



**Mission Statement:**

**Continuous Secure Data Accessibility & Availability**

**The Cyber Security Experts**

[www.PanzerIT.com](http://www.PanzerIT.com)

# Type Of Protection

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



- Accessibility
- Availability
- Backup
- DLP
- Risk Management

# Solutions

The Cyber Security Experts

**Panzer IT**  
MAKE IT SECURE

Brands

Description

**ND** 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](#)

**SECP-INT**

[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](#)

**Impero**

[Secure Remote Access, Remote Connect](#)

**Netop**

**LetsGoCart**

[eComm – Software Website](#)

# ND NETAND HIWARE

---

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

# 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

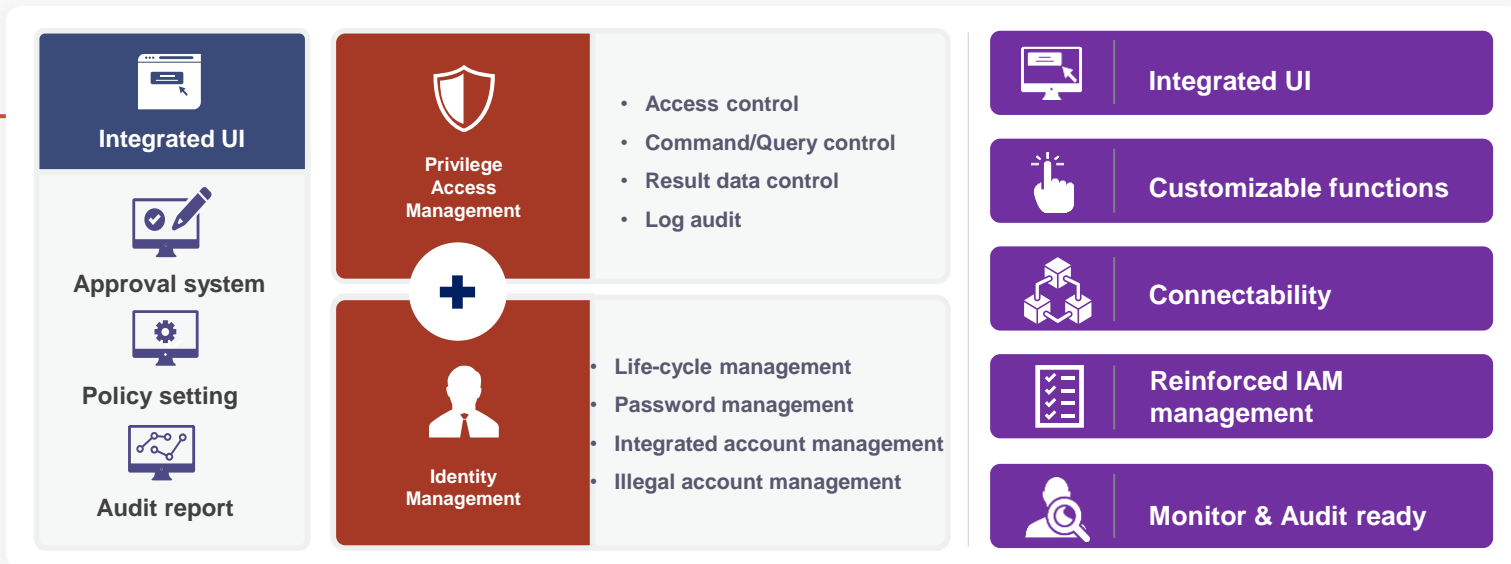
## Benefits of HIWARE

- 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

## Benefits of HIWARE

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

HIWARE Identity management + HIWARE Access management

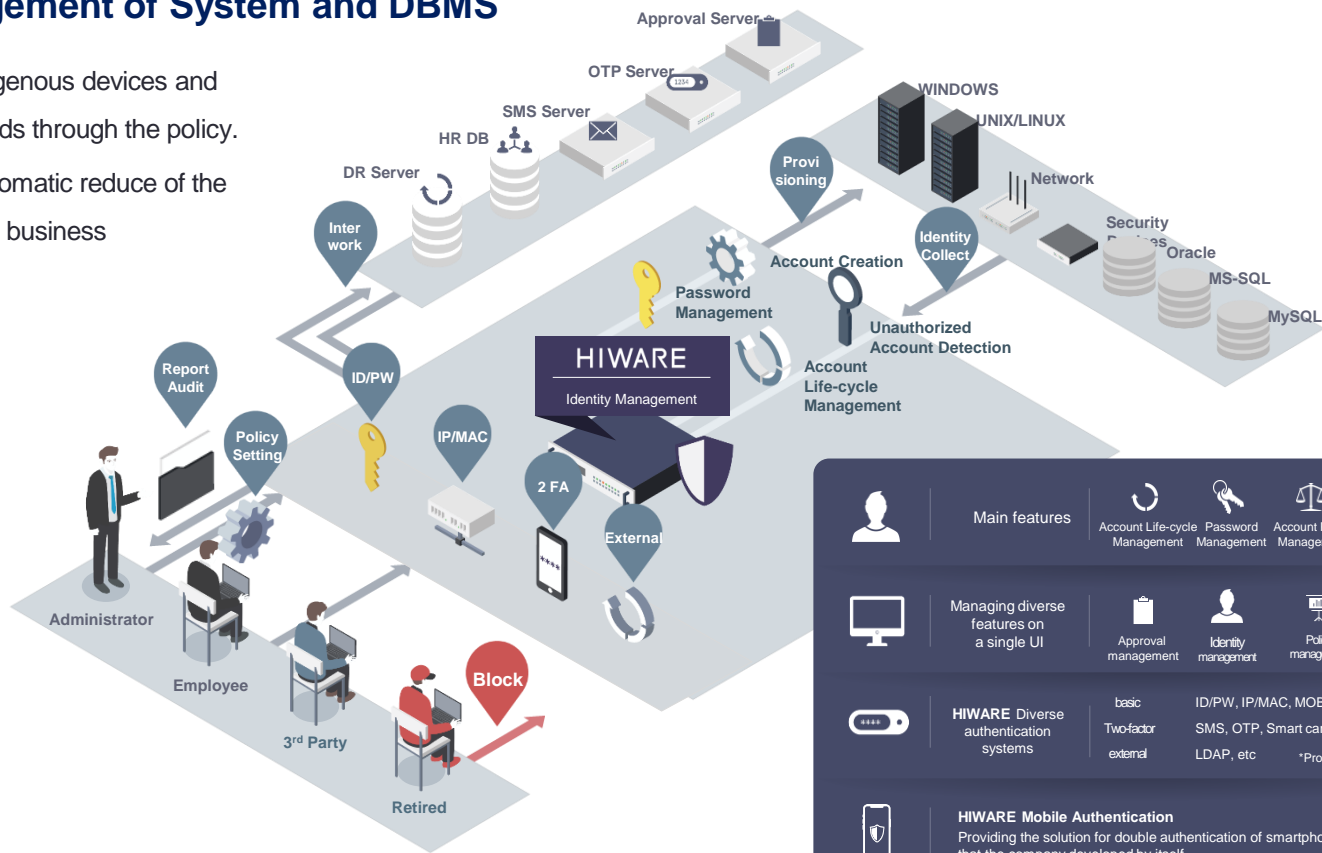


# HIWARE IM for System and DBMS

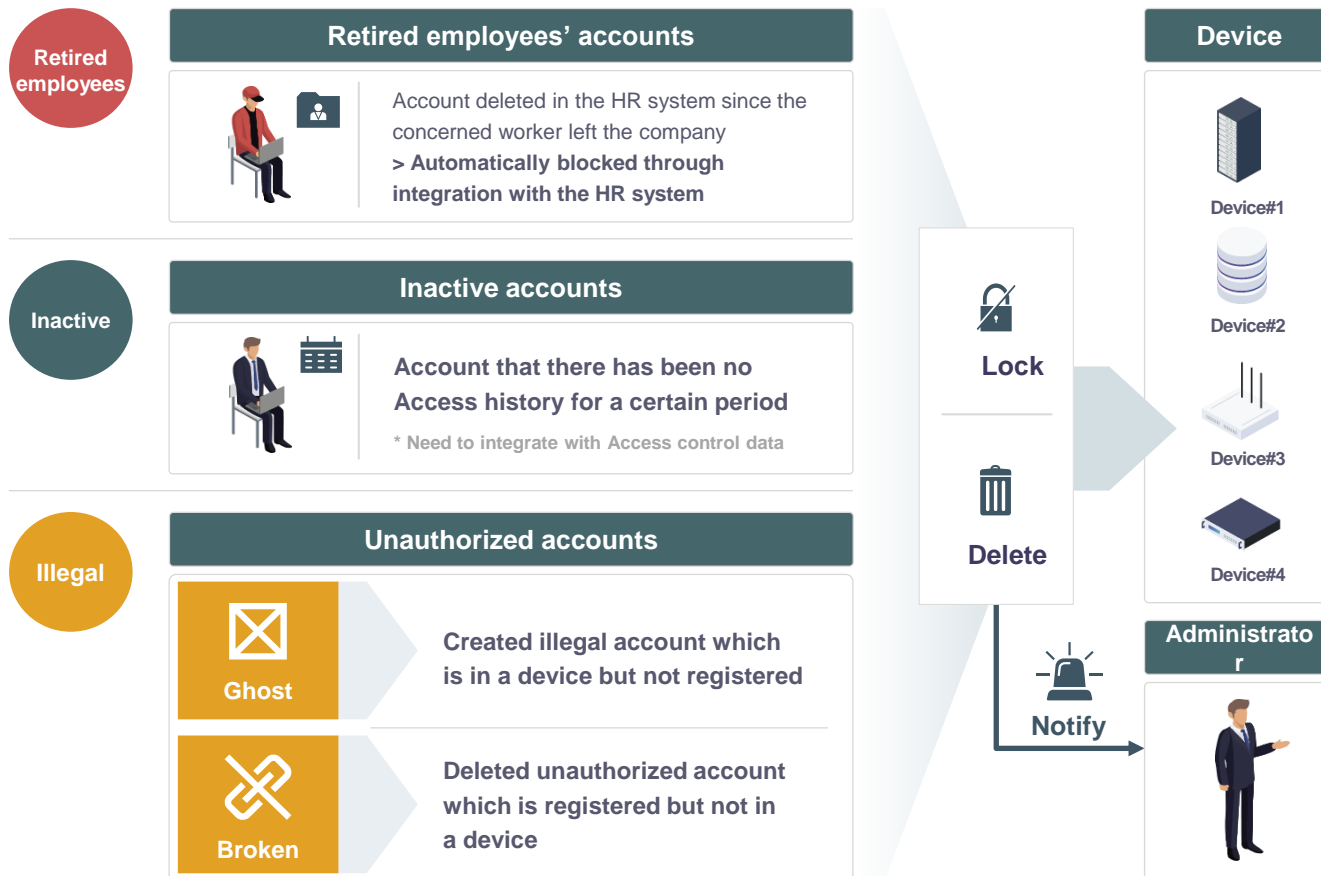
## HIWARE Identity Management of System and DBMS

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.

