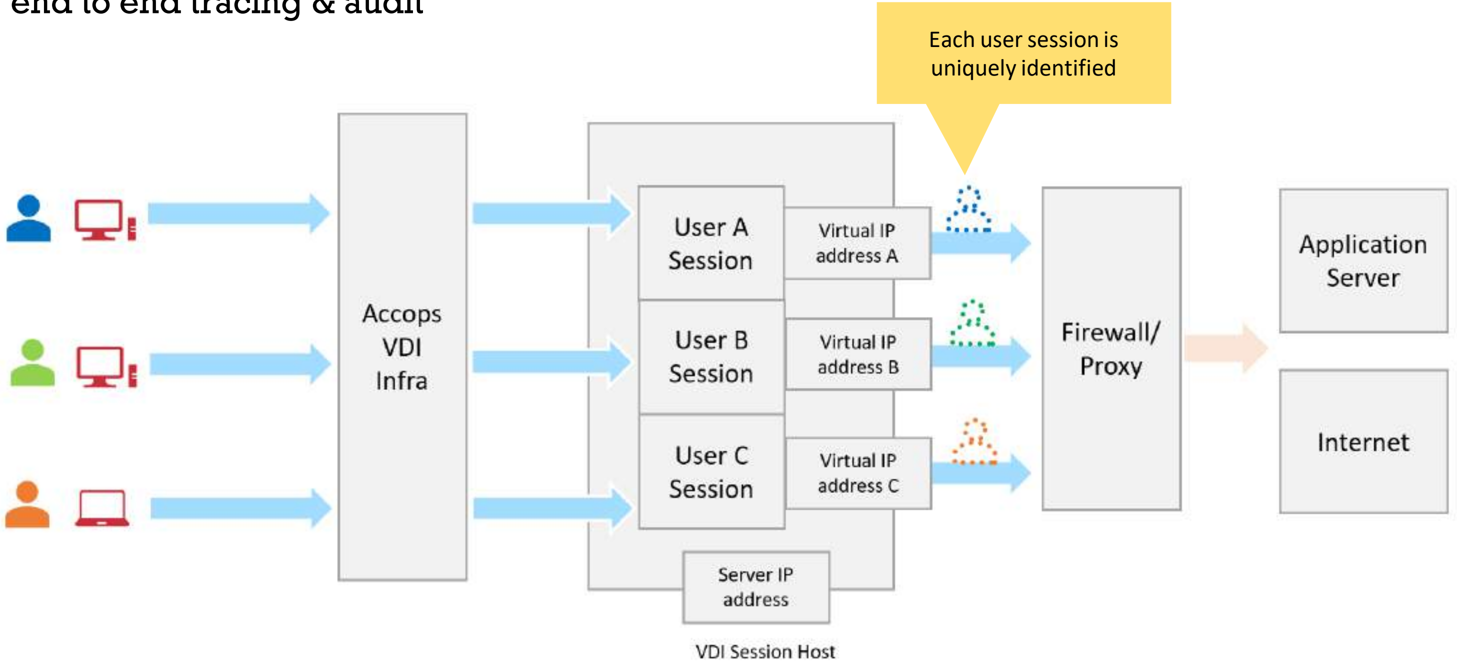
Threat	Accops' Solution
Network access controls are bypassed by VDI users, having more access than what they should have	VDI Infrastructure should be deployed in a separate segment and should be treated as end user network, separated from application server network
VDI design could bypass the perimeter security checks like Firewall access rules, WAF, Sandboxing, etc.	VDI Infrastructure should be considered as user LAN and must be placed in network such that all outgoing traffic from VDI should go through necessary security gears before reaching application servers
Client applications run in datacentre now, exposing data centre application server network to vulnerabilities	Client applications must be patched regularly, automated via VDI. The platform is in better control of IT with controlled changes
End users uploading potentially infected data into datacentre network	End user devices must have the same security gear as a desktop, unless using thin clients. Data upload must be allowed based on policy
End users connecting from unprotected devices to VDI	Device compliance controls must be enabled

