Panzer IT
MAKE IT SECURE

The Cyber Security Experts

MISSION STATEMENT

Continuous Secure Data Accessibility & Availability

www.PanzerIT.com

Type Of Protection

- Periphery Protection?
- Server Protection?
- Endpoint Protection?

- Accessibility
- Availability
- Backup, DR
- DLP
- Risk Management

Solutions

The Cyber Security Experts

Panzer IT
MAKE IT SECURE

Brands	Description
NETAND	Integrated Identity Management (IM) & Privileged Access Management (PAM)
scopd	Employee Monitoring, Risk Management, DLP, UBA
falcongaze	User Behavior Analysis, Employee Monitoring, DLP, Productivity
SOMANSA	Enterprise Data Leak Prevention, Data Discovery, Encryption
SECPOINT	Vulnerability Scanner & Assessment, Penetration Testing
EMSISOFT	Anti-Malware (Behavior based Prevention, AI, APT, Endpoint Security)
vembu Backup & Disaster Recovery	Data Backup & Disaster Recovery (Make in India)
Acronis	Automated Data Backup
Netop	Secure Remote Access, Remote Connect
LetsGoCart	eComm – Software Website

NETAND HIWARE

HIWARE, Integrated Identity and Access Management solution
actively responding to next-generation security paradigm

NETAND

What is HIWARE

Privileged Access Management for System

The beginning of the system security management are 'Manage' and 'Audit'.
HIWARE Privileged Access Management for System enables the complete management and supervision of users by controlling all accesses to, and operations of the IT infrastructure operating system such as network and server, monitoring work details in realtime and saving log records.

- ENHANCED USER AUTHENTICATION
- ACCESS AUTHORITY MANAGEMENT
- SYSTEM COMMAND MANAGEMENT
- REALTIME SESSION MANAGEMENT
- LOG RECORDING / AUDIT

Identity Management for System to work

Full and complete 'integration' and 'managing automation' are needed for easier and more powerful security.
HIWARE Identity Management for System manages all user accounts scattered across systems in an integrated fashion by interworking a client's HR system. It also automates the account and password management process for work efficiency and for more complete security.

- ACCOUNT LIFE-CYCLE POLICY MANAGEMENT
- PASSWORD POLICY MANAGEMENT
- INTEGRATED ACCOUNT POLICY MANAGEMENT
- DETECTION OF RETIREE/ INACTIVE/ ILLEGAL ACCOUNTS

Benefits of HIWARE

- Netand HIWARE is an integrated Identity Management (IM) and Privileged Access Management (PAM) solution which helps you balance security and efficiency at work by managing identities and access privilege.

- HIWARE PAM for System enables the complete management and supervision of users by controlling all accesses to and operations of the IT infrastructure such as network and server, monitoring work details in realtime and saving logs.

- HIWARE IM for Active Directory is developed to make up for a human error and security loophole from manual AD account management. It automatically manages AD accounts through consistent policies and unified management cycle by linking AD, HR system and server all together.

- HIWARE PAM for Database grants modular access to information in database differentially to each user and prevents information leak through SQL audit and log records.

- Integrated Solution for:
  - PSM for System
  - PAM for Database
  - IM for System
  - IM for Database
  - IM for Active Directory

Upgrade your security and work efficiency with implementing the integrated IAM solution in a single UI

HIWARE Identity management + HIWARE Access management

- Integrated UI
- Approval system
- Policy setting
- Audit report

Privilege Access Management

- Access control
- Command/Query control
- Result data control
- Log audit

Identity Management

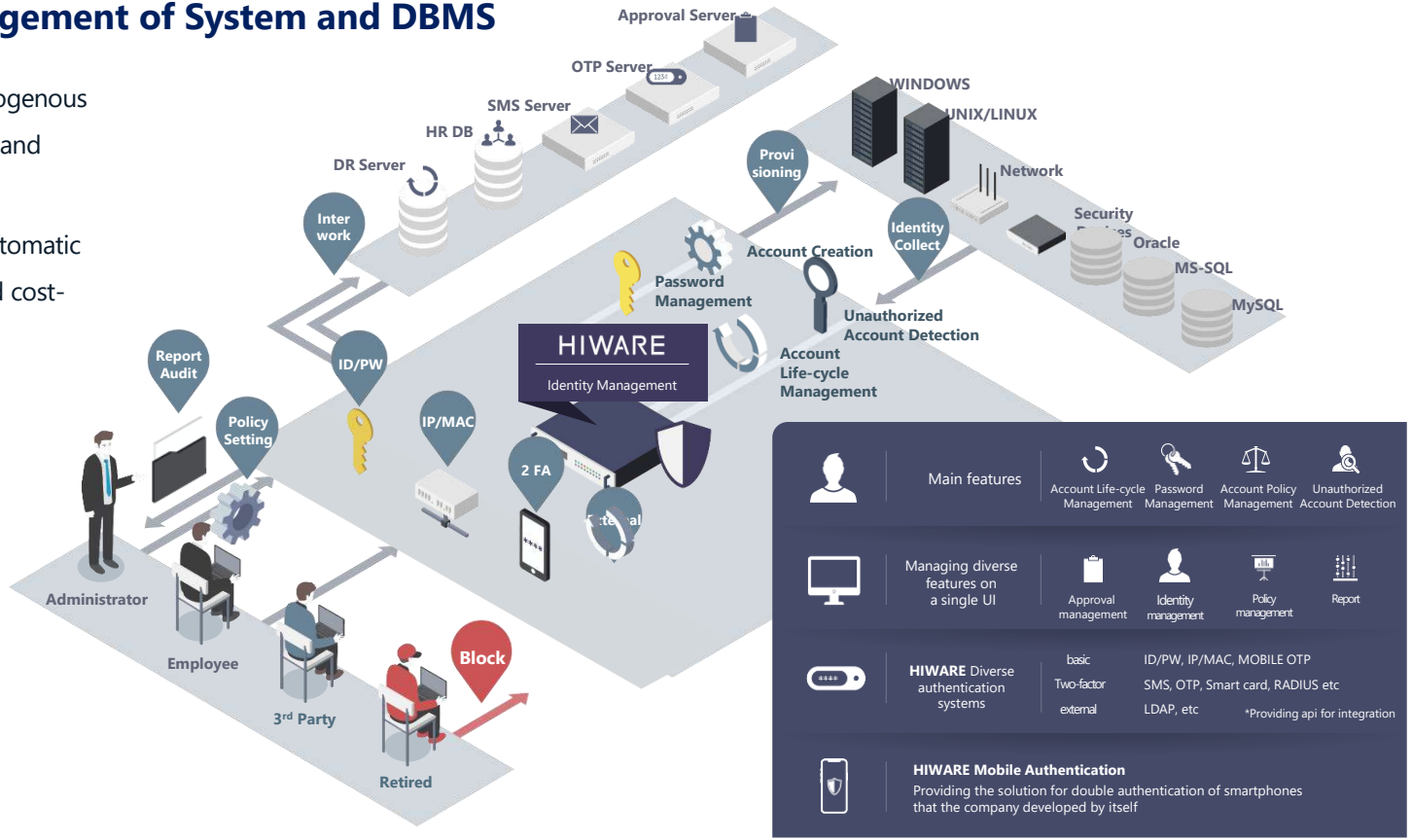
- Life-cycle management
- Password management
- Integrated account management
- Illegal account management

- Integrated UI
- Customizable functions
- Connectability
- Reinforced IAM management
- Monitor & Audit ready

HIWARE Identity Management of System and DBMS

HI-IM collects identities from heterogenous devices and manages the life-cycle and passwords through the policy.

Through main features can offer automatic reduce of the unnecessary time and cost-effective business environment.



Unauthorized Account Detection

Retired employees

Retired employees' accounts

Account deleted in the HR system since the concerned worker left the company
> Automatically blocked through integration with the HR system

Inactive

Inactive accounts

Account that there has been no Access history for a certain period

*** Need to integrate with Access control data**

Illegal

Unauthorized accounts

Ghost

Created illegal account which is in a device but not registered

Broken

Deleted unauthorized account which is registered but not in a device

HIWARE IM for Active Directory

Main features

- Account Life-cycle Management
- Password Management
- Account Policy Management
- Unauthorized Account Detection

Managing diverse features on a single UI

- Approval management
- Identity management
- Policy management
- Report

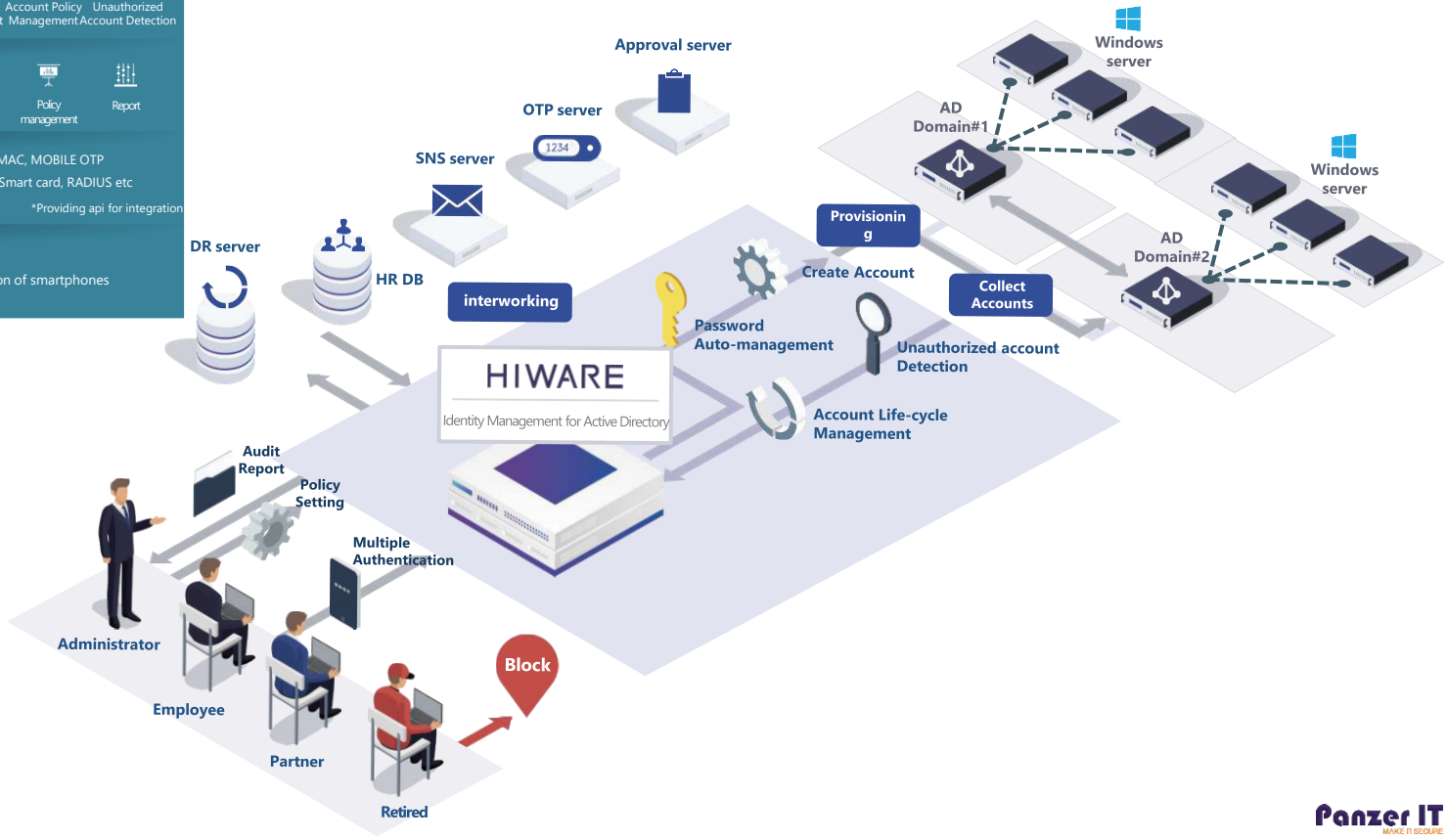
HIWARE Diverse authentication systems

basic	ID/PW, IP/MAC, MOBILE OTP
Two-factor	SMS, OTP, Smart card, RADIUS etc
external	LDAP, etc

*Providing api for integration

HIWARE Mobile Authentication

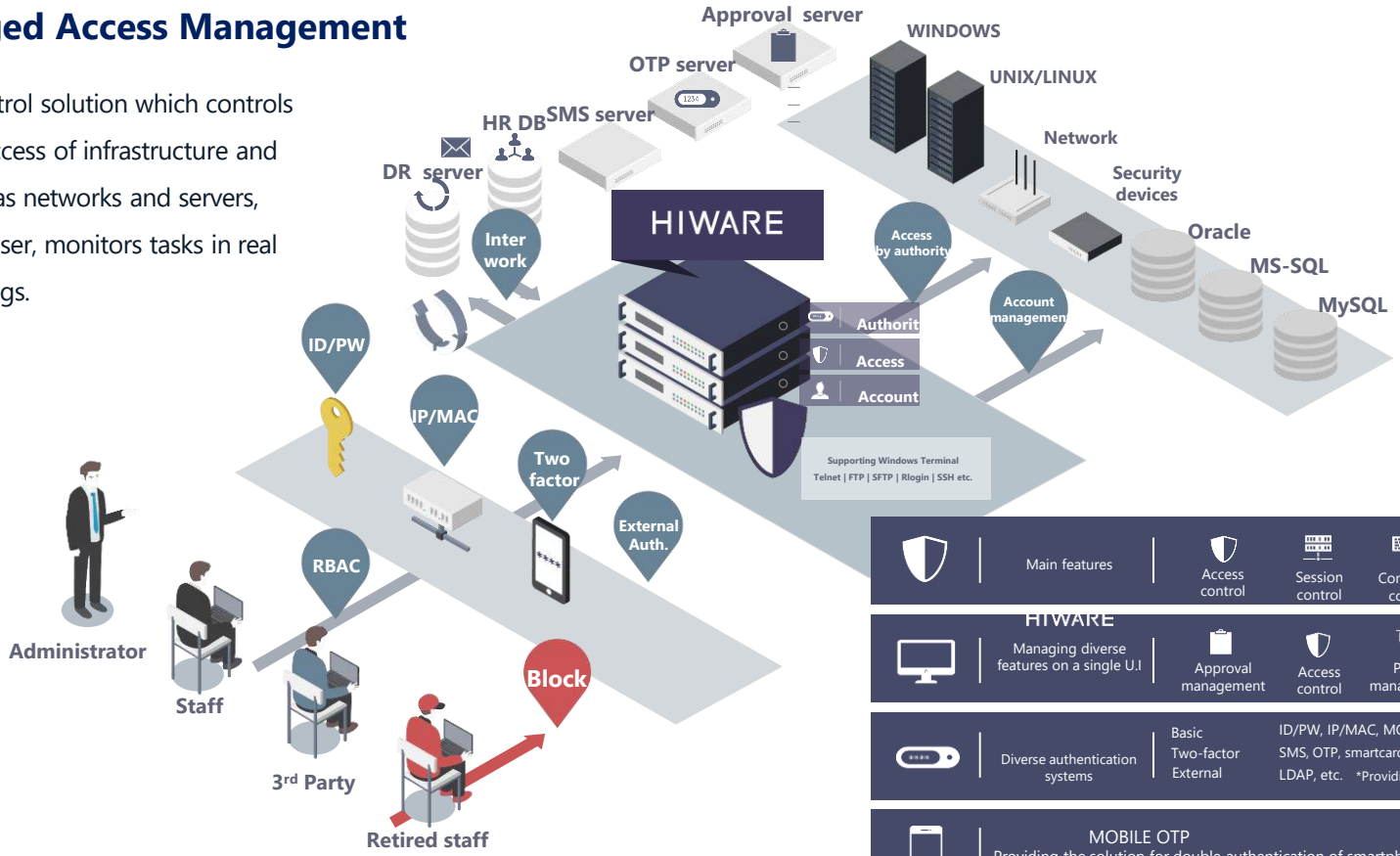
Providing the solution for double authentication of smartphones that the company developed by itself



NETAND

HIWARE Privileged Access Management

HI-PAM is an access control solution which controls and manages remote access of infrastructure and operation systems such as networks and servers, controls commands by user, monitors tasks in real time and creates audit logs.