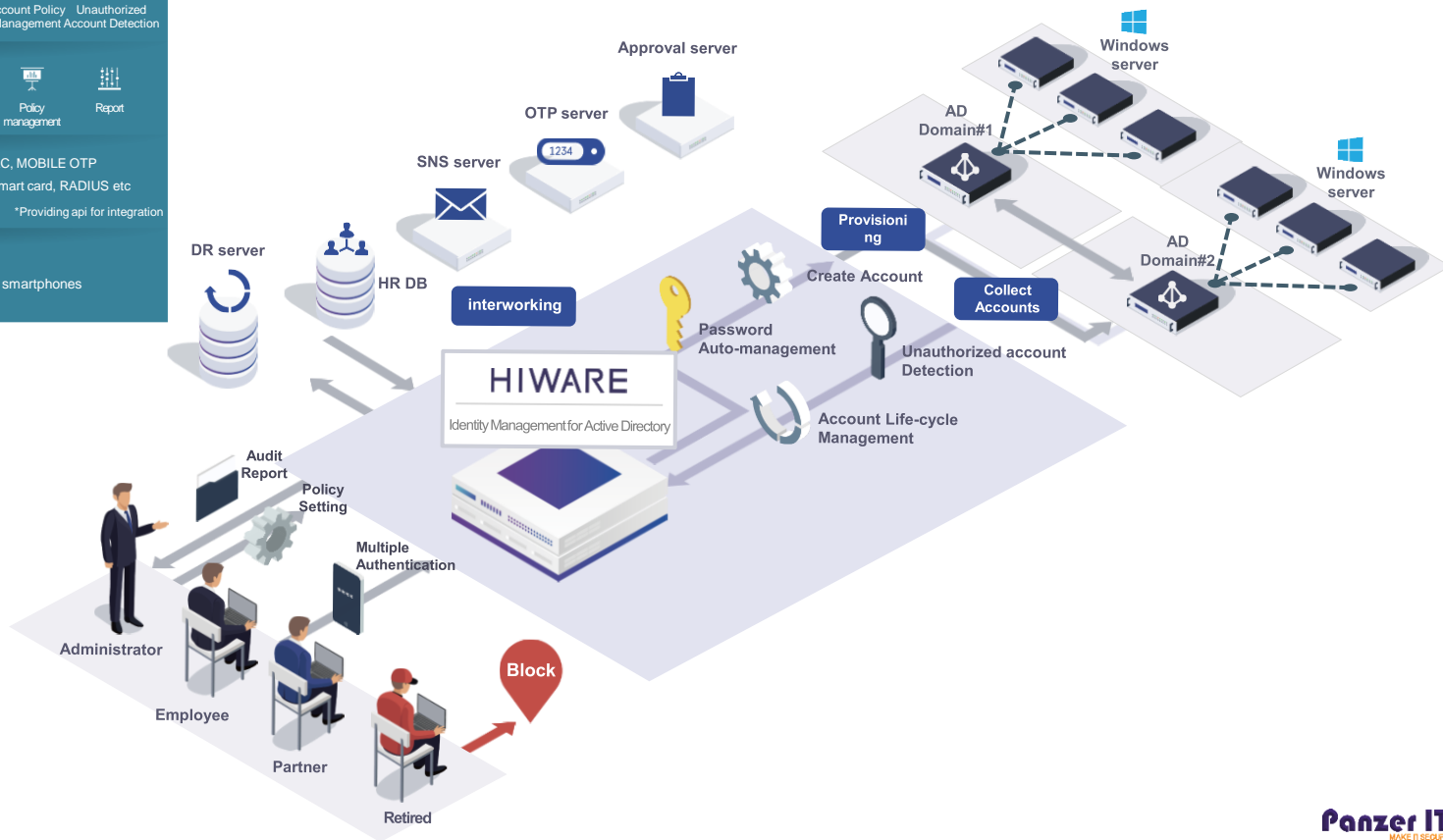


# Unauthorized Account Detection



# HIWARE IM for Active Directory

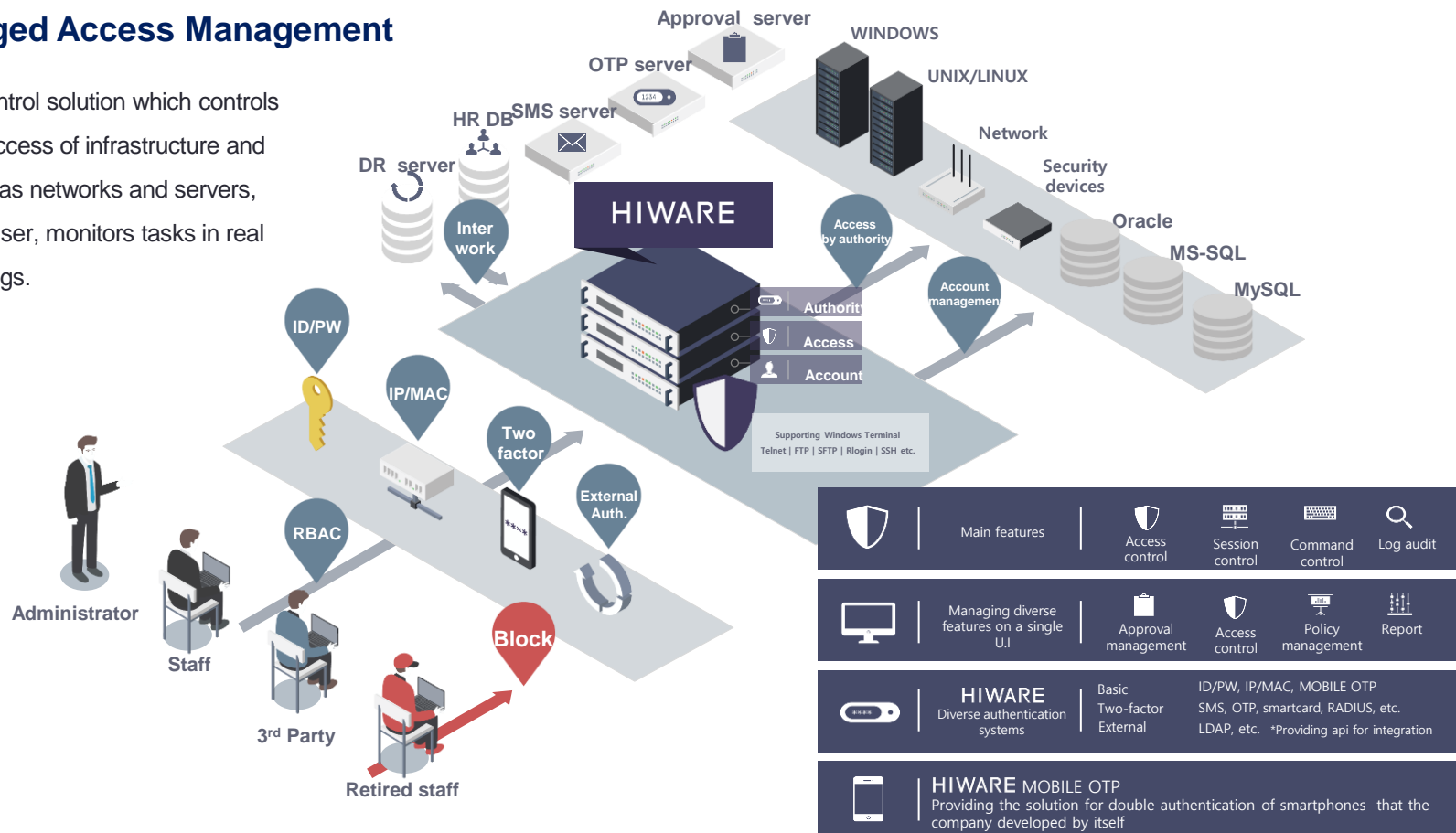
	<b>Main features</b>	Account Life-cycle Management Password Management Account Policy Management Unauthorized Account Detection
	<b>Managing diverse features on a single UI</b>	Approval management Identity management Policy management Report
	<b>HIWARE Diverse authentication systems</b>	basic ID/PW, IP/MAC, MOBILE OTP Two-factor external SMS, OTP, Smart card, RADIUS etc LDAP, etc *Providing api for integration
	<b>HIWARE Mobile Authentication</b>	Providing the solution for double authentication of smartphones that the company developed by itself



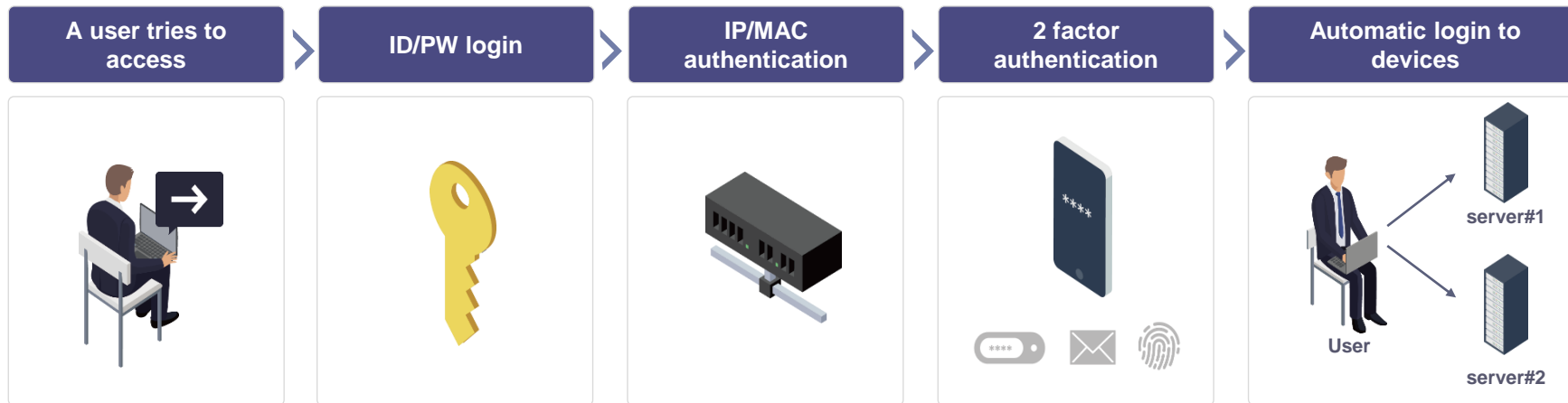
# HIWARE PAM for System and DBMS

## 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.



# Reinforce User Authentication



## 2 Factor Authentication

basic	ID/PW, IP/MAC, MOBILE OTP
Two-factor	SMS, OTP, SSO, Smart card, RADIUS, PKI, biometrics, etc.
external	LDAP, etc. <span style="float: right;">*Providing api for integration</span>