Common Concerns with WFH Addressed by Accops

Threat	Accops' Solution
Connecting user's PC from their home network can infect corporate network	Accops provide application tunnels and not Layer 2 or Layer 3 based tunnel like any other VPN solution. User's machine does not get bridged to corporate
Once published over Internet, anyone can login from anywhere	Accops provides strong device identity check and lock down the user to specific devices
Integration of multi-factor authentication is time consuming and needs user training	Accops provides built-in 2FA with easy enrollment
How the productivity of user will be managed	Accops provides complete user session life cycle as a report. This can be used to decide employee productivity

Unique Identification of each VDI Session

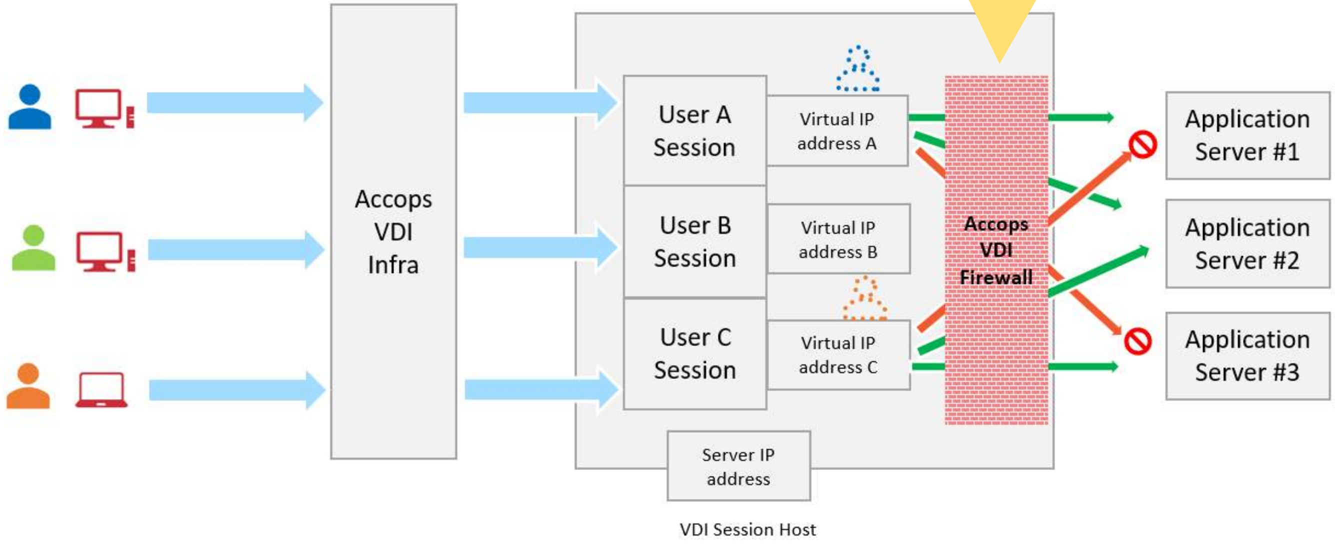
- Multiple users can share single Session host, in which the network identity of each user can be lost.
- A virtual IP address can be assigned to each user when they work over session host server
- Proxy or firewall sees user traffic coming from each user from a different IP address and can enforce same controls as a PC user
- Virtual IP address can be a static IP address and is mapped to username and user's device IP address for end to end tracing & audit



Accops’ VDI Firewall

- Accops can restrict user’s network activity based on set policy
- One user on session host can be restricted based on :
  - Server addresses and port, they can connect to
  - Applications that they can use to connect to these server addresses and port
  - Have a block all and explicit allow policies
- Another user on same server can have different set of polices

Accops monitors user’s traffic and blocks unwanted connections to application servers