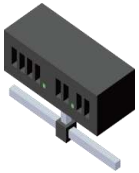


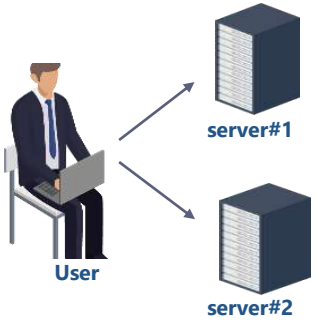
	Main features	Access control	Session control	Command control	Log audit
HIWARE	Managing diverse features on a single U.I	Approval management	Access control	Policy management	Report
	Diverse authentication systems	Basic Two-factor External	ID/PW, IP/MAC, MOBILE OTP SMS, OTP, smartcard, RADIUS, etc. LDAP, etc. *Providing api for integration		
	MOBILE OTP Providing the solution for double authentication of smartphones that the company developed by itself				

Reinforce User Authentication

NETAND

A user tries to access > ID/PW login > IP/MAC authentication > 2 factor authentication > Automatic login to devices





2 Factor Authentication

Basic	ID/PW, IP/MAC, MOBILE OTP
Two-factor	SMS, OTP, SSO, Smart card, RADIUS, PKI, biometrics, etc.
External	LDAP, etc. *Providing api for integration

HIWARE Mobile Authentication v1.0

Clients can save the cost to establish a security solution since we provide a mobile OTP product that we developed by ourselves

- Support Android/IOS
- Support off-line environment

Panzer IT
MAKE IT SECURE

System Command Control

NETAND

Permitted commands

Important commands

Inputting command

Worker

Processing depending on command policies

Permitted command — Immediately accepted

Important command — Confirmation text → Accepted

Prevent User's mistake

The command is executed.

Equipment

Prohibited command

prohibited command	Warning Massage	Not accept command	Block if N times of attempts to input	Notification
 Risky user	 Warning! Bad Command!		 Access Denied	  Administrator

Exceptions

Access for approval	Filling request form	Request approval	Administrator's approval	Using the command within a period
  User	 Time  Device  Command		 Administrator	  Possible to use the requested command

Panzer IT
MAKE IT SECURE

DBMS Query Control

NETAND

Permitted query

Inputting a query → **Processing depending on query policies** → **The query is executed**

Worker

Permitted query

Immediately accepted

Preventing a security incident caused by a user's mistake

DBMS

Prohibited query

Inputting a prohibited query → **Warning Massage** → **The query is not accepted.** → **Block if N times of attempts to input** → **Notification to an administrator**

Risky user

Warning!
Bad query!

Access Denied

Administrator

Exceptions

Access for approval → **Filling in a request form** → **Requesting approval** → **Administrator's approval** → **Using the query within a period**

User

Time
DBMS
query

Administrator

Possible to use the requested query

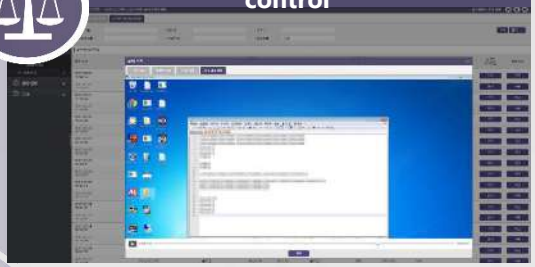
Panzer IT
MAKE IT SECURE

Real-time Session Monitoring & Control

- Real-time session monitoring
- Event monitoring
- Forcibly blocking users' session
- Providing real-time dashboard
- Session timeout

Real-time session statistics

Real-time event monitoring & control



Real-time session monitoring & control

References

Global Clients

Philippine SMART Communications	Cambodia ACLEDA Bank	Philippine RCBC Savings Bank	Shinhan Bank Japan

Manufacturing / Businesses

SAMSUNG	LG	ebay	HYUNDAI-KIA MOTORS	HYUNDAI HEAVY INDUSTRIES CO.,LTD.	GS	SK C&C
KOREAN AIR	Asiana Airlines	lotte.com	NEXON	MINI STOP	the Galleria	KORAIL

Finance

Standard Chartered	ING	Cigna	CIMB	CARDIF	BCcard	KEB
SAMSUNG	FINANCIAL SUPERVISORY SERVICE	SHINHAN BANK	kakaobank	LOTTECARD	Dongbu Securities	KDB

Public

central administrative agency of Korea

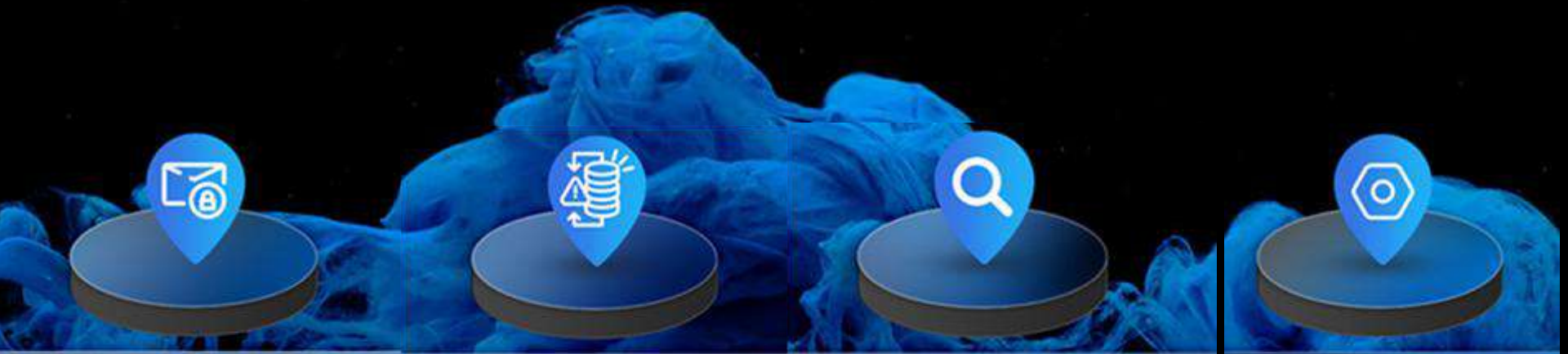
KISA	Ministry of Trade, Industry and Energy	Ministry of Strategy and Finance	Ministry of Culture, Sprots and Tourism	Fair Trade Commision	Defense Acquisition Program Administration	Korean National Police Agency
SUPREME COURT OF KOREA	Constitutional Court of Korea	KEPCO	KOREA POST	KoROAD	KORAIL NETWORK AUTHORITY	SEOUL

Broadcasting/telecommunications

olleh kt	SK telecom	CJ	KBS	MBC	SBS

A lightweight DLP solution tightly integrated with employee monitoring and insider threat detection.

Key Benefits of SCOPD: Real-Time Protection and Risk Mitigation



System Block & Alerts

Immediate blocking of compromised systems and real-time alerts to security teams.

Data Loss Prevention & Classification

Prevent unauthorized sharing of sensitive information by classifying data based on its importance and ensuring proper protection.

Insider Threat Detection

Monitor user behavior to identify potential internal risks before they escalate.

Compliance

Ensure alignment with data protection regulations like GDPR to avoid penalties.

Scopd - Why

- **Scopd** is not just an DLP with UBA solution, its much more than that. Scopd can improve productivity, increase revenue, improve profits and safeguard data.
- Scopd can be used for
  - Data Leak Prevention
  - Insider Threat Management
  - Employee Monitoring
  - User Behavior Analysis
    - Finding Disloyal Employees, Getting to know in advance who wants to leave job
  - User management
  - Endpoint management
  - Most importantly Safeguard Confidential & Crucial Data

See the Unseen, Secure the Unknown

Powered by UEBA (User and Entity Behavior Analytics) — transforming behavioral insights into proactive security.

Scopd - Highlights

- SCOPD is a comprehensive user behavior analysis & monitoring and security solution designed to enhance business efficiency & data security through various key features:
- Data Loss Prevention (DLP): Offers quick start and easy configuration of leakage monitoring, including a search engine to locate files on client machines and triggers for registering DLP events.
- Computer Monitoring: Record screens, capture screenshots, track user activity on the internet & in applications to monitor workflow
- Time Tracking and HR Analytics: Enables the creation of systems for analyzing employee performance, revealing real capabilities and achieved results.
- Remote Employee Monitoring: Provides tools to monitor remote workers, detect security threats, and prevent data leaks, ensuring productivity and security across various work environments.
- Biometric Authentication and Physical Security: Features include face recognition via webcam, analysis of keyboard handwriting, and prevention of screen photos, contributing to a zero-trust security policy.
- Analytics Report Group: Provides comprehensive assessments of individual employees and departments' effectiveness in a 24/7 mode, facilitating informed management decisions.

These features collectively provide organizations with the tools needed to monitor employee activities, enhance productivity, and ensure data security.

SCOPD Data Loss Prevention (DLP)

Prevent Sensitive Information from Leaving Your Organization

SCOPD DLP protects business data across multiple leakage channels:

- USB & Removable Media
- Internet Uploads
- Email Attachments
- Clipboard Operations
- Printing
- Document Reading
- Voice/Speech Monitoring
- Screen OCR

Flexible Response Options

- ✔ Monitor & Audit
- ✔ Classify Sensitive Files
- ✔ Alert Security Team
- ✔ Block Unauthorized Actions

Scopd - Key DLP Capabilities

Capability	Description
Content Inspection	Detect confidential information using keywords and Regular Expressions
USB Protection	Monitor or block copying to removable media
Internet Upload Monitoring	Detect or block file uploads to websites and cloud services
Clipboard Monitoring	Detect sensitive copy/paste activities
Print Monitoring	Monitor printing of confidential documents
Shadow Copy	Store copy of transferred files for forensic investigation
Document Classification	Search, discover & classify sensitive files
OCR Support	Detect text inside screenshots and images
Central Policy Management	Configure policies from a single console

Scopd - DLP Coverage Matrix

Data Leakage Channel	Monitor	Alert	Block
USB Drives	✔	✔	✔
Shared Folders	✔	✔	✔
Internet Uploads	✔	✔	✔
Email Attachments	✔	✔	✔
Clipboard	✔	✔	✔
Printing	✔	✔	✔
Documents	✔	✔	✔
Images (OCR)	✔	✔	✔
Voice/Speech	✔	✔	✔

Scopd - Features

Scopd - DLP with Employee Monitoring

- Employee monitoring for Windows, Mac, Linux and DLP for Windows
- Active and non-active time tracking
- Application, Websites, Data Transfer, web search
- Late arrival, Early departure, overwork, underwork
- Face recognition to find if unauthorised user working on PC
- StopPhoto: Prevent screenshot and taking screen photo from Mobile
- User behaviour analysis, changed behaviour, working pattern
- Stop Data Leaks for crucial data based on type, keywords, regex
- OCR, file hashes, data discovery, file search
- File Audit: move, copy, delete
- Live Audio, video, screen, mic monitoring
- Risk Analysis and alerts
- Compare employees, branches & department working pattern
- Achieve Compliance DPDP, RBI, SEBI, IRDA, GDPR etc
- Realtime desktop alerts
- Web-console: access anytime, anywhere, any device
- Hardware & Software Inventory of all device
- Domain Integration
- PostgreSQL, MS-SQL support ---More--
- Productive and non-productive time tracking
- Login-logout time; timesheet
- Top performers, Top violators
- Application & website blocking
- Geolocation tracking to find employee location
- Lock PC in case of unauthorised usage
- DLP for sending, upload, copy, printing, reading
- Email, USB drives, web uploads, printouts, messengers
- Central messaging and lock every PC in organization
- Screen recording, Periodic Screenshot capture
- Insider threat investigation
- LLM Integration
- Export reports to HTML, PDF, xls
- Reports on email, FTP, shared folder, web upload
- Customised console for HOD, HR, IT, CXO
- Silent or announced monitoring
- Uninstall protection & alert

scopd

Search

Basic functions


General information


Apps/windows list


Current screen

Live screen

Additional functions


Webcam images

Live webcam


Live audio

Speech to text


Search in files


Pause/resume of monitoring

Message and locking


Message only


Message and Lock


Block mouse and keyboard


Hard block for a while

Admin functions (computer)


Reboot


Power off


Execute command

Client log request


Update client software


Uninstall client software (and


Uninstall client software (keep

All reports | Favorite reports

Search


Files sending


File operations


Printing


File classification


Search in files

Event and activity monitoring


Events: user


Screenshots


Screenshots video


Search by templates


Face recognition

Internet searches


Chats/calls


Conversations analyzer


Mails (e-mail)