## HIWARE Mobile Authentication v1.0

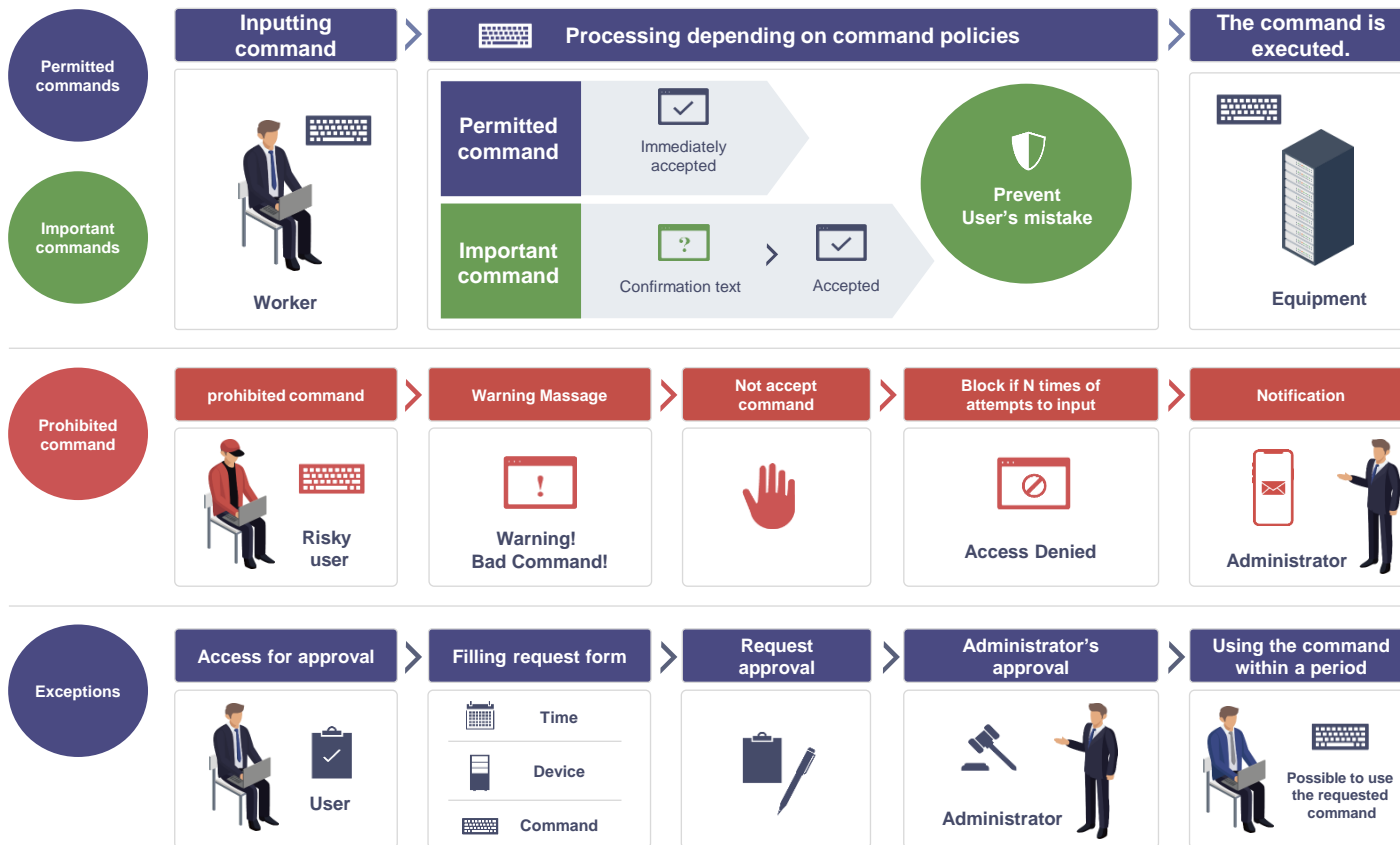


Clients can save the cost to establish a security solution since we provide a mobile OTP product that we developed by ourselves

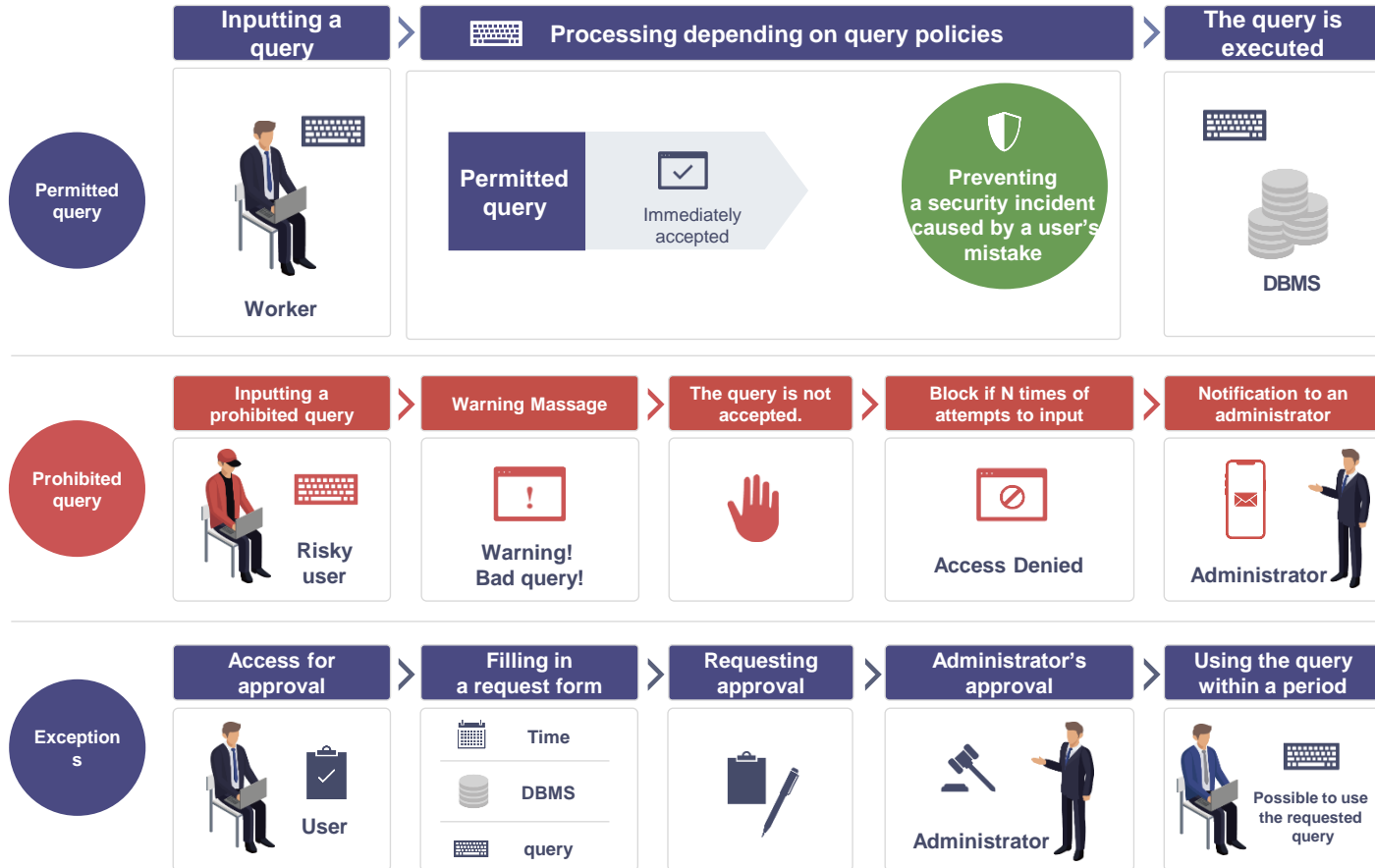
- Support Android/IOS

- Support off-line environment

# System Command Control



# DBMS Query Control



# Real-time Session Monitoring & Control

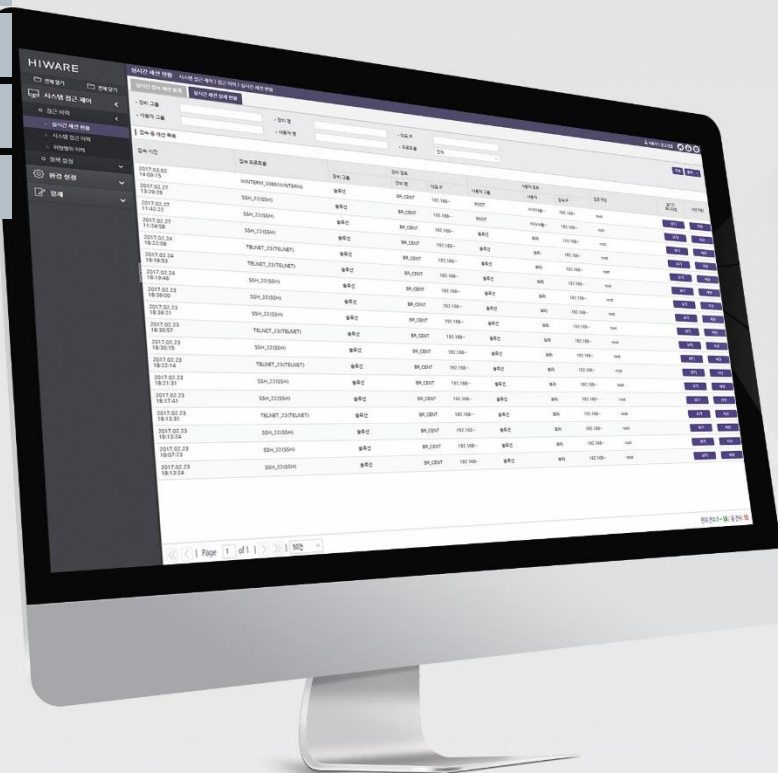
Real-time session monitoring

Event monitoring

Forcibly blocking users' session

Providing real-time dashboard

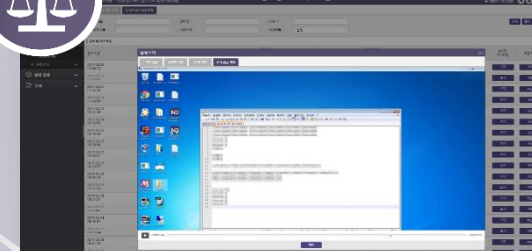
Session timeout



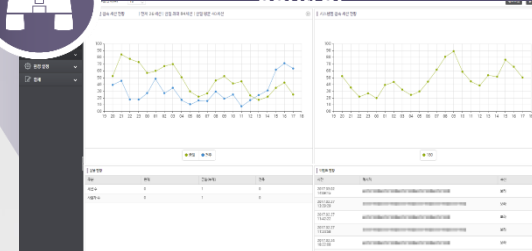
## Real-time session statistics



## Real-time event monitoring & control



## Real-time session monitoring & control



# References

## Global Clients

Philippine SMART Communications	Cambodia ACLEDA Bank	Philippine RCBC Savings Bank	SBJ銀行 Shinhan Bank Japan
---------------------------------	----------------------	------------------------------	--------------------------