Accops' Data Control Features

- Accops Solution provides following data control features
    - Block data exchange between user PC and VDI
    - Block data download
    - Block copy-paste
    - Block print-screen and screen recording
    - Block Internet completely or selectively enable Internet
- Enable data exchange or copy based on need-to-access basis
- Data downloaded from virtual desktop can be recorded and audited
- All user activity can be recorded for audit later

Accops' SecuFex: Secure File Exchange

- Accops' SecuFex feature ensures only clean files are uploaded (and downloaded) by users via VDI
- Any file uploaded by user is scanned by 8 anti-malware engines to increase probability of finding the new malware
- Any file uploaded by user is recreated using CDR (Content Disarm and Reconstruction) technology to create a clear file and remove zero-day attack malwares
- Each file uploaded or downloaded can be tracked and audited

Accops' Contextual VDI Access

- Accops' restricts access to Virtual Apps & Desktops based on adaptive risks
- Access within VDI can also be controlled based on real time risk
  - When working from office, full access from VDI to app servers
  - When working from home, same VDI session but access is restricted to limited app servers
- User's can be locked to use specific device
- Device health is continuously monitored

Accops

- Established in 2012
- Headquartered in Pune, India
- 100% Make in India

500+ Enterprise customers

400,000+ Active Users

100+ Channel Partners

100+ Team Size

Worldwide Footprint

India I Japan I Dubai I USA
Germany I Peru I Tunisia

Technology Partners

Gold Microsoft Partner Microsoft

Brightstar

NUTANIX

cisco

aws partner network

HITACHI Inspire the Next

Centerm

FUJITSU

Members

International Association of Microsoft Channel Partners

TSANET

NASSCOM

#startupindia

Awards

Technical Innovation 2020 by ISA

IAMCP 2017 Partner Awards Silver Winner APAC

NASSCOM Product Conclave Top 5

InTech50

What do we do

Using our standard based

Zero Trust Network Access / SDP &

End User Computing Virtualization,

Identity & Access management technologies,

We enable organizations to

Consolidate, Secure & Speed up Access

to their IT infrastructure

Few Reference Customers

BFSI

AXIS BANK
Deutsche Bank
SvcBANK
IDFC FIRST Bank
THE NEW INDIA ASSURANCE COMPANY LTD.
LIC भारतीय जीवन बीमा निगम
SOUTH INDIAN Bank
एक्ज़िम बैंक EXIM BANK
देना बैंक DENA BANK
DENA GUJARAT GRAMIN BANK
Canara HSBC OBC Life Insurance
IndusInd Bank

FINANCIAL SERVICES

BAJAJ FINSERV
Fidelity INVESTMENTS
SBI MUTUAL FUND A partner for life
IDBI FEDERAL IDBI Federal Life Insurance Co Ltd
Liberty General Insurance
IndiaFirst
ADITYA BIRLA CAPITAL
RADIANT GROUP
Sharekhan
RSBL RIDDISIDDHI BULLIONS LTD.
GEOJIT BNP PARIBAS
IL&FS Securities Services Limited
fincare Small Finance Bank
Birla Sun Life Insurance
SBI General INSURANCE
IFFCO KISAN
FRR SHARES MAKES YOU REALISE

EDUCATION

ashoka UNIVERSITY
KYOTO UNIVERSITY FOUNDED 1897
Aptech COMPUTER EDUCATION
Tobago Library Services
FTII Film & Television Institute of India
CL educate
Bal Bharati PUBLIC SCHOOL
SARDAR PATEL VIDYALAYA
National Institute of Oceanography, Goa
K. R. MANGALAM WORLD SCHOOL
Rajarambapu Institute of Technology
rit