Contacts


Contacts graph

Contacts graph (3D)


Clipboard


Audio recording

Files sending

2026-07-01 / 2026-07-27

22 Employee

MS Excel | OpenOffice Calc

Vocabulary	Count	Vocabulary	Size, MB
	2586		152961.8
Productive	726	Productive	4010.8
Unproductive	2	Unproductive	2.8
Total	**3114**	**Total**	**156975**

view 523 from 3114

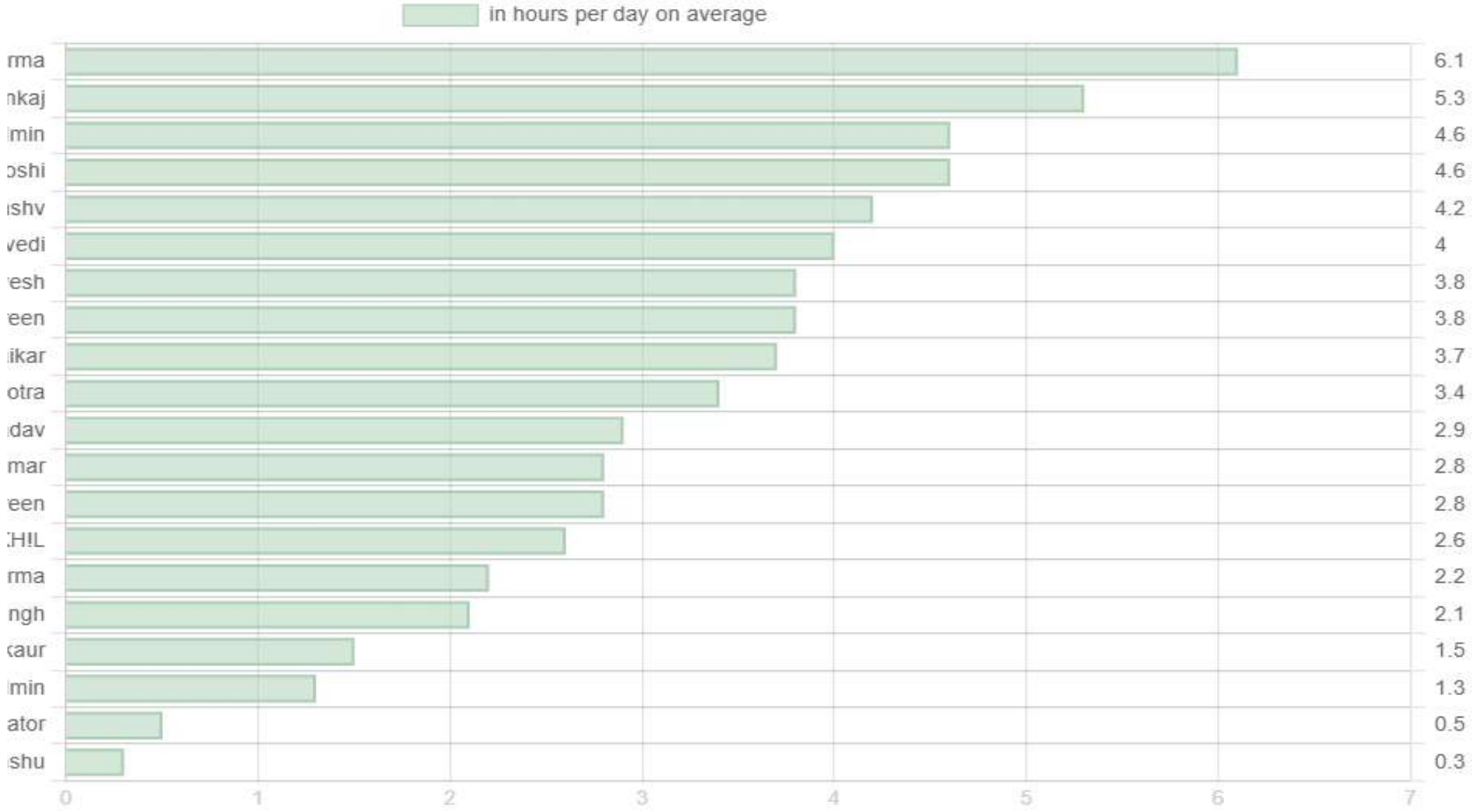
Search

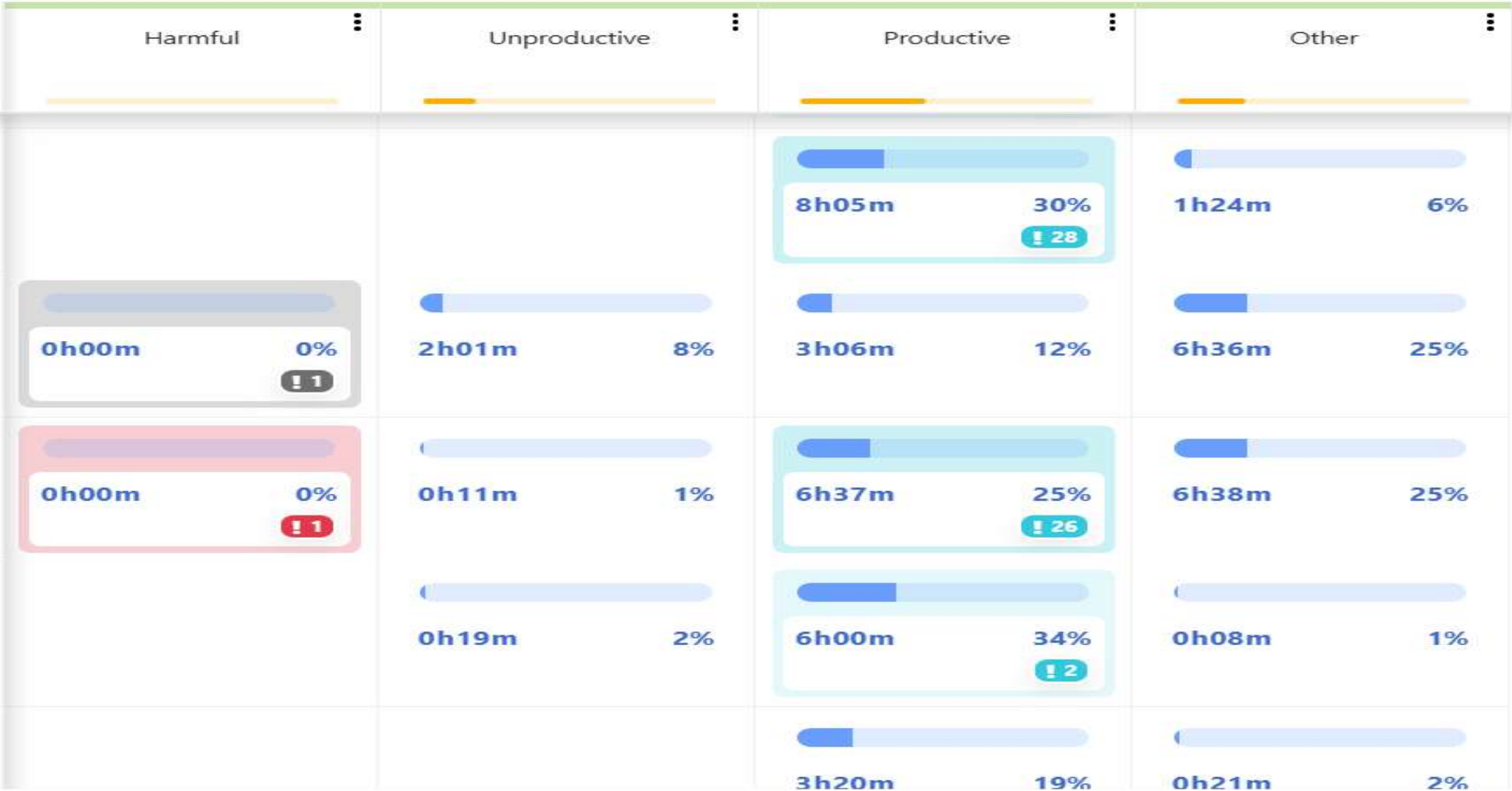
#	User	Time	Size, KB	Type	File	Application/Site	Destination
	sarvesh						
2417	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-01 15:18:56	2725	.rar	D:\Help - PanzerIT\SecPoint\Customers VAPT report\Western India Forgings\VAPT_Scan_Western India Forgings.rar	Microsoft Outlook	Inbox - sarvesh@panzerit.com - Outloo (OUTLOOK.EXE)
2418	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-02 17:44:49	106	.jpeg	C:\Users\Sarvesh\Downloads\WhatsApp Image 2026-07-02 at 17.41.02.jpeg	web.whatsapp.com	https://web.whatsapp.com
2419	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-03 18:18:23	1524	.pdf	C:\Users\Sarvesh\Pictures\Digital-Personal-Data-Protection-Act.pdf	web.whatsapp.com	https://web.whatsapp.com
2420	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-03 18:18:35	1524	.pdf	C:\Users\Sarvesh\Pictures\Digital-Personal-Data-Protection-Act.pdf	web.whatsapp.com	https://web.whatsapp.com
2421	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-04 18:25:09	3	.html	C:\Users\Sarvesh\Downloads\PanzerIT_Partner_Mailer_v2.html	web.whatsapp.com	https://web.whatsapp.com
2422	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-04 18:33:58	2893	.pdf	C:\Users\Sarvesh\Downloads\Blue Lotus Capital Advisors LLP Work	chatgpt.com	https://chatgpt.com
2423	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-06 14:15:27	550	.pdf	D:\Help - PanzerIT\SecPoint\Sample Reports\VAPT_Scan_Server.pdf	web.whatsapp.com	https://web.whatsapp.com
2424	PIT-DELL-SARVES\Sarvesh (Sarvesh)	2026-07-06 14:51:39	553	.pdf	D:\Help - PanzerIT\SecPoint\Sample Reports\VAPT_Scan_Server.pdf	Microsoft Outlook	Untitled - Message (HTML) (OUTLOOK.EXE)

View by all (3,114)

Page 1 from 1

1


in hours per day on average
rma
nkaj
min
oshi
ishv
vedi
esh
een
ikar
otra
dav
mar
een
CHIL
rma
ngh
kaur
min
ator
shu
6.1
5.3
4.6
4.6
4.2
4
3.8
3.8
3.7
3.4
2.9
2.8
2.8
2.6
2.2
2.1
1.5
1.3
0.5
0.3
0
1
2
3
4
5
6
7


Harmful
Unproductive
Productive
Other
8h05m 30% 28
1h24m 6%
0h00m 0% 1
2h01m 8%
3h06m 12%
6h36m 25%
0h00m 0% 1
0h11m 1%
6h37m 25% 26
6h38m 25%
0h19m 2%
6h00m 34% 2
0h08m 1%
3h20m 19%
0h21m 2%

Deviations

2026-07-25 / 2026-07-27

62 Employee

MS Excel | OpenOffice Calc

Categories | By hierarchy | By departments | By employees | Deviations | Resources

268 rows

Search

#	Category	Application/Site	Value	Total by category	Tot
1	**Other**	"WhatsApp.Root"	4h55m	**32h21m**	
2	**Other**	resdex.naukri.com	3h53m	**32h21m**	
3	**Other**	outlook.cloud.microsoft	2h22m	**32h21m**	
4	**Other**	hurawatch.sx	2h07m	**32h21m**	
5	**Other**	cineby.at	1h55m	**32h21m**	
6	**Other**	"ChatGPT Classic"	1h23m	**32h21m**	
7	**Other**	"%ProgramFiles%\Talk\PrimeEditLog\talk.exe"	1h19m	**32h21m**	

View by all (268)

Page 1 from 1

1

Deviations

2026-07-01 / 2026-07-27

62 Employee

MS Excel | OpenOffice Calc

Categories | By hierarchy | By departments | By employees | Deviations | Resources

92 rows

Search

#	Category	...	Value
30	**Time at work (average)**	Accounts	0h00m
31	**Time at work (average)**	Sales	209h50m
32	**Time at work (average)**	Tech	223h54m
33	**Active time (average)**		26h41m
34	**Active time (average)**	Accounts	0h00m
35	**Active time (average)**	Sales	112h27m
36	**Active time (average)**	Tech	103h03m

View by all (92)

Page 1 from 1

1

Scopd System Requirements

Server (Windows):	Win10/11/2012/2016/2019/2022 and latest OS versions (32/64-bit) – Onprem or hosted cloud
Client (Windows):	XP(SP3)/2003/Vista/Win7/2008/Win8/2012/Win10/11/2016/2019/2022 and latest OS versions (32/64-bit)
Client (Linux):	Astra, CentOS, Debian, Mint, Ubuntu, Rosa, RED OS (full list)
Client (MacOS):	El Capitan, Sierra, High Sierra, Mojave, Catalina, Big Sur, Monterey, Ventura
SQL server:	MS SQL Server (minimum 2008), PostgreSQL (minimum 11)
Operation in terminals:	supported
Supported PACS systems:	Sigur (Sphinx)


falcongaze

SecureTower – DLP + UBA

- Control of Data Transfer Channels
- Detection of Sensitive Data Content
- Data Leak Prevention
- Incident Response
- Productivity Analysis | Employee Monitoring
- Archive of Intercepted Data
- Extensive & Custom Reports
- Modular, group wise access for policies & reports

SecureTower – DLP + UBA

SecureTower controls data-in-use, data-at-rest and data-in-motion

Network control

Mail processing server
- **EWS (MS Exchange)**
- **POP3**
- **SMTP**
- **IMAP**

SPAN-port
- **Mail**
- **WEB**
- **Messengers**
- **FTP**

ICAP-server
- **WEB**

Data discovery
- **Full archive of all intercept data**
- **Indexing files**
- **Search engine**
- **Security center & Reports engine**
- **OCR, Voice, Identity**
- **Credit Cards, PAN, Aadhar, Account**

Endpoint control

Endpoint agents
- **Mail, WEB**
- **Messengers**
- **External devices, Printer**
- **FTP(S), Apps, Torrents**
- **User activity**