## Manufacturing / Businesses


## Finance


## Public

					central administrative agency of Korea	

## Broadcasting/telecommunications

--	--	--	--	--	--

# 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

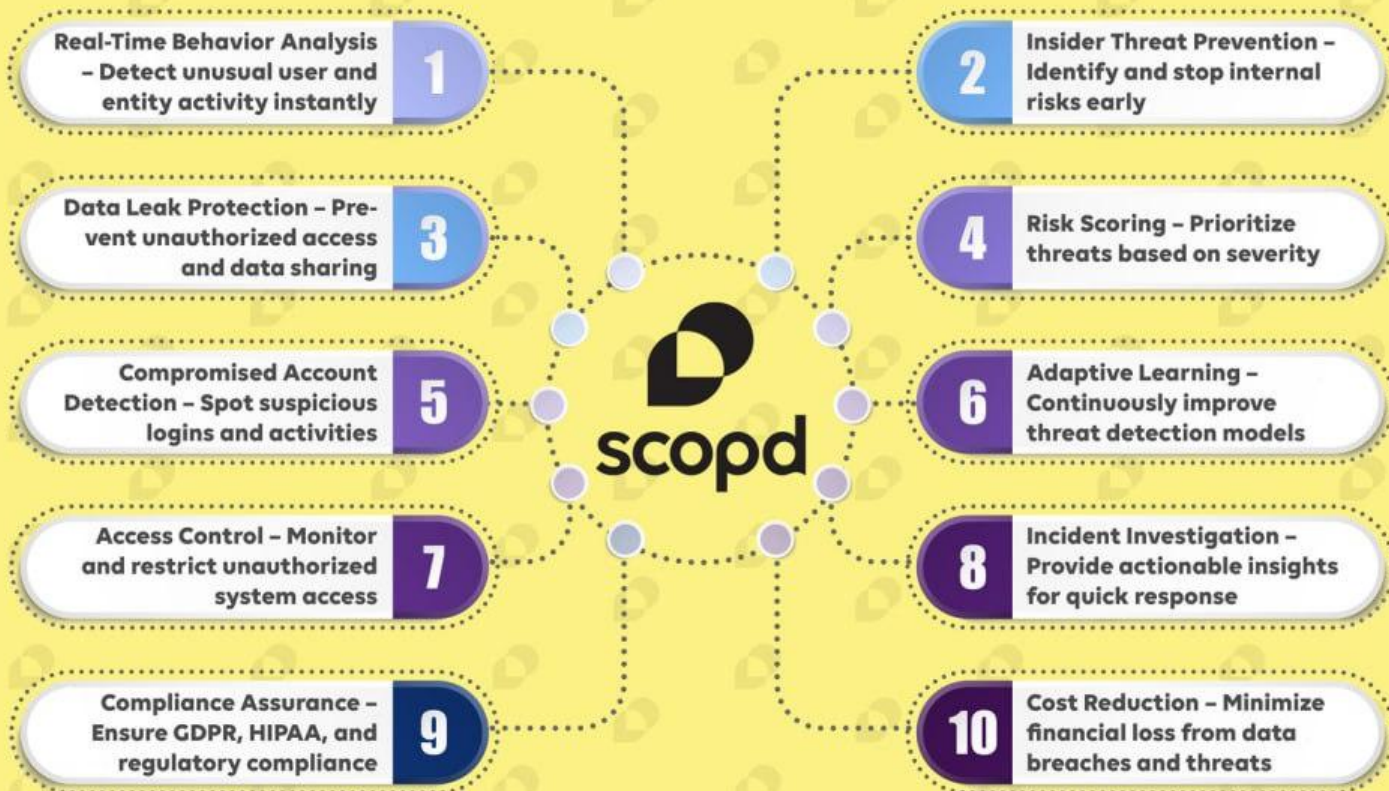
Ensure alignment with data protection regulations like GDPR to avoid penalties.

# Scopd - Why



- **Scopd** is not just an Employee Monitoring solution, its much more than that. Scopd can improve productivity, increase revenue, improve profits and safeguard data.
- Scopd can be used for
  - Insider Threat Management
  - Employee Monitoring
  - User Behavior Analysis
    - Finding Disloyal Employees, Getting to know in advance who wants to leave job
  - Data Leak Prevention
  - 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 employee monitoring and security solution designed to enhance business efficiency & data security through various key features:
- **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.
- **Time Management:** Record working hours, breaks and vacations, and generate time reports, aiding in effective time analysis.
- **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.
- **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.

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

# 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
-  Lock PC in case of unauthorised usage
-  Live Audio, video, screen, mic monitoring
-  Risk Analysis and alerts
-  Compare employees, branches & department working pattern
-  Stop Data Leaks for crucial data based on type, keywords, regex
-  Email, USB drives, web uploads, printouts, messengers
-  Achieve Compliance RBI, SEBI, IRDA, MeitY, GDPR etc
-  Realtime desktop alerts
-  Web-console: access anytime, anywhere, any device
-  Hardware & Software Inventory of all device
-  Domain Integration
-  Productive and non-productive time tracking
-  Login-logout time; timesheet
-  Top performers, Top violators
-  Geolocation tracking to find employee location
-  Central messaging and lock every PC in group or organization
-  Screen recording
-  Insider threat investigation
-  File Audit: create, move, copy, delete
-  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
-  MySQL, PostgreSQL, MS-SQL support

---More--



# 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

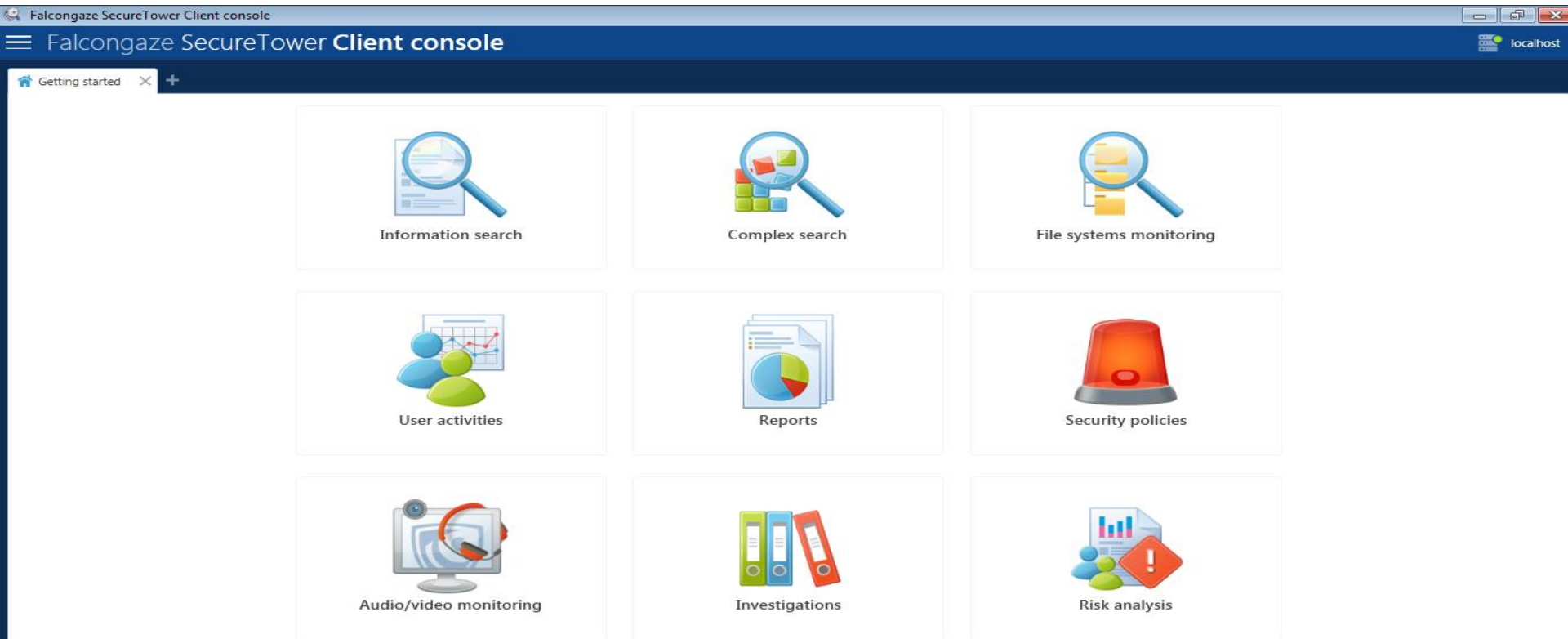
- **Clients:** OneDrive, iCloud, Google Drive, Dropbox, Yandex.Drive
- **Web-access:** all



### Social networks

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

# SecureTower – DLP + UBA





# SecureTower – DLP + UBA

Falcongaze SecureTower Client console

File View Search Tools Help

Connect to server User activity Information search Complex search File systems monitoring Reports Center Security Center Audio/video monitoring Investigation Center

Getting started Reports Center User activity

## User list

All users View mode Refresh

Find user

- Administrator**  
In-built system administrator
- Jarman Robbert**  
HR  
robbert.jarman@gmail.com
- LPT-DELL-PJ Pankaj**  
pankajokk@gmail.com, pankaj@panzerit.com
- LPT-HP Pankaj**
- Mendes Leona**  
Secretary  
leonamendes5@gmail.com
- Miller Ted**  
IT Manager  
ted.miller78@gmail.com
- PIT-APP-SRV.PANZERIT.LOCAL A...**

## User activity report Mendes Leona

Today Past 2 days Past 7 days Past 30 days Date range Refresh Save

Date	Mails	Messengers	Files	Web	Other activities
9:00					
10:00					
11:00				➔ 1 url	3 screenshots 39 minutes activity 178 keys pressed
12:00				➔ 2 urls	3 screenshots 25 minutes activity 95 keys pressed
13:00				➔ 2 urls ➔ 2 search queries	2 screenshots 17 minutes activity 13 keys pressed
14:00					3 screenshots 24 minutes activity 139 keys pressed
15:00				➔ 11 urls	3 screenshots 43 minutes activity 3 minutes activity 211 keys pressed
16:00			2 files		3 screenshots 26 minutes activity 311 keys pressed
17:00	1 mail Received: 1		1 file 2 files		1 minute activity 1 minute activity 4 copies to clipboard 48 keys pressed
18:00				➔ 3 urls	2 screenshots 24 minutes activity 5 minutes activity 1 key pressed
19:00	2 mails Sent: 2		1 file	➔ 2 search queries	2 screenshots 0 minutes activity

Daily activity Activity statistics User relations

Panzer IT

# SecureTower – DLP + UBA

Falcongaze SecureTower Client console

File View Search Tools Help

Connect to server User activity Information search Complex search File systems monitoring Reports Center Security Center Audio/video monitoring Investigation Center

Getting started Reports Center

Generate report Add Modify Delete Save Print

Name

- Reports
  - My reports
  - Predefined reports
    - Consolidated reports
      - Consolidated report
    - Personal reports
      - Personal report
    - Security Center reports
      - Security center report
  - TOP-reports
    - Clipboard
      - Clipboard copy counter
    - Desktop activity
      - Activity time**
      - Average activity time
      - Average end time
      - Average idle time
      - Average start time
      - Average working time
      - Idle time
      - Working time
    - Files from devices
      - USB file counter
      - USB file size

**Activity time**

All users [Modify](#)

Report type: Total / Activity time [Modify](#)

Reporting period: All time [Modify](#)