HEALTHCARE

WOCKHARDT HOSPITALS
LIFE WINS
شركة صيدلية المدينة CITY PHARMACY CO.
Ahalia Group UAE
RAJIV GANDHI CANCER INSTITUTE & RESEARCH CENTRE
SUBURBAN DIAGNOSTICS
tynor
Intercare Medical Centre
MAYARMED
مستشفى زليخة
مركز الشمس للطبي و التشخيص ذ.م.م al shams medical & diagnostic centre LLC
焼津市立総合病院 Yaizu City Hospital
Zulekha Hospital
MED FACHARZTZENTRUM
مستشفى الزهراء الشارقة AL-ZAHRA HOSPITAL SHARJAH THE HEALING TOUCH

PHARMACEUTICALS

WOCKHARDT
LIFE WINS
Bharat Biotech Lead Innovation
Safe International
Himalaya SINCE 1930
HIMEDIA FOR LIFE IS PRECIOUS
PHEONAX
BULK DRUGS ADPL Anjan Drug Private Limited
fbl Fermenta Biotech Limited
NUTRA
Plethico Pledged to Ethics
Mankind

GOVERNMENT

प ऊ वि DAE
NIC
NYPCL
हिन्दुस्तान पेट्रोलियम HP
DRDO
LIC
बी एच ई एल BHEL
محاكم دبي DUBAI COURTS
AIR INDIA
ABU DHABI FUND FOR DEVELOPMENT
茨城県 Ibaraki Prefectural Government
TATA POWER-DDL

MANUFACTURING

POLYCAB
SOMANY
ADITYA BIRLA GRASIM
Samsonite
THERMAX
YAZAKI
Varroc
SANDHAR Sandhar Technologies Limited
Birla Cellulose
YOKOHAMA
Nilkamal

IT & ITES & OTHERS

Tech Mahindra
NSEIT
ramco
ENVESTNET YODLEE
Microsoft
EQUIFAX
xpanxion UST Global Group
Flipkart
LARSEN & TOUBRO
Ecom Express
3i Infotech LIMITLESS EXCELLENCE

accops

Global Customers

ENVESTNET YODLEE
Fidelity INVESTMENTS
KYOTO UNIVERSITY FOUNDED 1897
MED FACHARZTZENTRUM
TATA STEEL
DUBAI COURTS
CCI
GELDERS ARCHIEF
Bacon CONSTRUCTION
Continental foods WHERE LOCAL BRANDS THRIVE
KOLEKTOR
COMMUNE DE 1030 SCHAERBEEK
JUNKERWERK
FRESENIUS KABI
AGIO ROYAL AGIO CIGARS CIGAR MAKERS SINCE 1904
TelekomSlovenije
Lunor eyewear
nalis
allied ALLIED STAR BUILDING MATERIALS TRADING L.L.C
Ahalia Group UAE

Dubai Courts
Al Shams Medical Centre
City Pharmacy LLC
Intercare
NLGI
Zulekha hospital
ABC International
Ahalia Medical Group
Desert Group
Allied Star Building Materials
Al Zahra Hospital
SAFE International
City of Ibbenbüren,
Ravago
CNC Grondstoffen B.V.,
Fresenius Kabi Horatev CZ
Gelders Archief
Kolektor Group d.o.o.
Fresenius Kabi Horatev CZ s.r.o
Continental Foods
MICRODYN-NADIR GmbH
Kalle GmbH

Kyoto University
Ibaraki Prefectural
Yamatotakada City
Kiyosu City
Arakawa Ward Office
Kitanihon Computer Service
Takatuki City
Higashikurume City
handbell care
Higashikurume City
Iwate Pref
Suginami Ward Ofiice
tagawa city
Yamatotakada City
Kitanihon Computer Service
Kumamoti City
Yaizu City Hospital
Nisshin City
Hachiouji City
individuelles betriebliches
Stadt Füssen
Wolfgang Thein GmbH
Continental Candy Industries

accops

VIRTUALIZE. SECURE. DELIVER.

sales@accops.com | http://accops.com

amazon web services | Partner Network

Microsoft Partner

redhat. READY ISV PARTNER

NASSCOM PRODUCT CONCLAVE 2016 Pune TOP 5

InTech50

RED HERRING ASIA 100 FINALIST