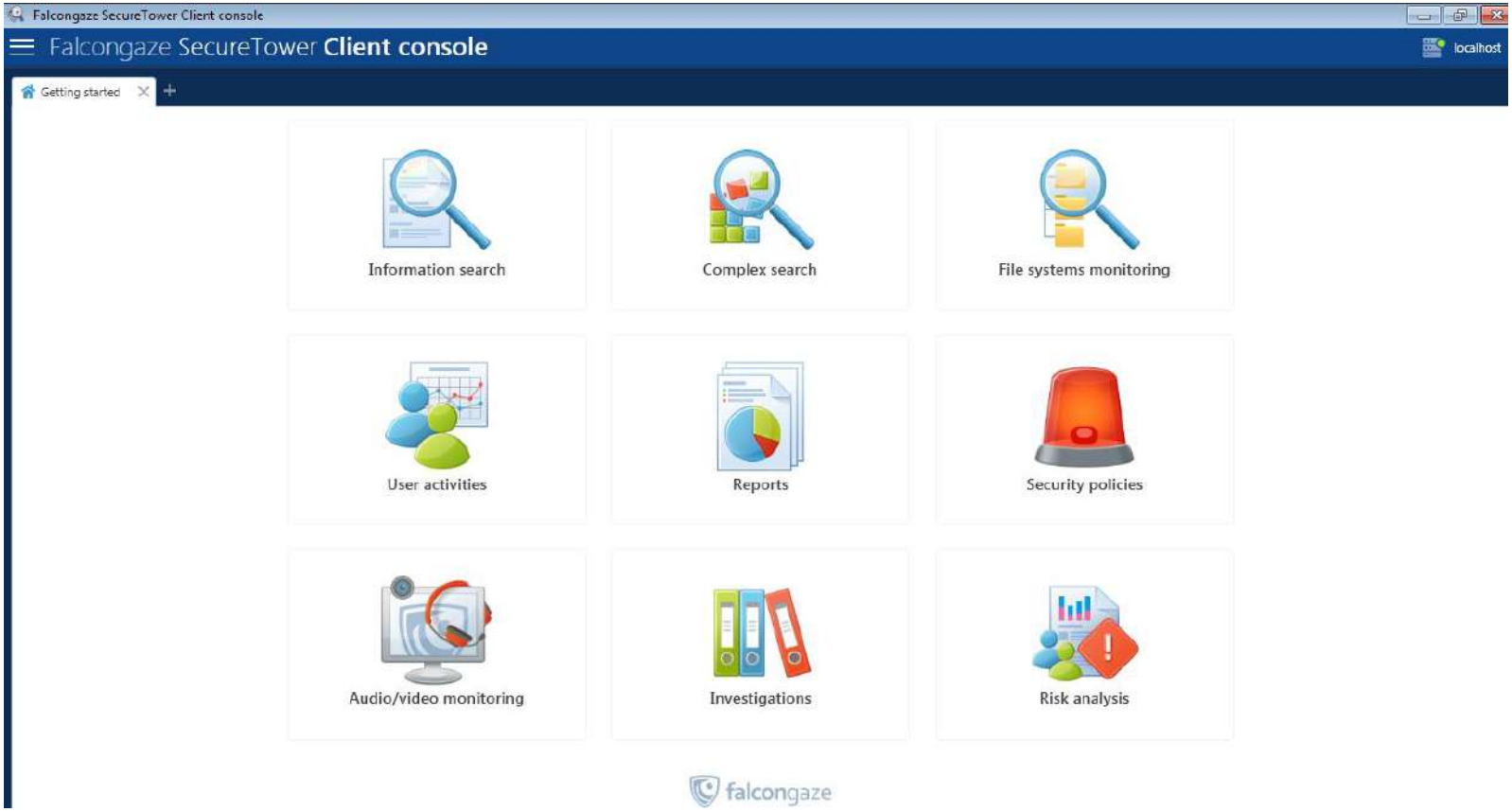
E-mail
- **Protocols:** POP3, SMTP, IMAP, MAPI
- **Mail servers:** Microsoft Exchange Server, Lotus Notes, Postfix, Sendmail
- **Web-based:** Gmail, O365, Yahoo.Mail, and other

Workstation control
- **Scanners**
- **Printers**
- **CD/DVD**
- **External devices**
- **Clipboard**

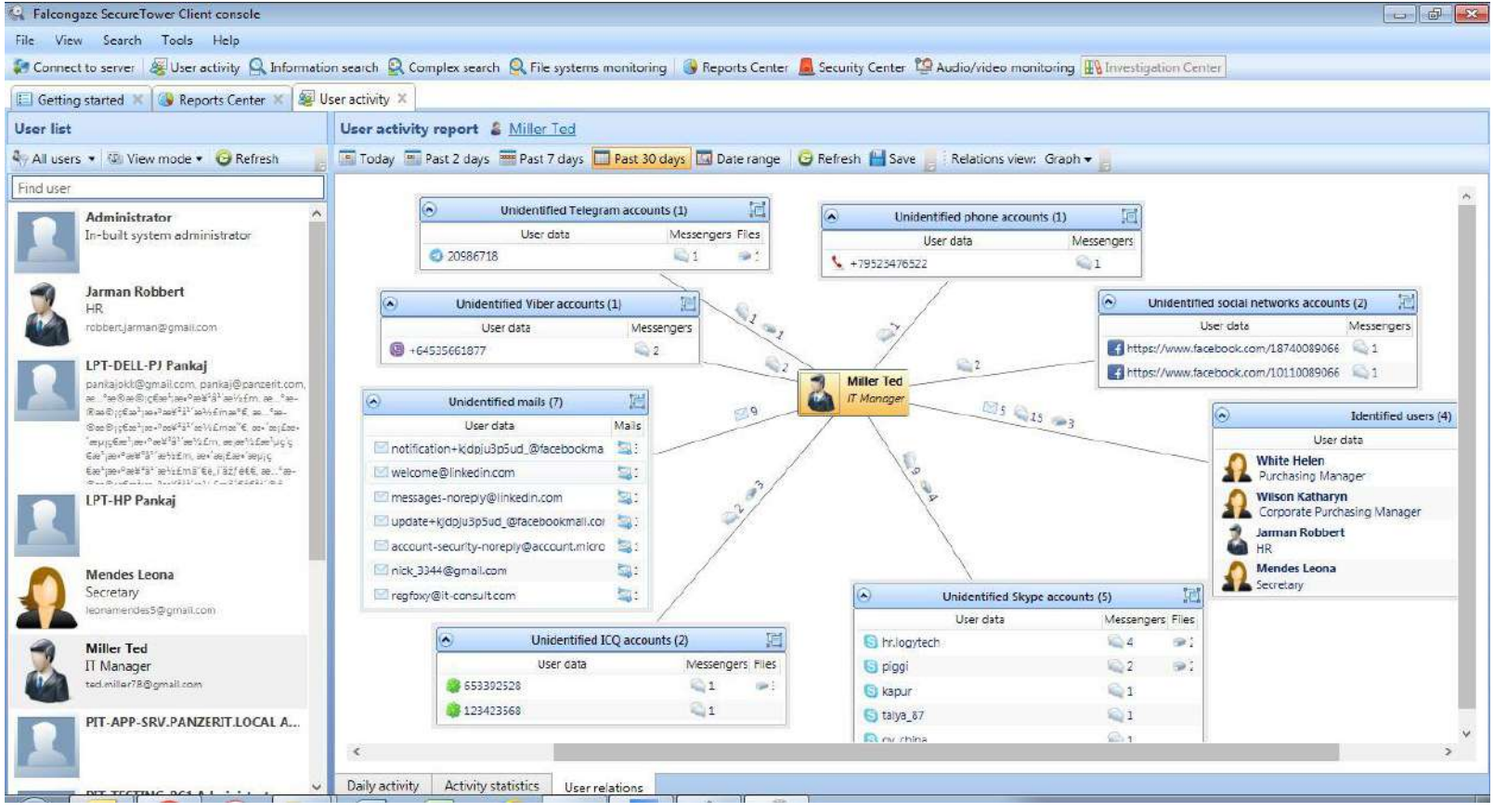
Cloud storage
- **Clients:** OneDrive, iCloud, Google Drive, Dropbox, Yandex.Drive
- **Web-access:** all

Social networks
- **Integrations:** Facebook, LinkedIn, Vk.com
- **Other:** blogs, online chats, forums