User	Activity Time
PIT-APP-SRV.PANZERIT.LOCAL Administrator	53:03:49
LPT-DELL-PJ Pankaj	46:53:18
Wilson Katharyn	18:03:36
Mendes Leona	15:30:16
Jarman Robbert	15:30:16
White Helen	12:24:48
Miller Ted	10:06:04
LPT-HP Pankaj	06:15:30
PIT-VM-PC1 VM	00:33:43

Panzer IT



**SOMANSA**

# Somansa: Privacy-i Endpoint DLP

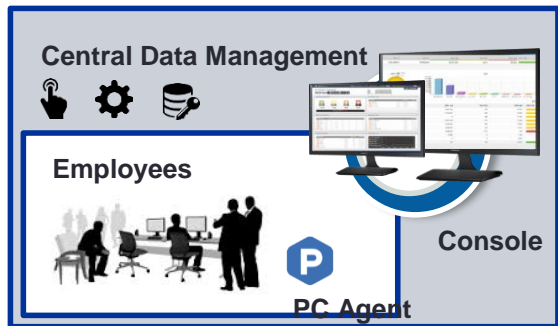
## Privacy-i and Data Security Process

### ❖ 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

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



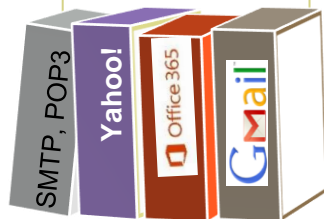
### Mail-i protects sensitive data in motion

- 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



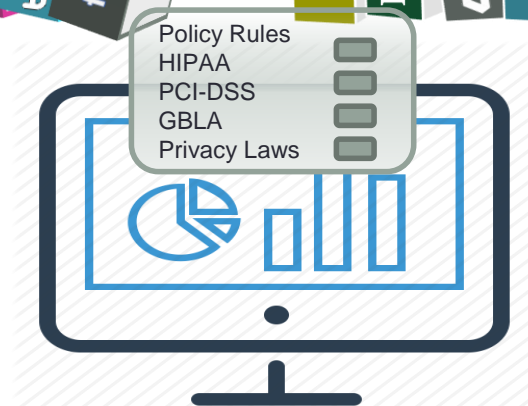
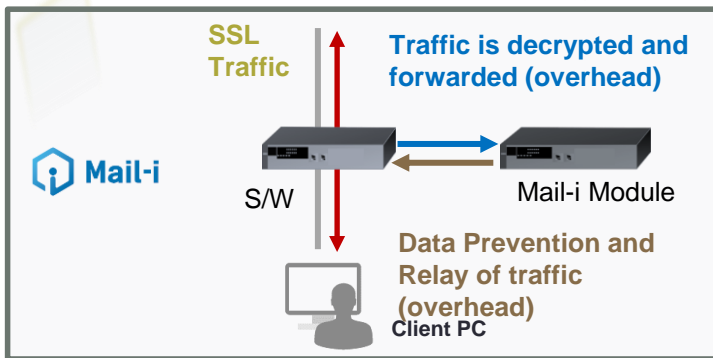
#### Social Media

- 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



SOMANSA

**Multiple products, One view**

All products can be managed by one central console

Central Management

Request approval

Set Policy/  
Apply

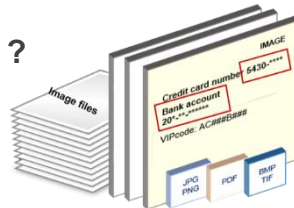
Block/Allow logs and copied files

**Fast Search & Report Big Data**

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

**What if there's sensitive data in the image ?**

Sensitive data in image file can be detected as OCR feature (Optical Character Recognition)



# Structure of SOMANSA's DLP

## Integrated Policies

## Integrated Management Control

DASHBOARD	REPORTS	INCIDENTS	POLICIES	MANA
Top Users				
Filter ▾				
Total 9,113				
Encrypt				

Detect

Discover

Endpoint

Network

Patterns	
+ Add New	
Order	Pattern Name
0	ALL: Confidential Data
0	ALL: Corporate Financial Information
0	ALL: Credit Card Number
0	ALL: Customer Code
0	ALL: Customer Data
0	ALL: E-Mail
0	ALL: Employee Code
0	ALL: Employee Data
0	ALL: IP Address
0	ALL: Merger and Acquisition Agreements
0	ALL: Sales Information
0	BR: Cadastro de Pessoa Física
0	BR: Cadastro Nacional Pessoa Jurídica
0	MX: Clave de Elector



### Channels

Online/Offline ☒ Online ☒ Offline

Details

Copy Prevent+	<input checked="" type="radio"/> Pass <input type="radio"/> Control
Upload Prevent+	<input checked="" type="radio"/> Pass <input type="radio"/> Control
Print Prevent+	<input checked="" type="radio"/> Pass <input type="radio"/> Control
Clipboard Prevent+	<input checked="" type="radio"/> Pass <input type="radio"/> Control
Shared Folder Prevent+	<input checked="" type="radio"/> Pass <input type="radio"/> Control
Application Control	<input checked="" type="radio"/> Pass <input type="radio"/> Control
Media Control	<input checked="" type="radio"/> Pass <input type="radio"/> Control
PC Security	<input checked="" type="radio"/> Pass <input type="radio"/> Control



### Net App to Control

Agent: default(12.0.250.181)

Policy Type: ☐ Control ☒ Prevent ☐ Approval Detection Rule:  Select

Net App Settings

Electronic Mail (0/2)	<input type="checkbox"/> Body/File Content	Recipient E-mail: <input type="text"/>	Sender E-mail: <input type="text"/>
Web Mail (0/12)	<input type="checkbox"/> Body/File Content	Recipient E-mail: <input type="text"/>	Sender E-mail: <input type="text"/>
Instant Messaging (0/6)	<input type="checkbox"/> Chat <input type="checkbox"/> File Transfer		
Remote Access (0/1)	<input type="checkbox"/> Body Content		
Networking (0/2)	<input type="checkbox"/> Body/File Content	Include URL: <input type="text"/>	Exclude URL: <input type="text"/>
Social Network Service (0/13)	<input type="checkbox"/> Body Content <input type="checkbox"/> Body/File Content		
File Storage and Sharing (0/8)	<input type="checkbox"/> File Transfer <input type="checkbox"/> Body/File Content		
Personal File Sharing (0/1)	<input type="checkbox"/> File Transfer		

# SOMANSA | Who we are ?



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



Gartner

Magic Quadrant  
Enterprise DLP



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 ★★★★★<sub>1/5</sub>

4.5/5.0 Rating



# SecPoint<sup>®</sup> Penetrator<sup>™</sup>

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

# SecPoint<sup>®</sup> Cloud Penetrator<sup>™</sup>

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



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 &amp; WiFi Pen Testing

## List of Vulnerability Scans

Search

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

# Features and Benefits

No Data Collection, Backdoor Free

11 Scan Profiles, HIPAA, OWASP top 10, Prepare for

PCI, Firewall Scan, SCADA & more

Launch Real Exploits

Advanced Audit Options

Schedule scans daily, weekly, monthly

Prevent Hackers To Access Your Server

Vulnerability Scanning

Vulnerability Assessment

60.000 + Vulnerabilities

Distributed Scanning Capability

Advanced Web Crawler - SQL Injection - XSS - SSL

Audits any OS

Scan any OS and Network devices

Reports Branding

Detailed Remedies for Identified Vulnerabilities

Secure Design All Data Stored on Unit

Option for syslog remote logging

Vulnerability Audit

Launch DoS & DDoS attacks

OS Independent Interface

Bugtraq ID / Mitre CVE / Ubuntu USN / Microsoft / OSBDB

Automatic Web Crawl Script Engine

Multi User Support

Launch Real Exploits

Ticket System for full Vulnerability Management

Option for centralized update point

Distributed Auditing

XML, PDF and HTML Reports

Finds SQL Injection

### 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, Umbraco, 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 - QuickWeb Scan - Normal Scan - Full Scan - Firewall Scan - OWASP- Prepare for PCI - HIPAA - Aggressive DoS - SCADA

EMSIISOFT

# What is Malware

**Panzer IT**  
MAKE IT SECURE

Computer Program

Software

Malware

LetsGoCart

Operating System

Applications

Virus

Ransomware

Microsoft  
Windows

Linux

MS Office

Antivirus

Trojan

Phishing

Mac

Android

Adobe

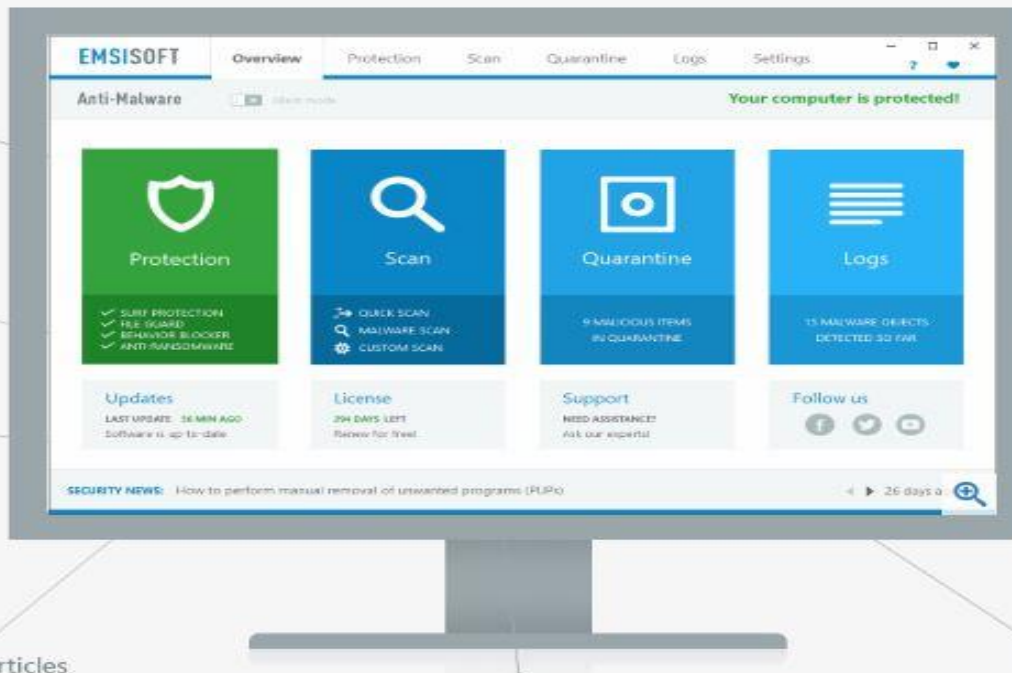
Angry Bird

Unwanted  
webpages

Unwanted  
Applications

# Emsisoft Anti-Malware

## ANTIVIRUS NOT ENOUGH, YOU NEED ANTI-MALWARE



Unique: Dual-engine malware scanner

The core: 4-layer protection incl. Anti-Ransomware

Hourly updates: Against 300,000 new threats every day

Advanced: Cleaning and restoration capabilities

No bloat: Easy to navigate, lightweight to use

Extended logs to look up past actions

Security knowledge articles and outbreak alerts

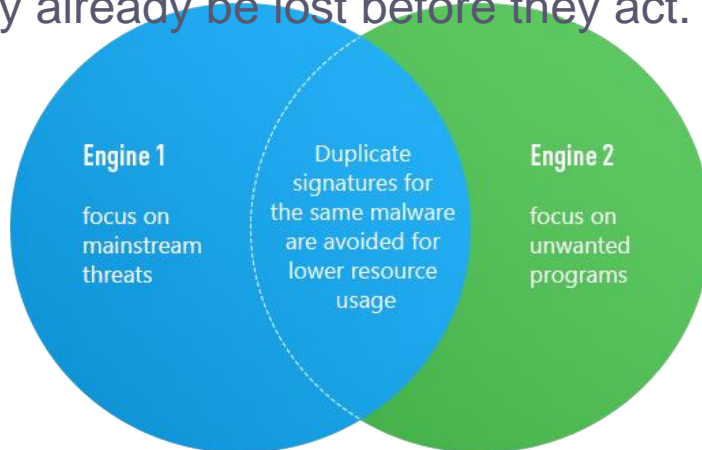
Ultra-fast: Malware scans in about 1 minute only!

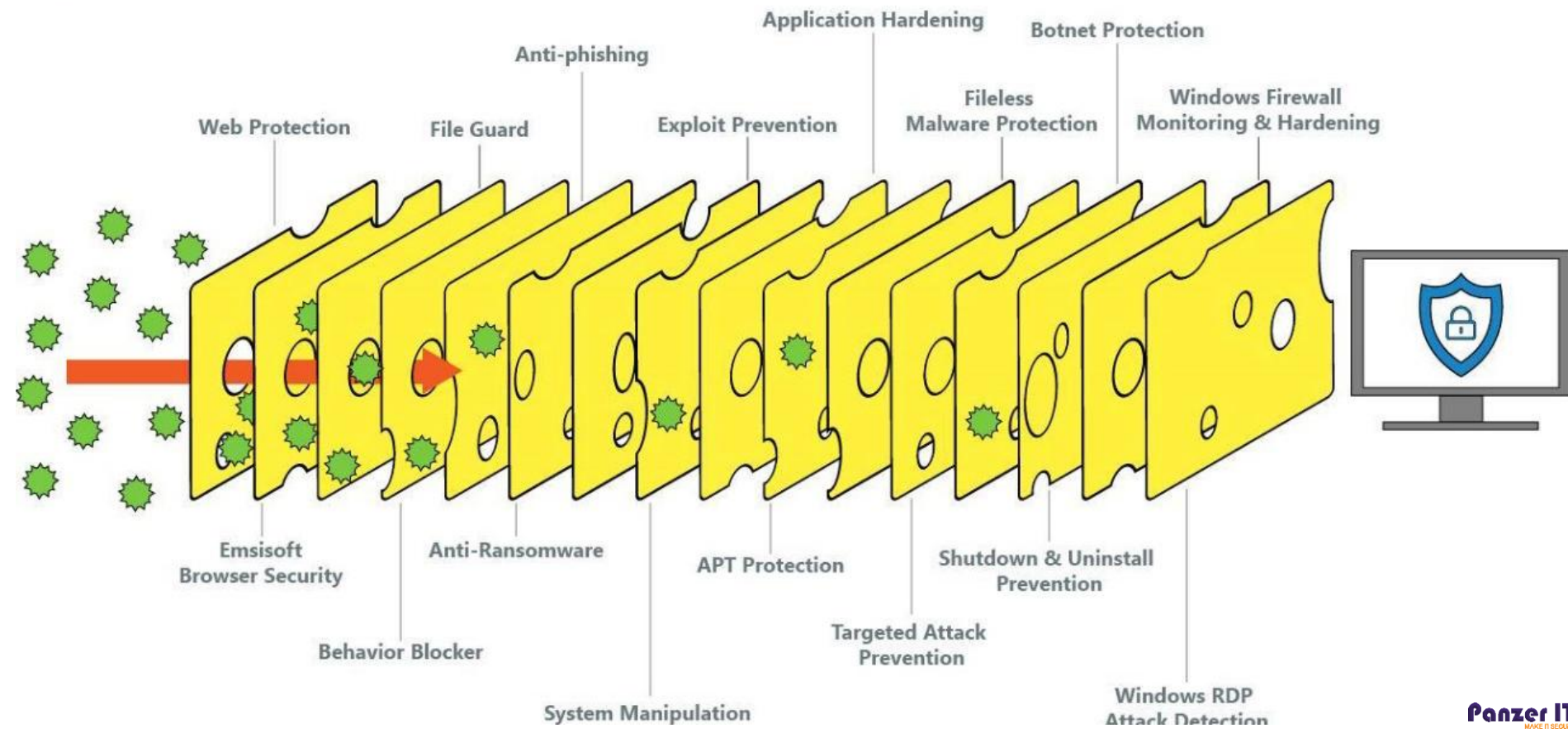
Outstanding: Quick and helpful customer support

# Emsisoft Anti-Malware

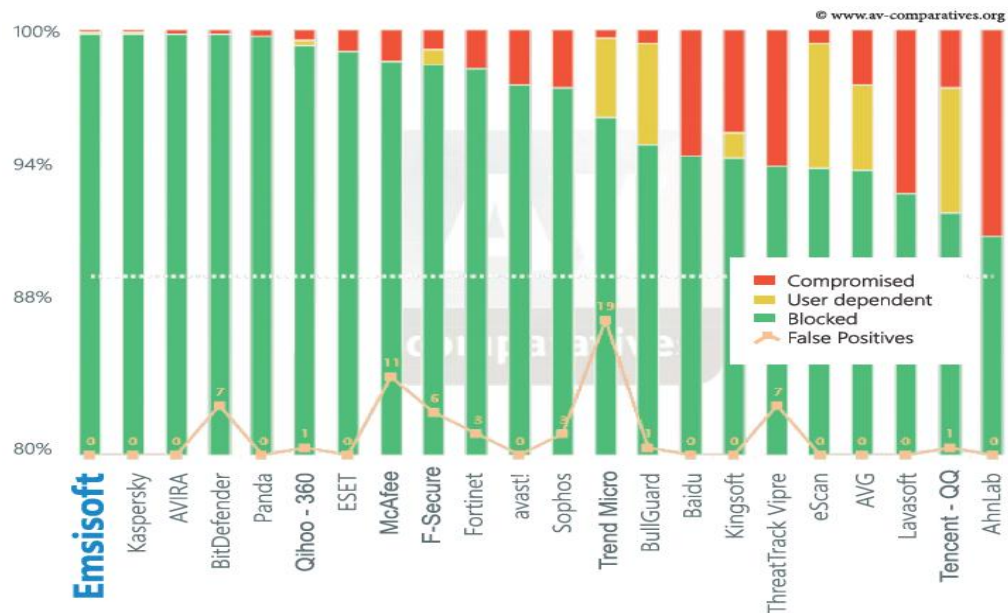
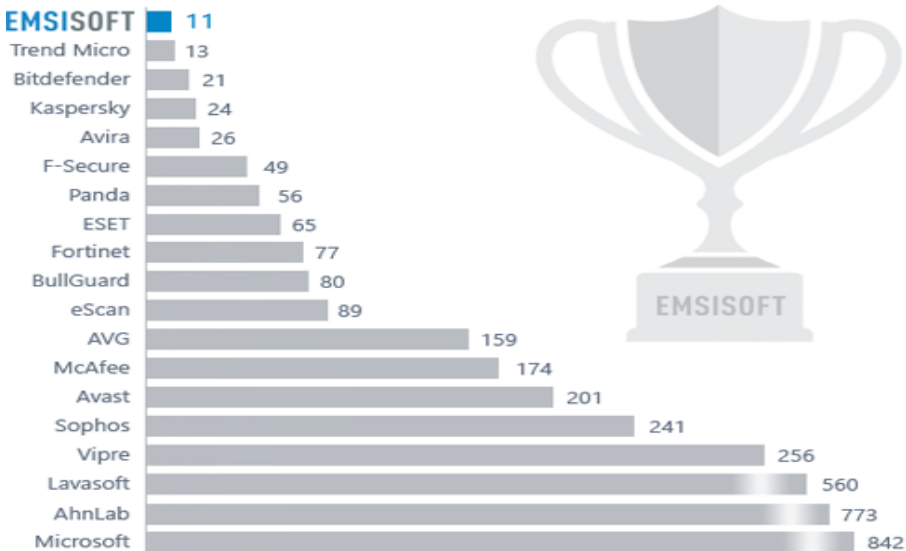
Stops Ransomware. Before it encrypts your files.

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 Anti-Malware



## AWARDS & CERTIFICATIONS





# Comprehensive Backup & Disaster Recovery with Vembu BDR Suite



# Few of Vembu customers



100+ countries



4000+ partners



60000+ businesses



24/7 Support





**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 Vembu Cloud



**G- Suite Backup** - Backup G-suite mails, calendars, contacts & drive to Vembu Cloud



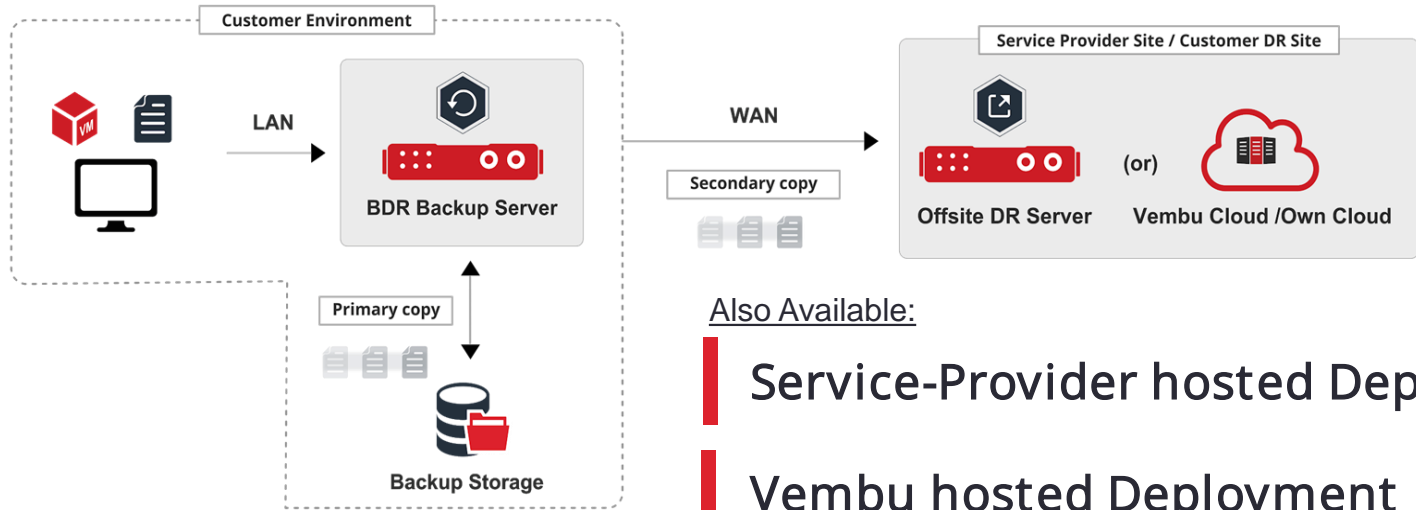
**BDR 360** - Centralized Monitoring Tool