SecureTower – DLP + UBA

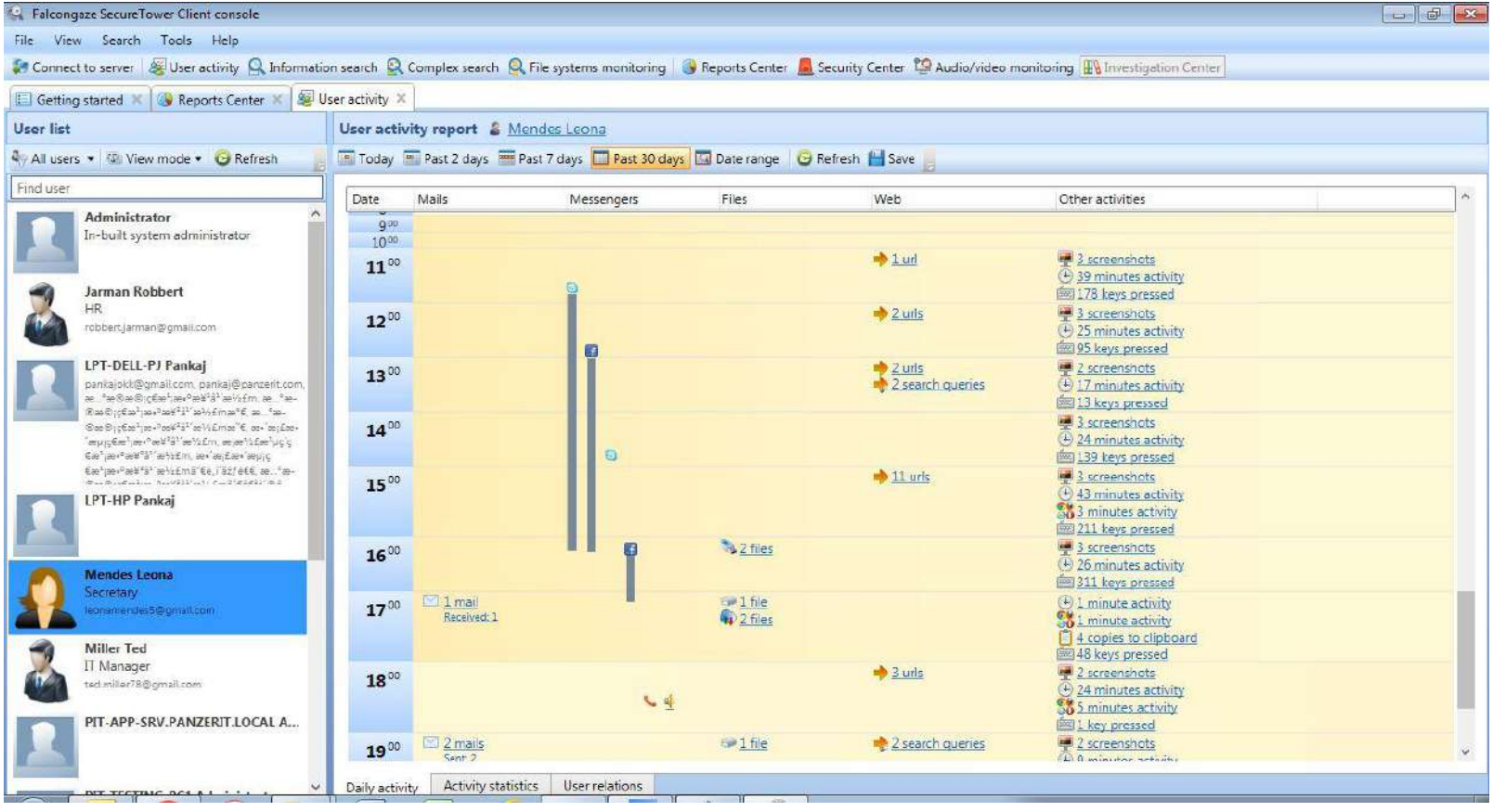


SecureTower – DLP + UBA



falcongaze™

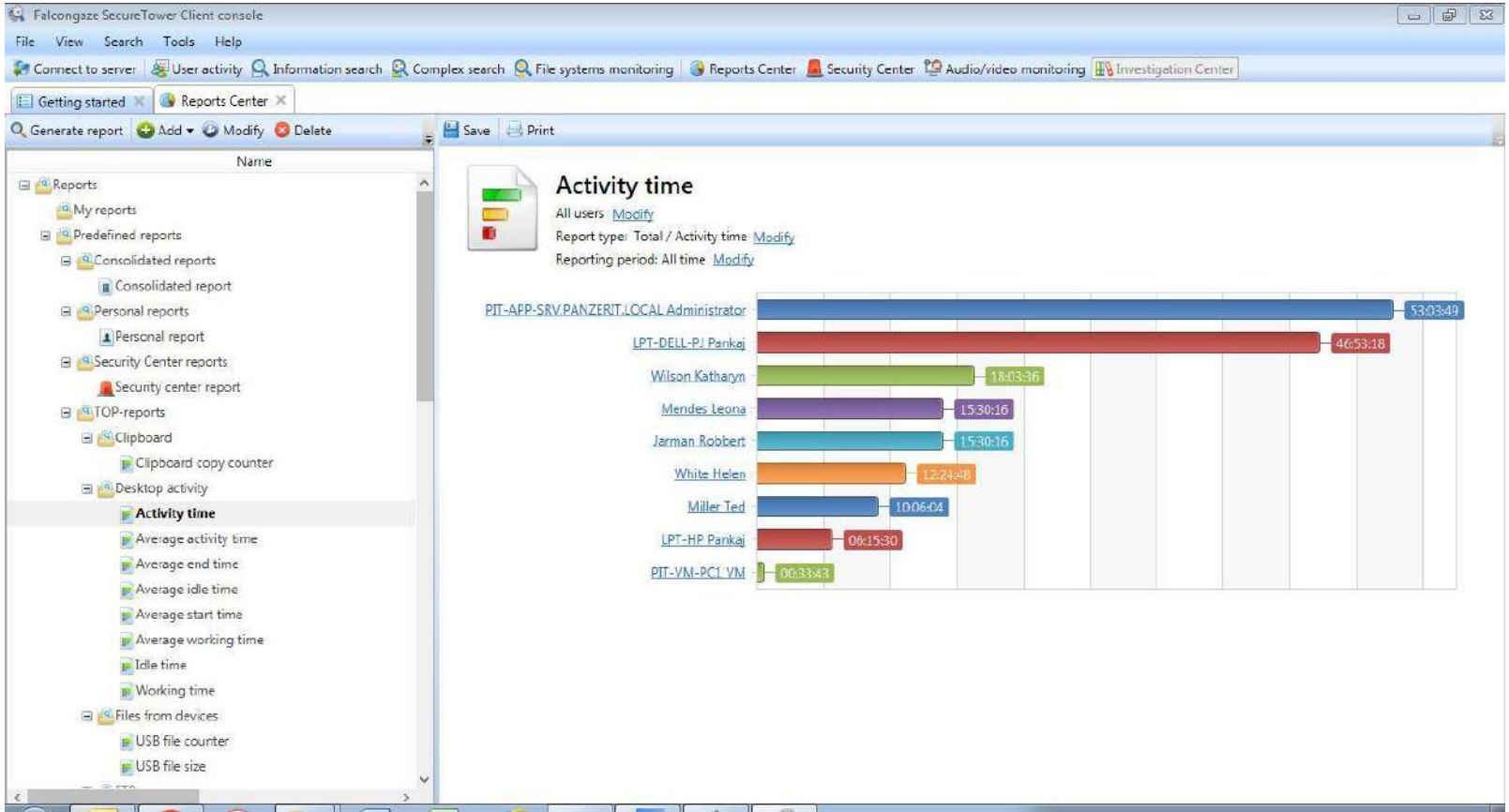
SecureTower – DLP + UBA



Panzer IT
MAKE IT SECURE

falcongaze™

SecureTower – DLP + UBA



Panzer IT
MAKE IT SECURE

SOMANSA

Somansa: Privacy-i Endpoint DLP

SOMANSA

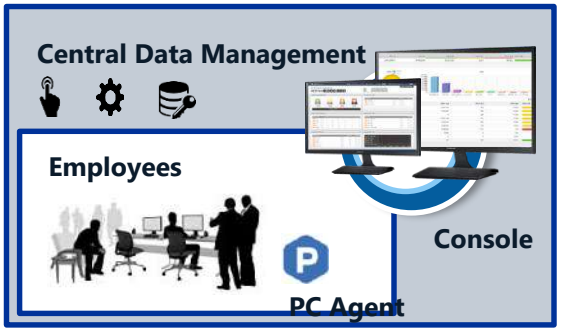
Privacy-i and Data Security Process

❖ **Privacy-i protects sensitive data at rest**

- Privacy-i is designed to follow phases set out in the data protections laws

DISCOVER Sensitive Data

- Scan and Locate sensitive data (PCs, Servers, Databases)
- Encrypt or Delete Data

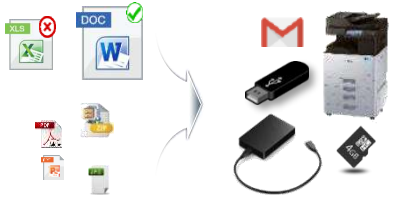


Strategy 1

- Define, Who, What, Where Sensitive Data Stored.
- Complete visibility of sensitive data within the organization

PREVENT Data Breach

- Prevent data breach via removable storage, printer, network services(e.g. email)



Strategy 2

- Create breach prevention policy tuned for each organization
- Monitor for policy violations, block unauthorized use of removable disk, printer, or upload on the internet

REPORT

- Real-time Alerts of incidents
- Event logs and forensic evidence

Strategy 3

- Real-time event monitoring, log analysis, user/file activity analysis help security team to detect, respond to potential breach
- Audit trail for compliance

Somansa: Mail-i Network DLP

SOMANSA

Mail-i: E-mail & NetApps Control/Monitor

Mail-i protects sensitive data in motion

- Mail-i Logs outgoing data in a real-time (email, social media, messenger, cloud service, etc)

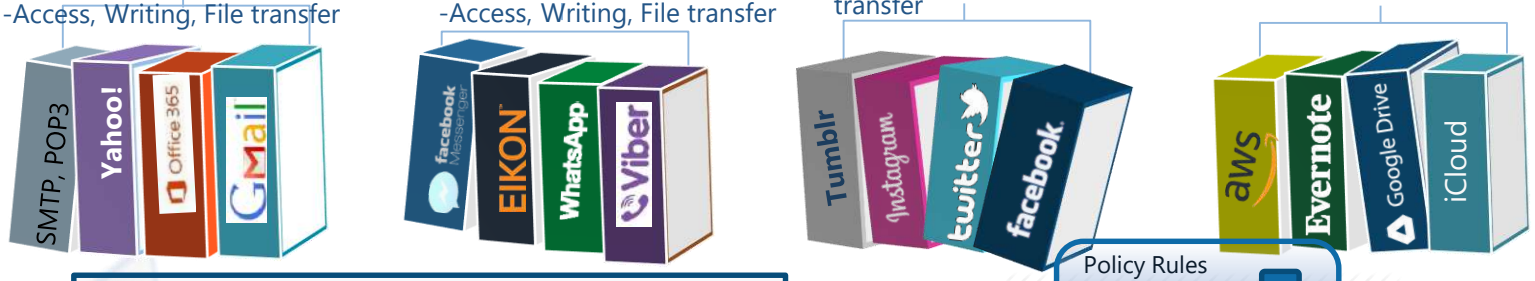
Mail-i data Logging & Granular Control

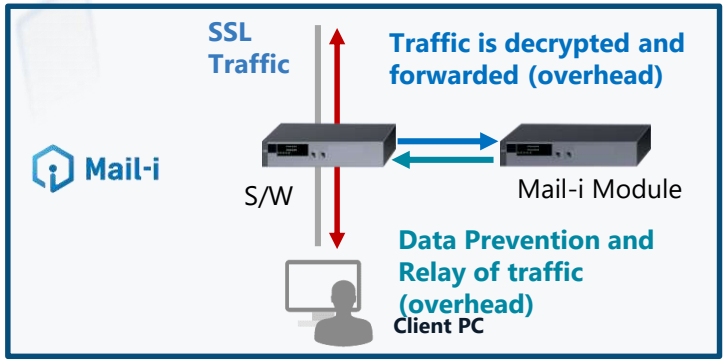
E-mail(SMTP, POP3, IMAP)
-E-mail data logging(real-time)
-Access, Writing, File transfer

Instant Messenger(Web, Apps)
-Support popular messengers
-Access, Writing, File transfer

Social Media
-Logs uploaded contents
-Access, Writing, File transfer

Cloud Storage
-Logs transferred data
-Control over various SaaS





SOMANSA'S STRENGTHS

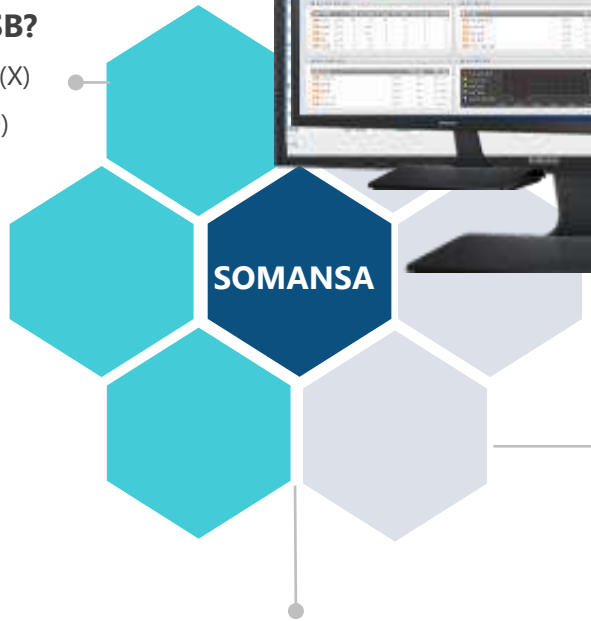
Do you want to use only approved USB?

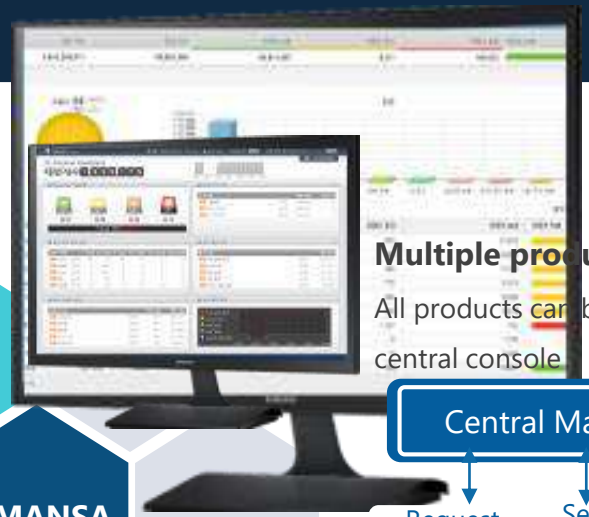
Unauthorized USB ➔ READ (X), WRITE (X)

Authorized USB ➔ READ (O), WRITE (O)

Must obtain approval to transfer files

Unauthorized transfer of data from desktop PC is blocked without permission / approval





Multiple products, One view

All products can be managed by one central console

Central Management

Request approval

Set Policy/ Apply

Block/Allow logs and copied files

Fast Search & Report Big Data

Return search results in max. 3 minutes (in millions of logs / more than 30 keywords)

Application Blacklist

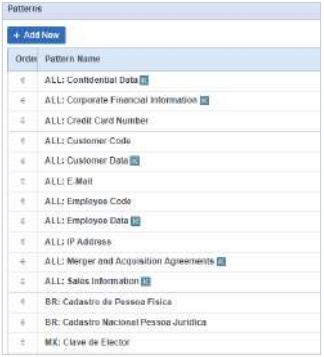
Allow to block dangerous applications

Structure of SOMANSA's DLP

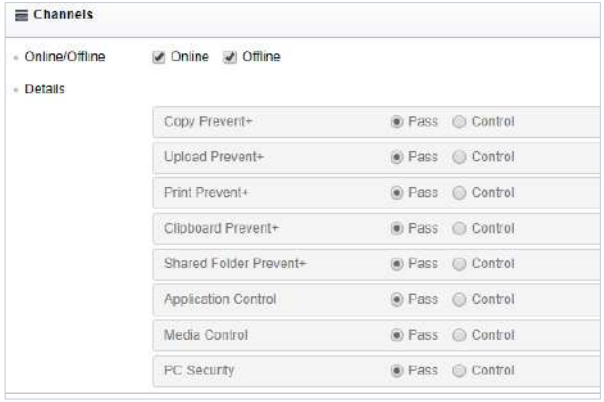
SOMANSA

Integrated Policies

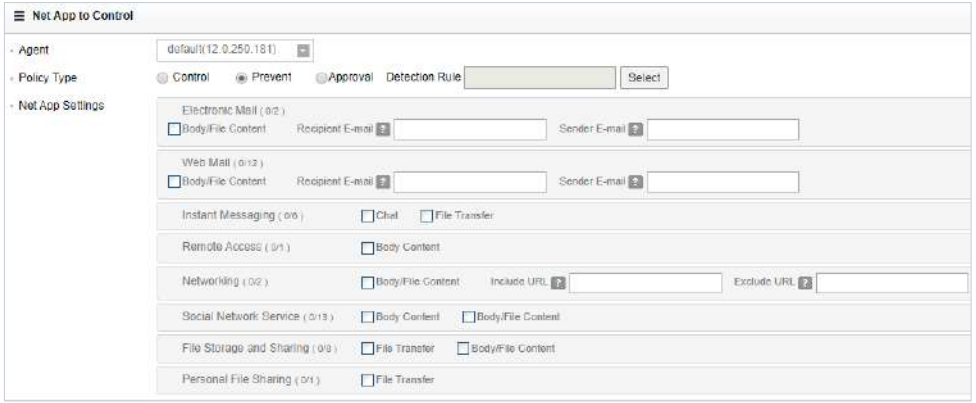
Integrated Management Control



Privacy-i



Mail-i



SOMANSA | Who we are ?

SOMANSA

Over 20 years experience

in Electronic Data Security and Management

Leader in Data Security

Data loss prevention (DLP) and database activity monitoring solutions

2000+ worldwide customer

from large enterprises to small and medium businesses

World's Top 10 Gartner Magic Quadrant

First and Only Asian Company

SC MAGAZINE

Gartner

Magic Quadrant

Enterprise DLP

CRN PARTNER PROGRAM GUIDE WINNER 2019

General Data Protection Regulation

HIPAA

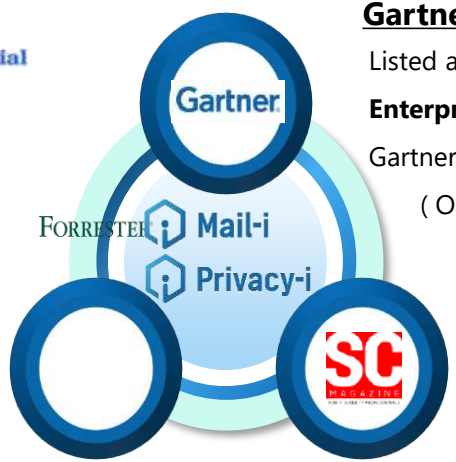
Gramm-Leach Bliley Act

PCI DSS COMPLIANT

Forrester Research

Global Top 10 DLP,

Top 7 Content-Aware DLP



Gartner Magic Quadrant

Listed as **the world's Top 10 Enterprise DLP solution** in Gartner Magic Quadrant (16-17)

(Out of 100+ Products)

SC Magazine UK

Endpoint DLP Product Review ★★★★½

4.5/5.0 Rating

Panzer IT MAKE IT SECURE


SECPOINT®
www.secpoint.com

SecPoint® Penetrator™

- 64 Bit High Performance
- Scans Local & Public IPs
- Best Vulnerability & Assessment Scanning
- Easy Solutions to found vulnerabilities
- Virtual VMware & Hyper-V Support

SecPoint® Cloud Penetrator™

- Web Vulnerability Scanner
- SQL Injection, XSS Scanning
- Scans Websites, Webshops, Firewalls
- No Software Required
- SCADA Vulnerability Scanning
- 11 Scan Profiles