# 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



## Recovery Time Objectives (RTO)

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



Quick VM Recovery



Instant File Recovery



Failover and Failback

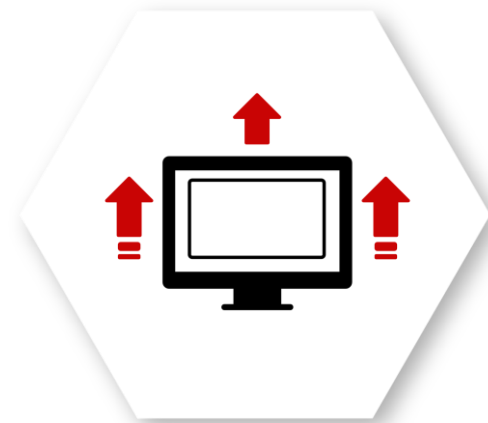


Explorer for Microsoft Exchange,  
SharePoint, SQL and Active Directory

## 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

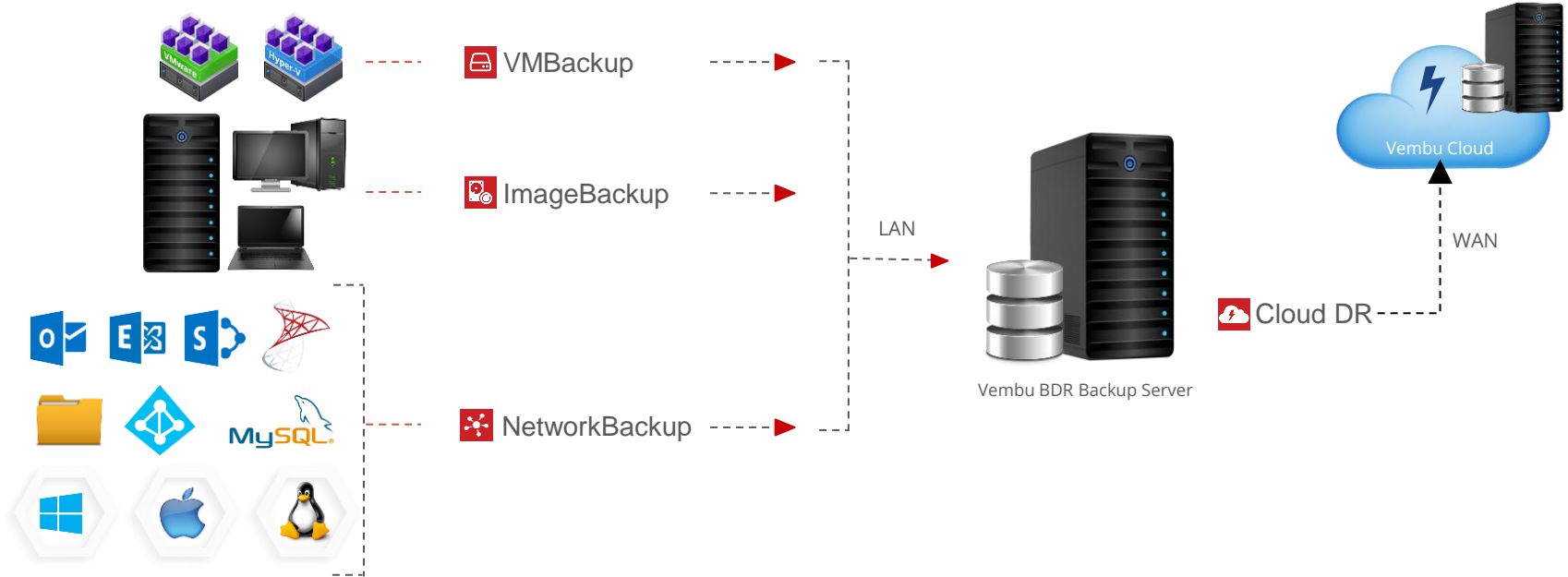
Vembu BDR Backup Server utilizes VembuHIVE™ file system to effectively manage storage repositories. VembuHIVE™ is an efficient cloud file system designed for large-scale backup and disaster recovery application with support for advanced use-cases. VembuHIVE™ can be defined as a filesystem for filesystem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

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



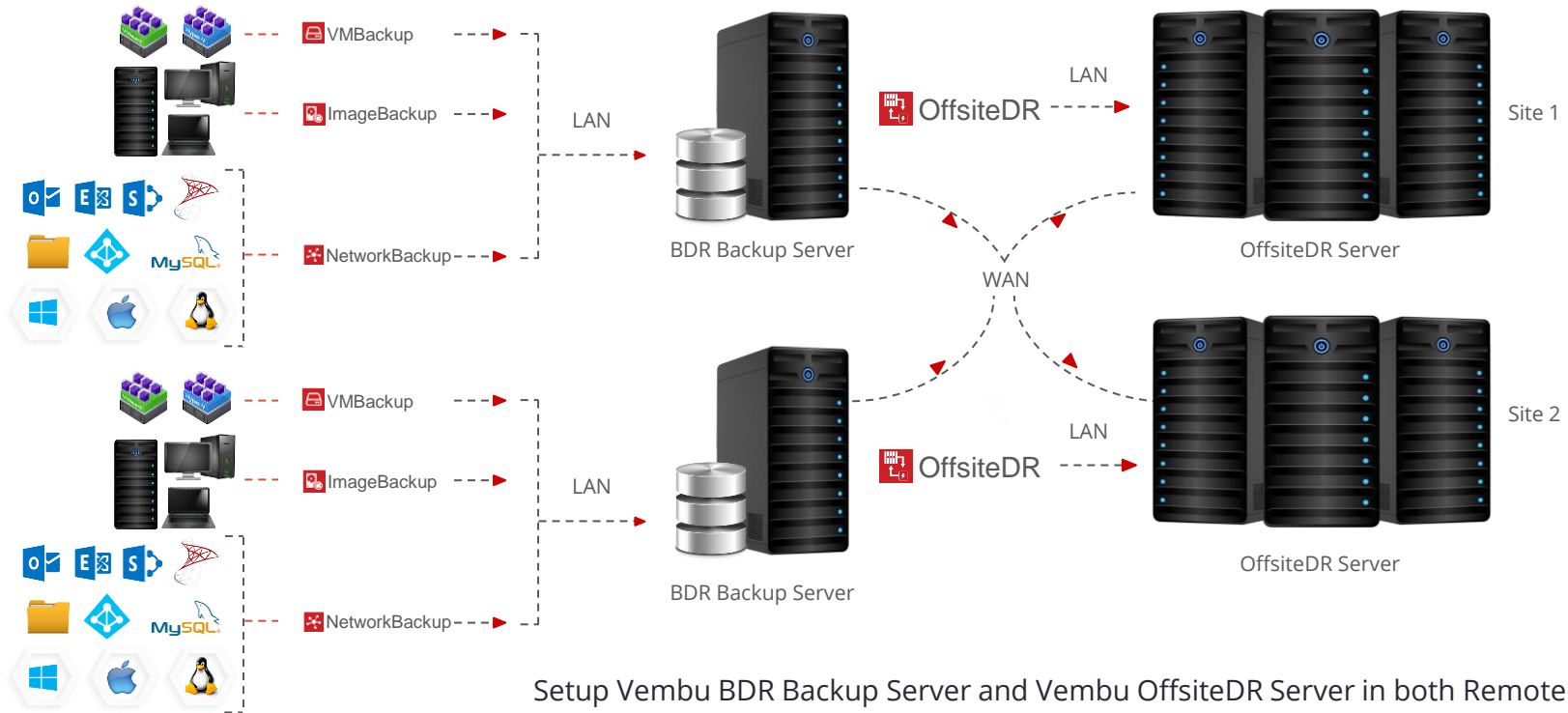
## Migration Plan (P2V, V2V & V2P)

## 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

All-in-one Backup Solution ①

② One Edition for all Businesses

Quick VM Recovery ③

④ Hybrid Cloud Deployment

Scale-Out Storage Repositories ⑤

⑥ Patented In-House File System

Cross Platform Recovery ⑦

⑧ Universal Recovery Tool

24/7/365 Free Support ⑨

⑩ Affordable Pricing



# Acronis

New Generation Data Protection

[www.acronis.com](http://www.acronis.com)



[twitter.com/acronis](https://twitter.com/acronis)



[blog.acronis.com](http://blog.acronis.com)



[facebook.com/acronis](https://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



BASF  
The Chemical Company



LEGO



TESCO PLC



TOTAL

**+200,000 SMBs**

### AMERICAS 40%



IBM



Pfizer



hp



3M



GM



WD



Honeywell



M&S  
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  
National University  
of Singapore



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 3<sup>rd</sup> 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



### Any Storage



### Any Recovery

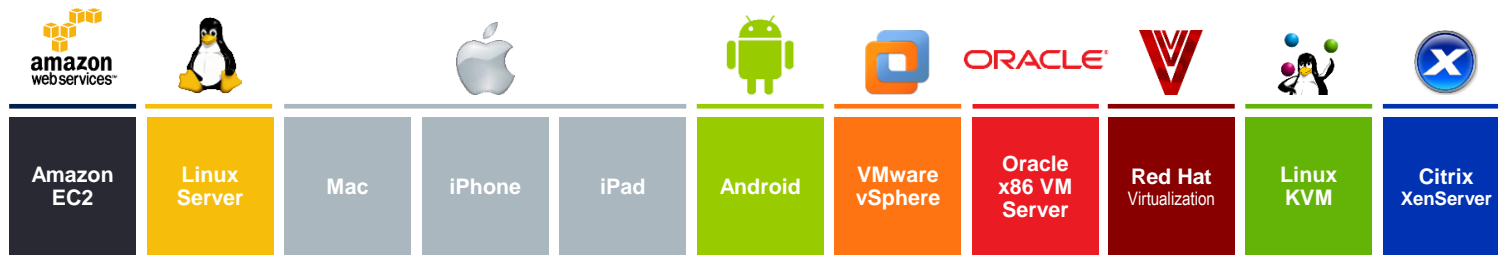
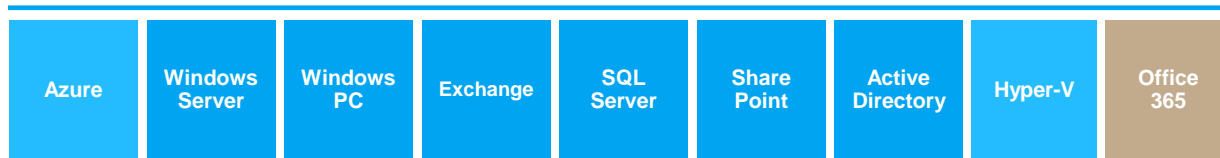
- ✓ Data Recovery
  - ✓ File Recovery
  - ✓ Mailbox & E-mail Recovery
  - ✓ Database Recovery
- ✓ System Recovery
  - ✓ Bare-Metal Recovery
  - ✓ Active Restore
  - ✓ Instant Restore™
  - ✓ vmFlashBack
- ✓ Dissimilar Hardware Recovery & Migration
  - ✓ P2V, V2V, V2P, P2P
  - ✓ P2C, V2C, C2C, C2V, C2P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