SECPOINT

https://192.168.1.2/spscan/welcome.php

Search

SECPOINT
www.secpoint.com

PENETRATOR™
VULNERABILITY ASSESSMENT & WIFI PEN TESTING

admin

- Home
- Vulnerability Scanner 9
- Schedule
- AI Processing 2
- Statistics 2
- Tickets 3
- WiFi Pen Test 15
- Cloud Users 5
- Scan Distribution
- System 18
- Network Setup
- Update 4
- Support 19

SecPoint® Penetrator - Vulnerability Assessment & WiFi Pen Testing

List of Vulnerability Scans

Search

	Date	Scan Name	Profile	Progress	Risk					Options
☐	17-06-2020	LAN5	Quick Scan	Processing.. 6%	Low	0	0	0	0	
☐	16-06-2020	LAN4	Quick Scan	Complete	High	1	7	1	8	
☐	16-06-2020	LAN3	Quick Scan	Cancelled	Low	0	0	0	0	
☐	11-06-2020	LAN	Best Scan	Complete	High	2	14	9	21	
☐	06-11-2019	Ctm02	Best Scan	Complete	High	1390	1782	483	4106	
☐	28-10-2019	Ctm_26-09-2019_2	Best Scan	Complete	High	389	1322	352	673	
☐	21-08-2019	MCs_21-08-2019	Best Scan	Complete	High	42	2138	292	958	
☐	21-08-2019	MServers_21-04-2020	Best Scan	Complete	High	1084	243	31	484	
☐	21-08-2019	Fun 21-08-2019	Best Scan	Cancelled	High	1	4	12	12	
☐	19-08-2019	Fun 19-08-2019	Best Scan	Complete	High	1	7	1	7	

First Previous 1 2 Next Last

Panzer IT

Features and Benefits

No Data Collection, Backdoor Free	Distributed Scanning Capability	OS Independent Interface
30+ Scan Profiles, HIPAA,OWASP top 10, Prepare for	Advanced Web Crawler - SQL Injection - XSS - SSL	Bugtraq ID / Mitre CVE / Ubuntu USN /Microsoft / OSBDB
PCI, Firewall Scan, SCADA & more	Audits any OS	Automatic Web Crawl Script Engine
Launch Real Exploits	Scan any OS and Network devices	Multi User Support
Advanced Audit Options	Reports Branding	Launch Real Exploits
Schedule scans daily, weekly, monthly	Detailed Remedies for Identified Vulnerabilities	Ticket System for full Vulnerability Management
Prevent Hackers To Access Your Server	Secure Design All Data Stored on Unit	Option for centralized update point
Vulnerability Scanning	Option for syslog remote logging	Distributed Auditing
Vulnerability Assessment	Vulnerability Audit	XML, PDF and HTML Reports
100,000 + Vulnerabilities	Launch DoS & DDoS attacks	Finds SQL Injection

SECPOINT

Security Audit Features

- √ Vulnerability assessment
- √ 60.000+ vulnerabilities
- √ Unlimited auditing
- √ No software installation
- √ Advanced audit options
- √ Launch real exploits
- √ Security audit any OS
- √ Automatic web crawl script
- √ OS independent interface
- √ SANS top 20
- √ Malware Detection

Easy-to-understand Reporting

- √ XML PDF and HTML reports
- √ Reports branding allowed
- √ Option for syslog remote logging

Distribution Security Auditing

- √ Security audit remote locations from a centralized point
- √ Centralized reporting
- √ Centralized data storage
- √ Centralized control

Security Audit Configuration

- √ Virtual host auditing
- √ Audit specific ports
- √ Audit specific web directories
- √ Email notification when an audit is finished

Security Scanning of

- √ Wordpress, Drupal,Magento,Shopify,Umraco, Joomla, Webshops

Finds Cross Site Scripting, SQL Injection, SSL and Web Errors

- √ Automatic web crawling engine identifies known and unknown files on websites
- √ Finds Cross Site Scripting
- √ Finds SQL Injection
- √ Finds Web Errors
- √ Black Hat SEO Scanner
- √ Google Hack DB
- √ Extensive SSL checks

Multi User Support

- √ Supports multiple users to login at the same time
- √ Individual user accounts with different audit options and IP ranges
- √ Individual user security level
- √ Admin and regular users

Scheduled Auditing

- √ Automatic scheduled auditing
- √ Automatic alert about new identified security vulnerabilities
- √ Shows new vulnerabilities discovered and compares them with old records to show the progress in the security level

Scalable and Upgradeable

- √ All units can be upgraded for network growth via a software license
- √ Investment protection

Penetration Testing

- √ Launch real exploits for Windows, Unix, Routers, Firewalls and more
- √ Launch real denial of service attacks
- √ Launch distributed denial of service via distributed setup

Automatic Update

- √ Automatic daily database updates
- √ Automatic firmware updates with new features and functionality
- √ Centralized update point
- √ Automatic alerts when database is expired
- √ Option to upload updates manually via the interface

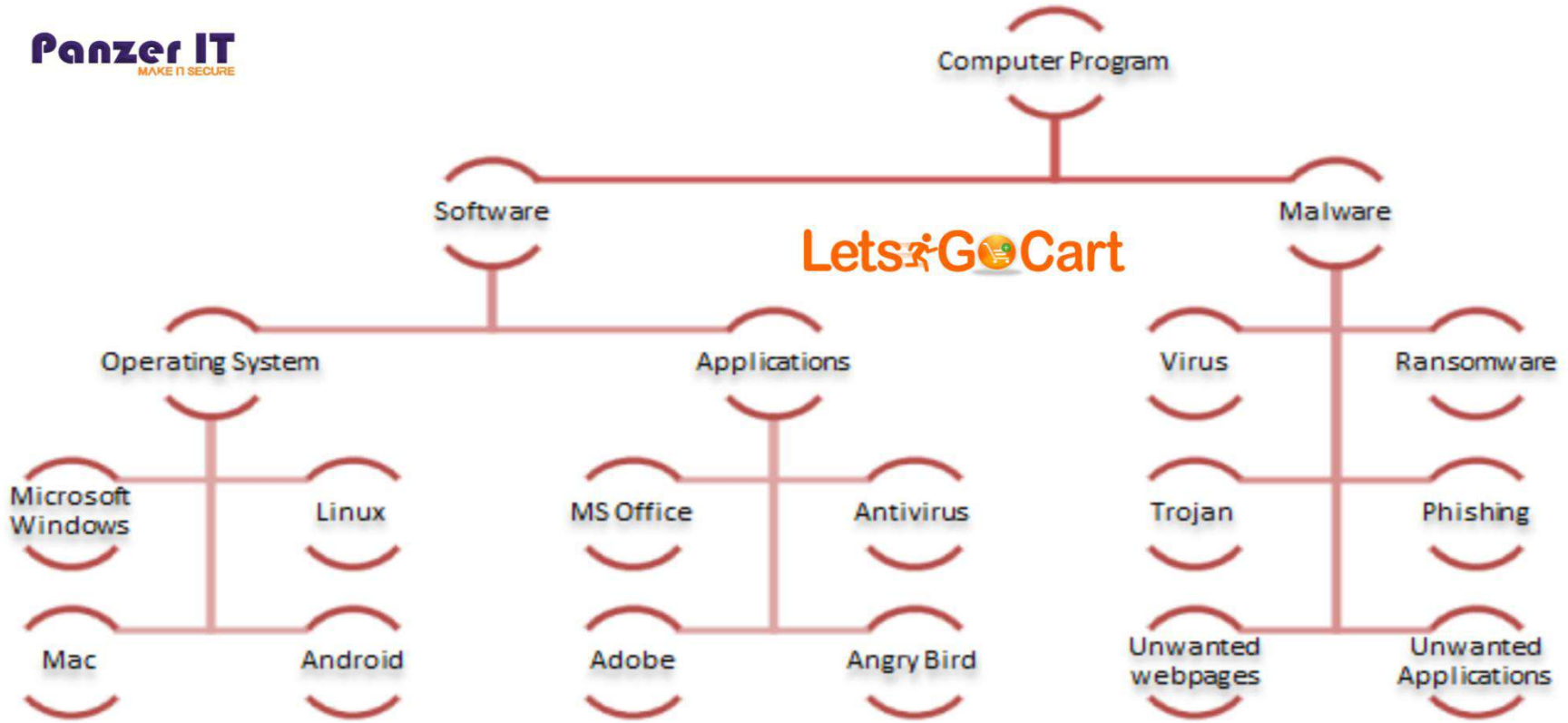
Support & Maintenance

- √ One year database subscription included
- √ Option for instant replacement hardware
- √ Web-based user interface (https)
- √ Quick setup wizard
- √ Configuration backup/restore
- √ Email alert and logging via syslog
- √ Built-in diagnostic function
- √ Full support included in price

Security Profile Scanning

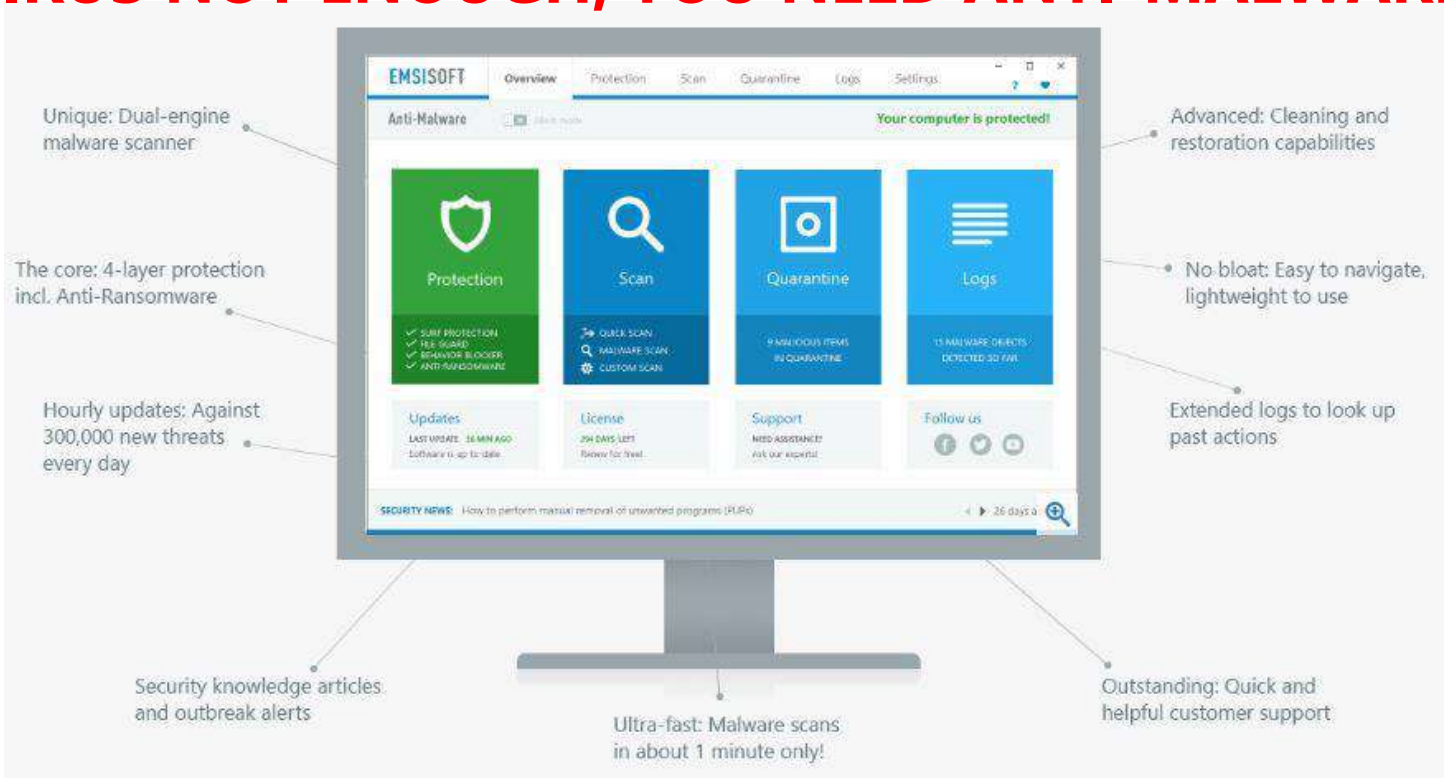
- √ 11 Profiles - Quick Scan - Quick Web Scan - Normal Scan - Full Scan - Firewall Scan - OWASP- Prepare for PCI - HIPAA - Agressive DoS - SCADA