Acronis Protects Your Entire Business – On-premises, Remote, Private Cloud, Public Cloud, Mobile

# Acronis Backup Cloud

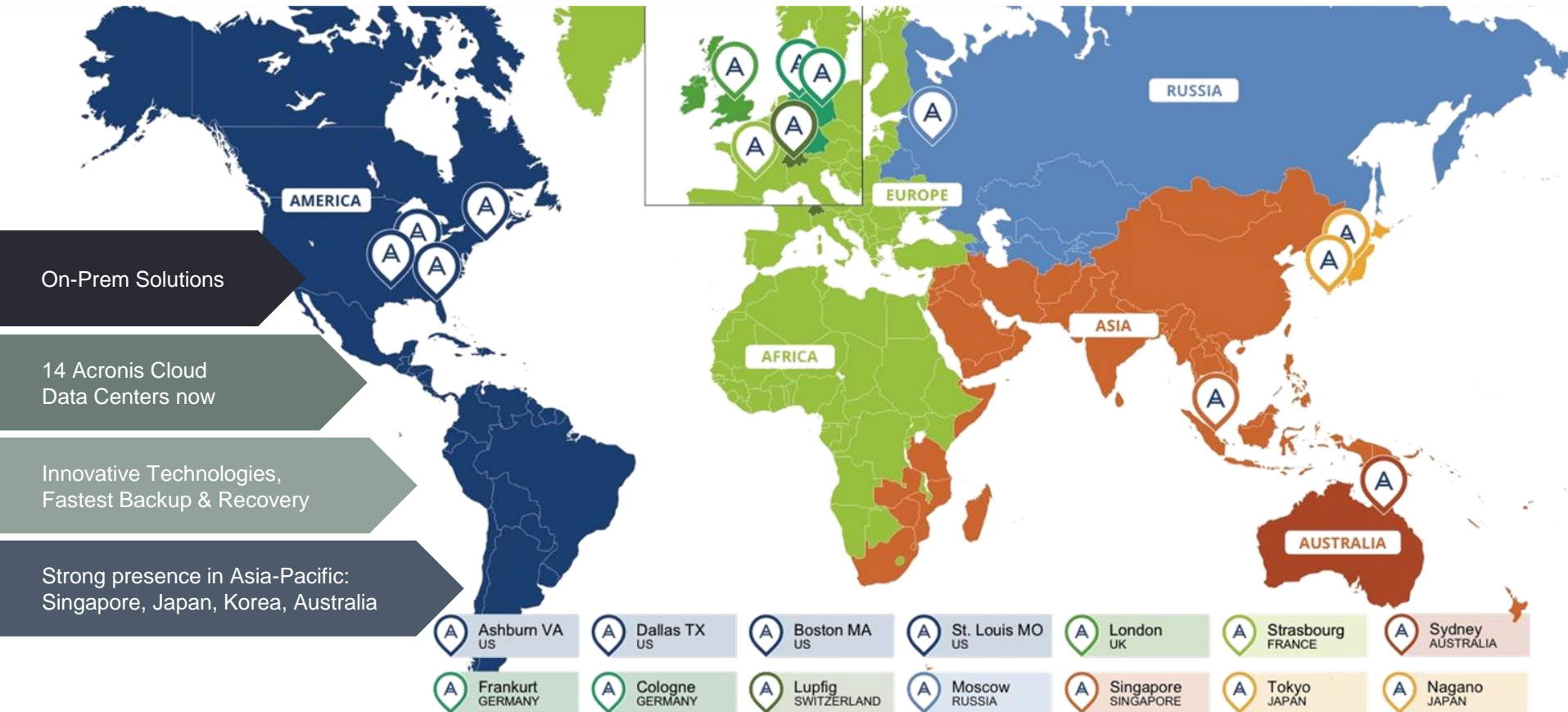
A powerful, hybrid cloud backup solution for service providers that protects more than 20 platforms and lets them quickly realize incremental revenues with zero upfront costs and a pay-as-you-go business model.



## 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



# Impero

## Connect

Fast, Secure Remote Access

# Impero Connect



- Impero 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 Impero 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 tunneling 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

# Impero Connect

MAKING CONNECTIONS

- WHO CHOOSES NETOP?

**50%**

Fortune 100

**23%**

World Top 100 Retailers



**60%**

Financial Times Top 100

**42%**

World Top 50 Banks

# Impero Connect



PORSCHE

SIEMENS



LEVITON

DAIMLER

FUJITSU



Volkswagen



AIR PRODUCTS



KONGSBERG



TOSHIBA



bmc software



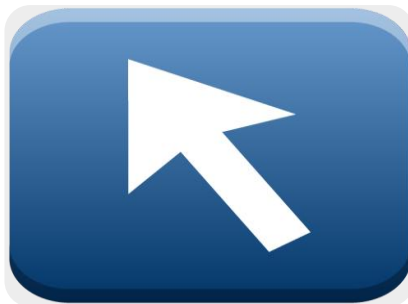
# Impero Connect

- Secure remote access and support



## Impero 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



# Data Security Platform

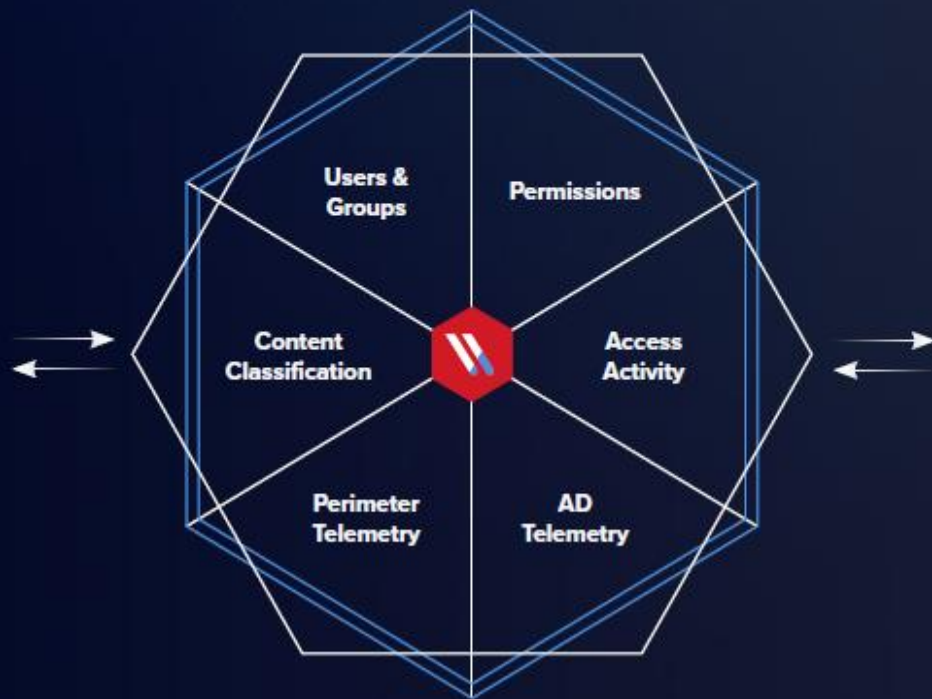
The most powerful way to find, monitor, and protect sensitive data on premises and in the cloud

**Rapidly reduce risk, detect advanced threats, and prove compliance**

Gain visibility into your critical  
data and infrastructure



Combine multiple data streams  
to discover security risks



Solve board-level data security  
problems at scale with automation



# COMPANY OVERVIEW

Varonis is a pioneer in data security and analytics, specializing in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyber attacks by analyzing file activity and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

# IF YOU ARE

- Enterprise that has file shares on Windows, Active Directory, Office 365, UNIX/Linux, NAS, SharePoint, or Exchange
- Enterprise with data on-premises, in the cloud, and especially both
- CISO / C-Level
- Looking for Security
- Having huge IT Storage
- Looking for Governance & Compliance
- Big data analytics

# QUESTIONS

- Where is your sensitive data, and where is it overexposed?
- Do you know where your sensitive data lives - and who can access it?
- What data is being used, and what's stale?
- Who does it belong to, and who has access they don't need?
- What does normal user behavior look like? Who abuses their access?
- Do you know what your service & privileged accounts are doing?
- How can you tell if your data is secure and living in the right location?
- Can you tell if your core systems are being attacked by malware, insider threats, or other security threats?

# KEY PAIN POINTS

- Unable to discover, identify, and classify sensitive data
- Vulnerable to data breaches, cyberattacks, and insider threats
- Unable to detect security violations or potential attacks (including malware and ransomware)
- Difficulty managing permissions and understanding who is accessing, deleting, moving data
- Unable to identify data owners
- No way of identifying stale data or knowing what data can (or should) be archived or deleted
- Compliance and regulatory requirements, including GDPR, PCI, SOX, HIPAA, HITECH, etc.

# IF YOU ARE LOOKING FOR

- User Behavior Analytics (UBA or UEBA)
- Security Analytics
- Data Classification and/or Indexing
- Data Loss Prevention (DLP)
- e-Discovery
- Security Information and Events Management (SIEM)
- Information Lifecycle Management (ILM)
- Hierarchical Storage Management (HSM)
- Identity and Access Management (IAM)
- Data Restructuring / Migration / Consolidation
- Governance, Risk, and Compliance (GRC)
- Compliance regulations: GDPR, SOX, HIPPA, PCI

# ENTERPRISE DATA AND THE INSIDER THREAT

- Varonis protects enterprise data stored on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property. Recognizing the complexities of data security, we have built a single integrated platform for security and analytics to simplify and streamline security and data management.
- **Gartner** estimates over 80% of organizational data is unstructured, and it's **growing 50%** year over year
- Nearly every **major security breach** starts with an **insider**, or an attacker using an insider's credentials – stealing unstructured data.
- It's a guarantee that some of these insiders exist in your organization. Every company has them. **Varonis helps you stop them.**

# HOW DOES VARONIS PROTECT DATA FROM THE INSIDE OUT?

- **Prevent data breaches:** Detect malware, investigate suspicious user behavior, and monitor activity on your data stores.
- **Reduce Risk:** Discover and classify sensitive data, manage permissions, and achieve least privilege.
- **Achieve Compliance:** GDPR | PCI DSS | HIPAA | ISO-27001 | NIST | and more...

# ROI

- **Reduce OP EX:** By introducing automation driven by big data analytics, Varonis measurably reduces overhead and improves the effectiveness of your IT department, and reduces the risk of a data breach by protecting your most sensitive data from insider threats.
- **Reduce CAP EX:** Varonis helps organizations identify and automatically migrate, archive, or delete stale data, in many cases saving thousands of dollars in storage costs per year.

# Panzer IT

MAKE IT SECURE

ND NETAND

scopd

Mirobase  
smart control

SECP-INT®

SOMANSA

falcongaze

EMSISOFT

Acronis

vembu  
Backup & Disaster Recovery

Impero

Netop

LetsGoCart

[www.PanzerIT.com](http://www.PanzerIT.com)