What is Malware



Emsisoft Anti-Malware

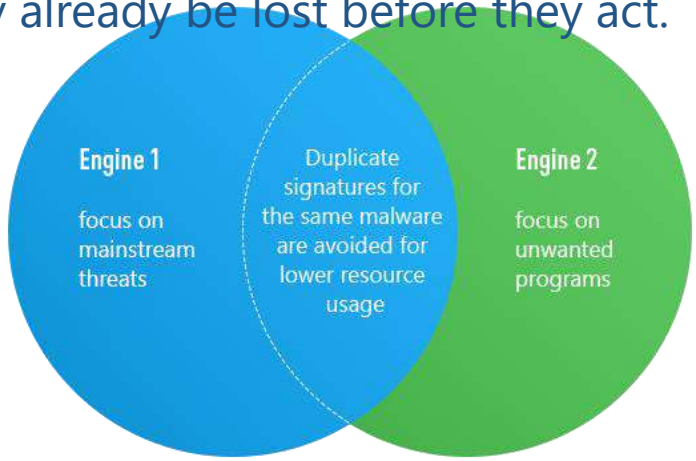
ANTIVIRUS NOT ENOUGH, YOU NEED ANTI-MALWARE



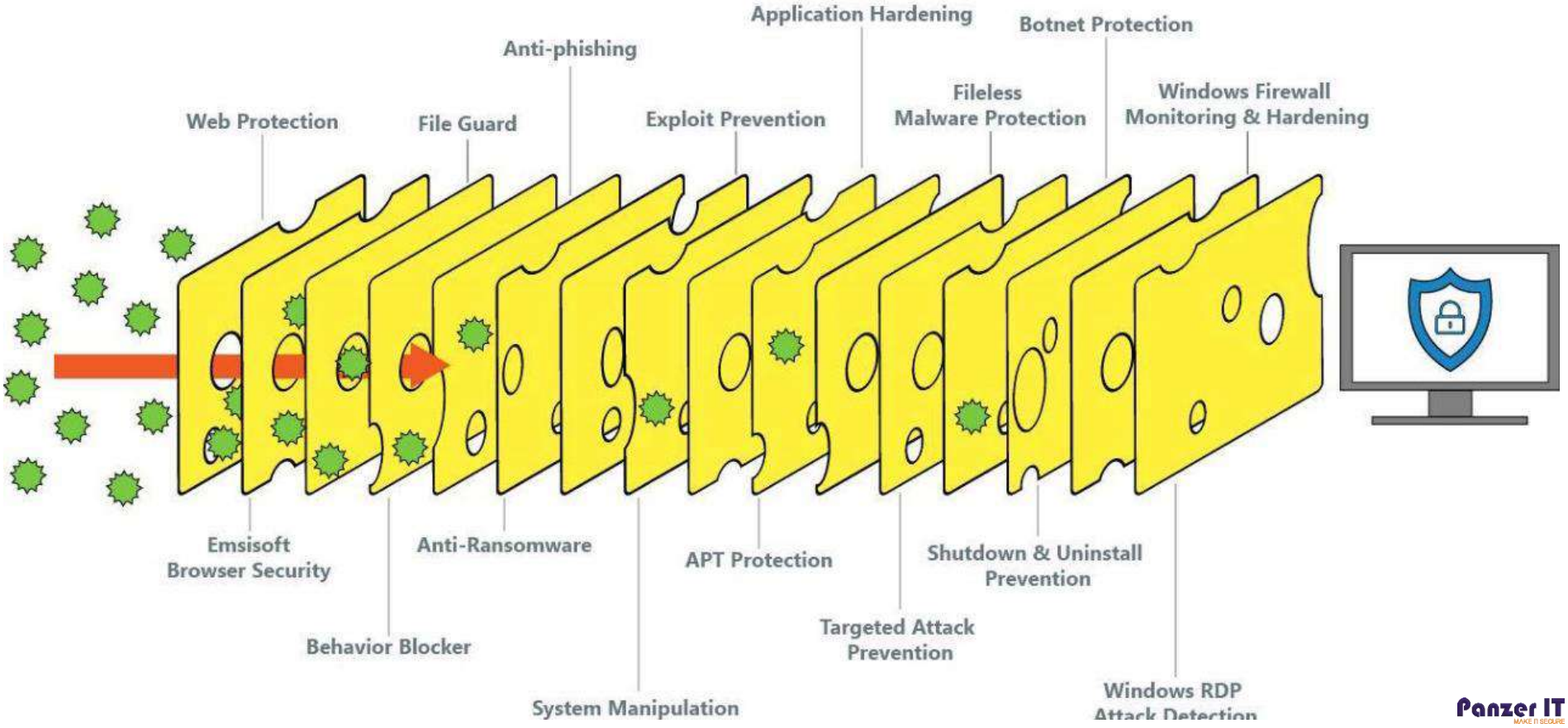
Emsisoft Anti-Malware

Stops Ransomware. Before it encrypts your files.

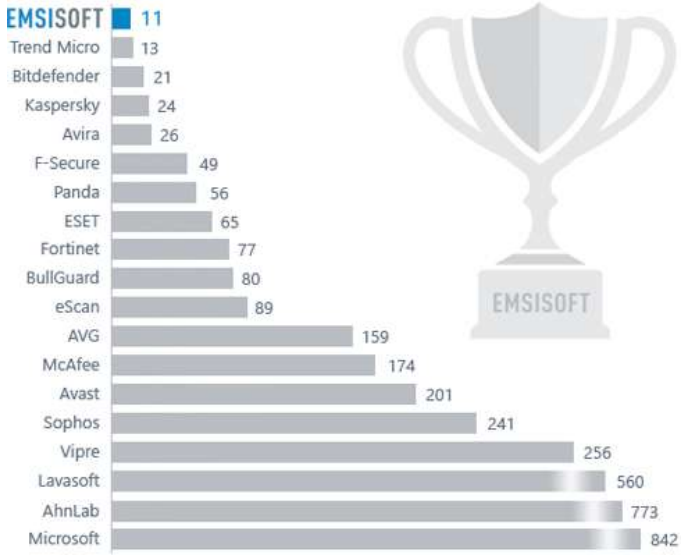
Emsisoft's Anti-Ransomware protection layer is custom-built to detect behavioral patterns of ransomware attacks and stop them before your files can be encrypted. Other anti-ransomware solutions rely on detection of repeated encryption, so your most valuable files may already be lost before they act.

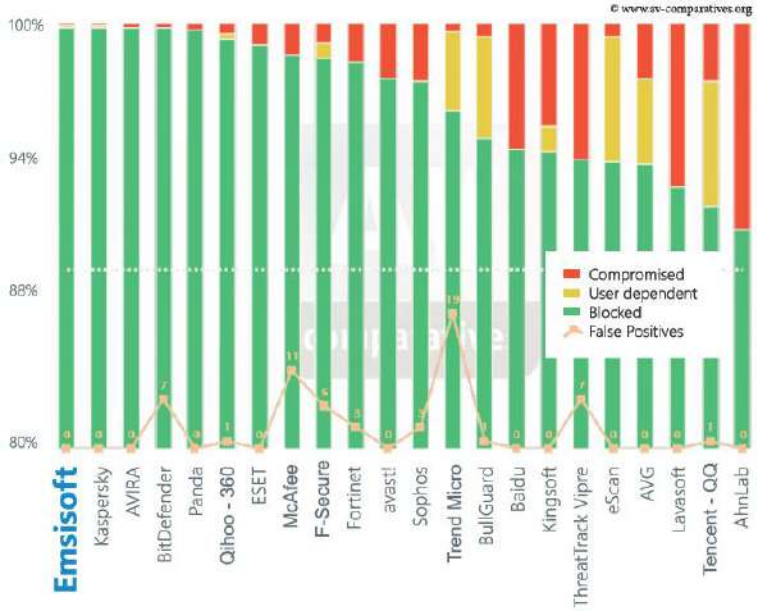


EMSISOFT



Emsisoft Anti-Malware





AWARDS & CERTIFICATIONS

vembu BDR

Comprehensive Backup & Disaster Recovery with Vembu BDR Suite

vmware PARTNER TECHNOLOGY ALLIANCE

Microsoft GOLD CERTIFIED Partner

redhat TECHNOLOGY PARTNER

Few of Vembu customers

100+ countries

4000+ partners

60000+ businesses

24/7 Support

NASA

FUJITSU

Kawasaki

SAMSUNG
FIRE & MARINE INSURANCE

DXC.technology

جامعة الملك سعود
King Saud University

City of Augusta!

EPIC GAMES

LNK
LINCOLN AIRPORT

Apergy

NITCO

ICRISAT
INTERNATIONAL CROPS RESEARCH INSTITUTE FOR THE SEMI-ARID TROPICS

CBK
CITIZENS BANK OF KANSAS

TOLEDO ZOO & AQUARIUM

EXCELLERATE

VMware Backup & Replication - VMware vSphere ESXi host/vCenter Server

Hyper-V Backup - Hyper-V Standalone host, Cluster, CSV & SMB

Windows Image Backup - Windows Servers & Workstations

File & Application Backup - Files/Folders on Windows, Linux, Mac, NAS & MS- Apps

Offsite DR - Replicate a copy of your backup data to Remote/Branch Office

Hybrid Cloud - Replicate a copy of your backup data to Vembu Cloud

Office 365 Backup - Backup Office 365 mails, calendars, contacts & onedrive to On-premise storage or Vembu Cloud Vembu Cloud

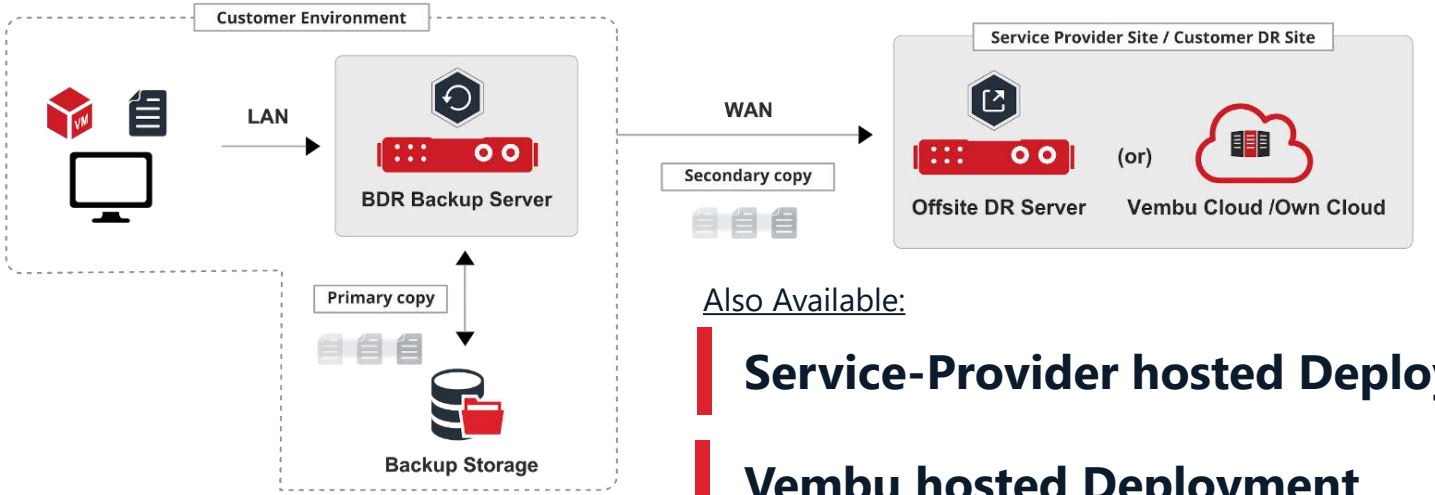
G- Suite Backup - Backup G-suite mails, calendars, contacts & drive to On-premise storage or Vembu Cloud

BDR 360 - Centralized Monitoring Tool

Customer hosted deployment

Backup data is stored in the customer's on-premise storage.
For additional data protection, a secondary copy of backups can be replicated to:

- Customer's Offsite (Remote/Branch office)
- Service Provider's site



Also Available:

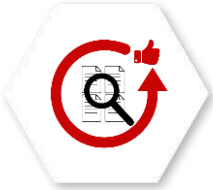
Service-Provider hosted Deployment

Vembu hosted Deployment

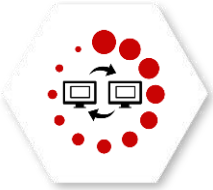
Recovery Time Objectives (RTO)

Vembu offers Industry best RTO which is less than 15 minutes.

Quick VM Recovery



Instant File Recovery



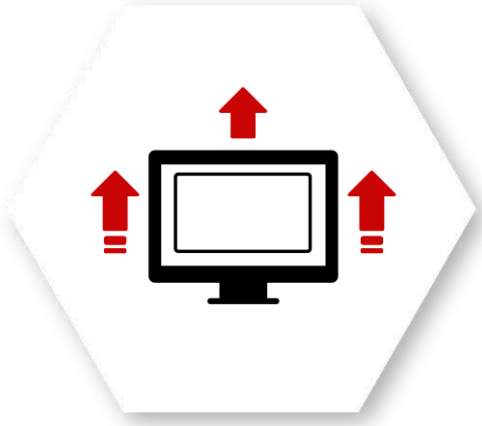
Failover and Failback

Explorer for Microsoft Exchange, SharePoint, SQL and Active Directory

Automatic Backup Verification

Backup data should be recoverable. If not, it is worthless. Vembu provides the ability to run automatic backup verification for all backed up VMs and physical machines

- Backup verification can be automated to run post completion of every backup schedule or once in a day.
- In the process, booting of backed up VM or physical machine will be carried out and screenshot of boot screen will be captured. This screenshot details will be sent to administrators via email.



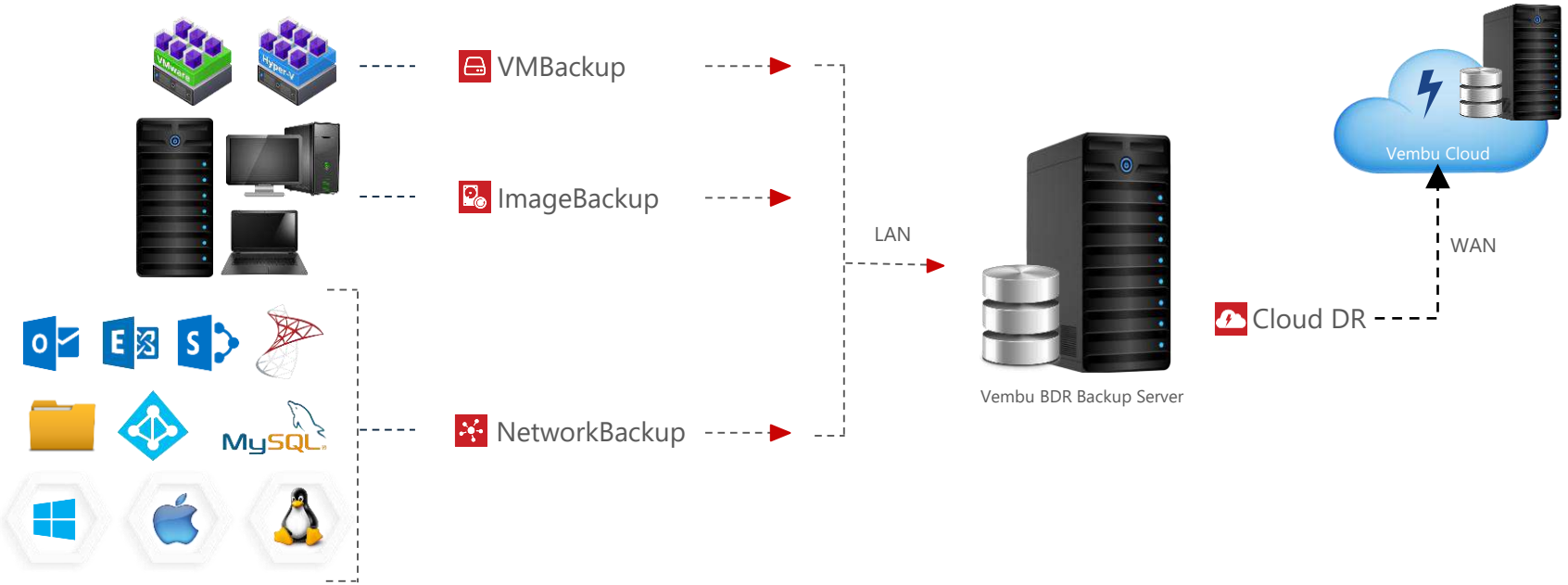
Efficient Storage Management

Vembu BDR Backup Server utilizes VembuHIVE™ file system to effectively manage storage repositories. VembuHIVE™ is an efficient cloud file system designed for large-scale backup and disaster recovery application with support for advanced use-cases. VembuHIVE™ can be defined as a filesystem for filesystem
.

- Supports SAN, NAS and DAS
- Automatically scale up/out the storage devices
- In-built version control and error correction
- In-built Compression & Deduplication
- Encryption

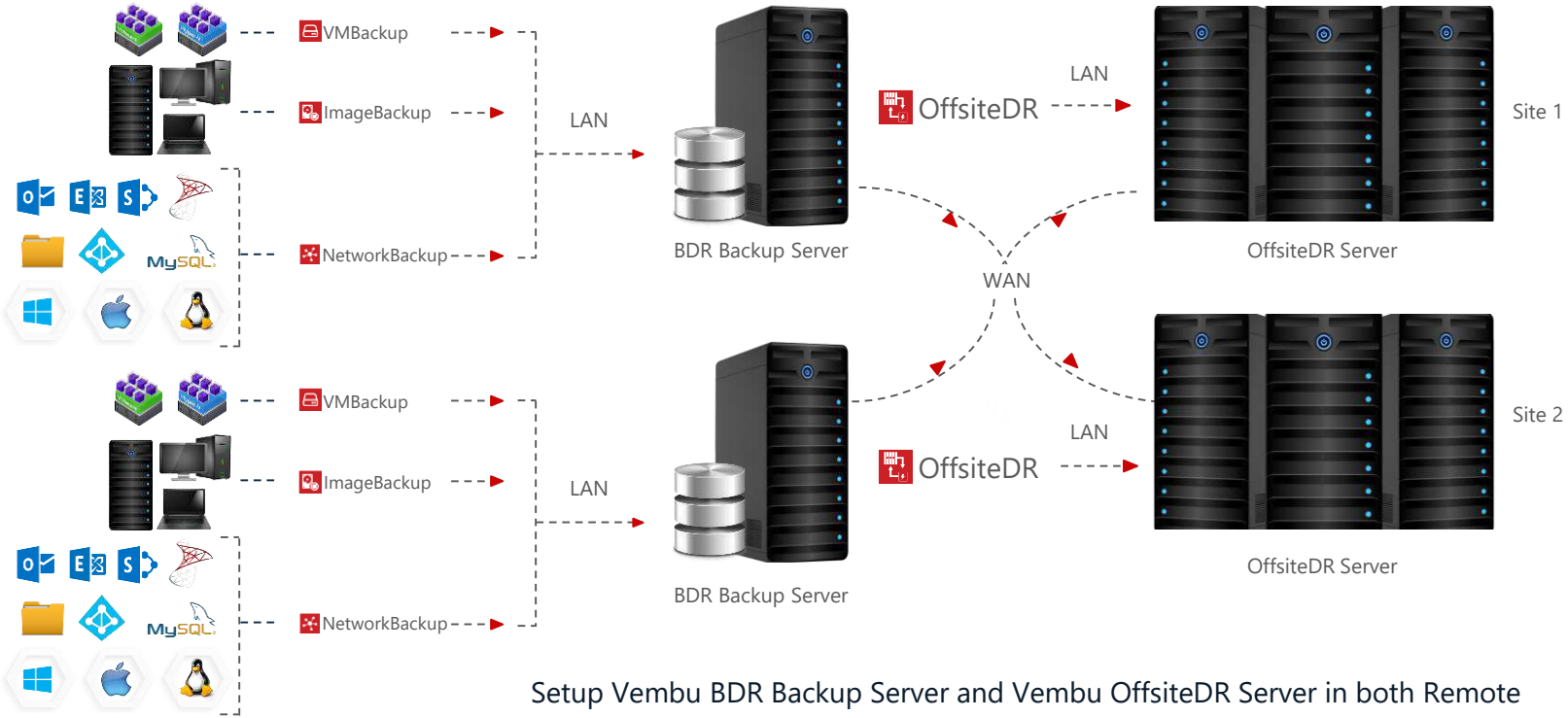
Migration Plan (P2V, V2V & V2P)

Hybrid Deployment - Scenario 1 (CloudDR)



Setup DR site in your local environment and backup via LAN connections and send another copy of backup data to Vembu Cloud via WAN connection by signing up to Vembu CloudDR service

Remote office/Branch office



Setup Vembu BDR Backup Server and Vembu OffsiteDR Server in both Remote office and Branch office and sync backup data between both the locations

Top 10 Reasons to Choose vembu

1. All-in-one Backup Solution
2. One Edition for all Businesses
3. Quick VM Recovery
4. Hybrid Cloud Deployment
5. Scale-Out Storage Repositories
6. Patented In-House File System
7. Cross Platform Recovery
8. Universal Recovery Tool
9. 24/7/365 Free Support
10. Affordable Pricing

Acronis

New Generation Data Protection

www.acronis.com

Toro Rosso Acronis

OFFICIAL PARTNER

twitter.com/acronis

blog.acronis.com

facebook.com/acronis

Acronis: 15+ Years Protecting Digital Lives & Businesses Worldwide

5,000+
petabytes of data under Acronis protection

50,000+
partners

10,000+
cloud partners

500,000+
business customers

5,000,000+
consumer customers

50,000,000+
OEM licenses

Global Headquarters in Singapore

EUROPE 40%

Audi, Deutsche Bank, University of Oxford, orange, AIRBUS, Unilever, axel springer, LEGO, BASF The Chemical Company, TESCO PLC, TOTAL

+200,000 SMBs

AMERICAS 40%

IBM, Pfizer, hp, 3M, GM, WD, Honeywell, MARS chocolate, LOCKHEED MARTIN, HBO

+200,000 SMBs

APJ/MEA 20%

Panasonic, SONY, NEC Empowered by Innovation, brother at your side, PETRONAS, NANYANG TECHNOLOGICAL UNIVERSITY, Singapore POST, NUS, SingTel, SINGAPORE POWER, FOODSTUFFS NORTH ISLAND

+100,000 SMBs

Acronis Hybrid Cloud Architecture

Unified Centralized Data Protection

Web-based User Interface Deployed On-premises or in the Cloud

Any Management

Management software deployed and controlled independently, enabling control of data protection by customer, service provider, vendor, partner, or 3rd party from public/partner/private cloud or customer premises

Any Protection

- Archiving
- Backup
- Cloud Storage
- Disaster Recovery
- e-Discovery
- File Sync and Share
- Monitoring
- Notary

Any Deployment

Any Workload

CLOUD

Microsoft Azure
amazon web services
Office 365

ON-PREMISES

- PHYSICAL
- VIRTUAL
- APPLICATIONS
- MOBILE

Any Storage

CLOUD

Acronis
Microsoft Azure
FTP/SFTP
amazon web services

ON-PREMISES

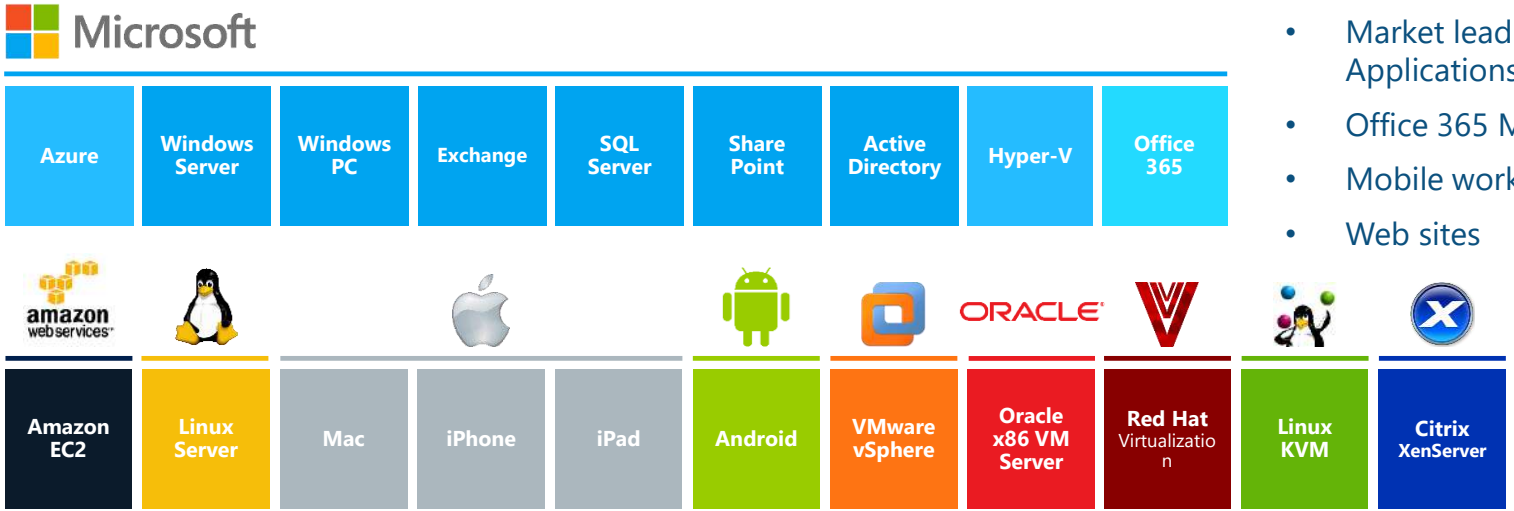
- DISKS
- TAPE
- NAS
- SAN

Any Recovery

- ✓ Data Recovery
  - ✓ File Recovery
  - ✓ Mailbox & E-mail Recovery
  - ✓ Database Recovery
- ✓ System Recovery
  - ✓ Bare-Metal Recovery
  - ✓ Active Restore
  - ✓ Instant Restore™
  - ✓ vmFlashBack
- ✓ Dissimilar Hardware Recovery & Migration
  - ✓ P2V, V2V, V2P, P2P
  - ✓ P2C, V2C, C2C, C2V, C2P
- ✓ Physical Data Shipment
- ✓ Cloud Disaster Recovery
- ✓ Replication
- ✓ High Availability

Acronis Backup Cloud

A powerful, hybrid cloud backup solution for service providers that protects more than 20 platforms and lets them quickly realize incremental revenues with zero upfront costs and a pay-as-you-go business model.



New Generation Data Protection for:

- Market leading Hypervisors
- Market leading Clouds
- Market leading Operating Systems
- Market leading Applications
- Office 365 Mailboxes
- Mobile workforce
- Web sites

Acronis Global

Acronis Cloud DC	Ashburn (VA), United States	Abu Dhabi, UAE	Auckland, New Zealand	Johannesburg, South Africa	
	Phoenix (AZ), United States	Berlin, Germany	Jakarta, Indonesia		
	Querétaro, Mexico	Billund, Denmark	Kanagawa, Japan		
	Sao Paulo, Brazil	Frankfurt, Germany	Kuala Lumpur, Malaysia		
	Toronto, Canada	Gothenburg, Sweden	Mumbai, India		
	Vancouver, Canada	Helsinki, Finland	Nagano, Japan		
		Istanbul, Türkiye	Seoul, Korea		
		Liechtenstein	Singapore		
		Lisbon, Portugal	Sydney, Australia		
		London, United Kingdom	Taipei, Taiwan		
		Lupfig, Switzerland			
		Oslo, Norway			
		Prague, Czech Republic	**Google Cloud Platform**	Montreal, Quebec, Canada	London, United Kingdom
		Rome, Italy		The Dalles (OR), United States	
		Sofia, Bulgaria			
		Strasbourg, France	**Microsoft Azure**	West Des Moines (IA), United States	Amsterdam, Netherlands
		Tel Aviv, Israel			Dublin, Ireland
		Thessaloniki, Greece			Chennai, India
		Valencia, Spain			
		Vienna, Austria			
		Warsaw, Poland			

Secure Remote Access Tool

Netop Remote Connect

- Netop Connect gives you flexible access across platforms, devices and network segments from a single, secure solution.
- Secure Remote Access Connect with confidence to any device, platform, or network.
- Consolidated Connectivity Across Multiple Platforms, One solution. All devices.
- Cross-platform support, including Windows, Linux, Mac and Android
- Centralized management of individual and group roles and permissions
- Secure access into complex networks – BFSI, POS, Production
- Support for embedded operating systems
- Self-hosted or cloud-based Internet connectivity through Connect's secure communication protocol
- Multiple options for multi-factor authentication, including Microsoft Azure
- Simplify maintenance and reduce network vulnerability by consolidating support with a single solution

Benefits Of Using Netop Remote Connect

- Secure remote control, compliant with industry regulations
- Enterprise-class security architecture
- Broad platform support for end users and devices, including mobile devices and production technology
- Scalable and versatile configuration for complex environments
- Web-enabled access for vendors & mobile employees
- Secures tunnelling for access between devices without the need to configure VPNs
- Professional services: expert consultants who can help companies save implementation time, reduce security risk and improve support efficiency
- Greater end-user satisfaction
- Better device uptime

Netop Remote Connect

MAKING CONNECTIONS

- WHO CHOOSES NETOP?

50%

Fortune 100

60%

Financial Times Top 100

23%

World Top 100 Retailers

42%

World Top 50 Banks

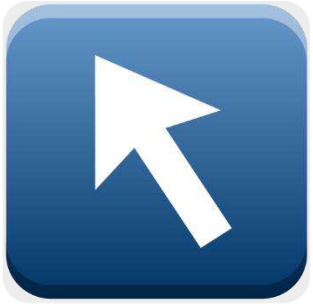
Netop Remote Connect

Netop Remote Connect

- Secure remote access and support

Netop Remote Connect

- Flagship product
- Classic remote support
- LAN/WAN/Internet
- Attended & unattended
- Client/Server based
- Windows, Linux & Mac



Connect On Demand

- Agent-less remote support
- Attended internet-based
- Temporary application
- No footprint
- Windows only

Connect Mobile & Embedded

- Mobile remote support
- Embedded remote support
- Attended & unattended
- Client/Server based
- Windows Mobile & CE
- Symbian, Android, iOS