



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.

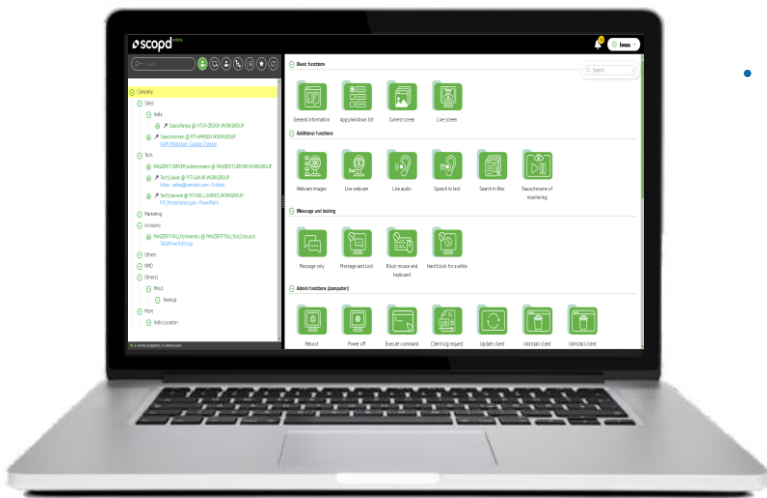


Compliance

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

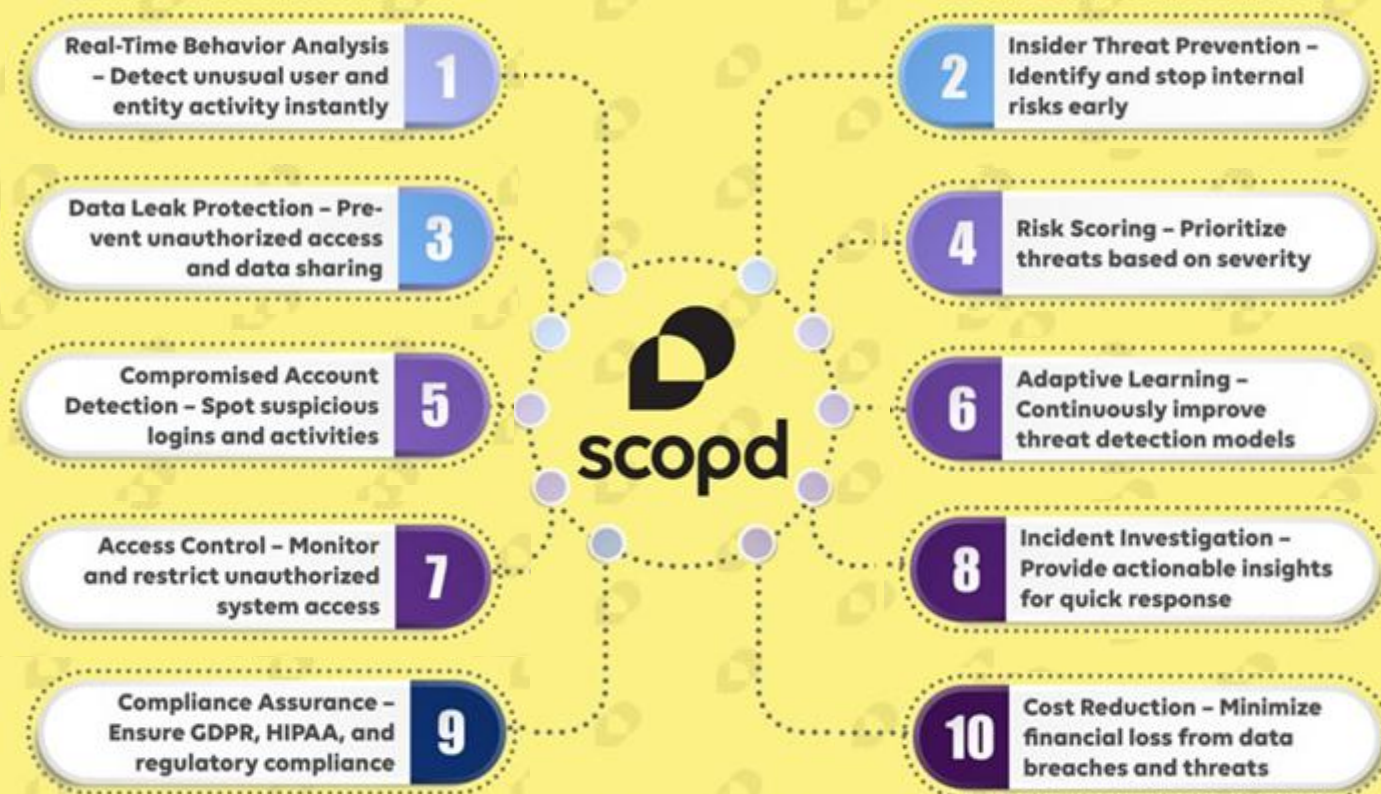


Scopd - Why



- **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
- ✓ Alert Security Team
- ✓ Classify Sensitive Files
- ✓ 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 DPDPA, 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

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



Files sending



File operations



Printing



File classification



Search in files

All reports ☐ Favorite reports

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
	2386		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 - Outlook (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)

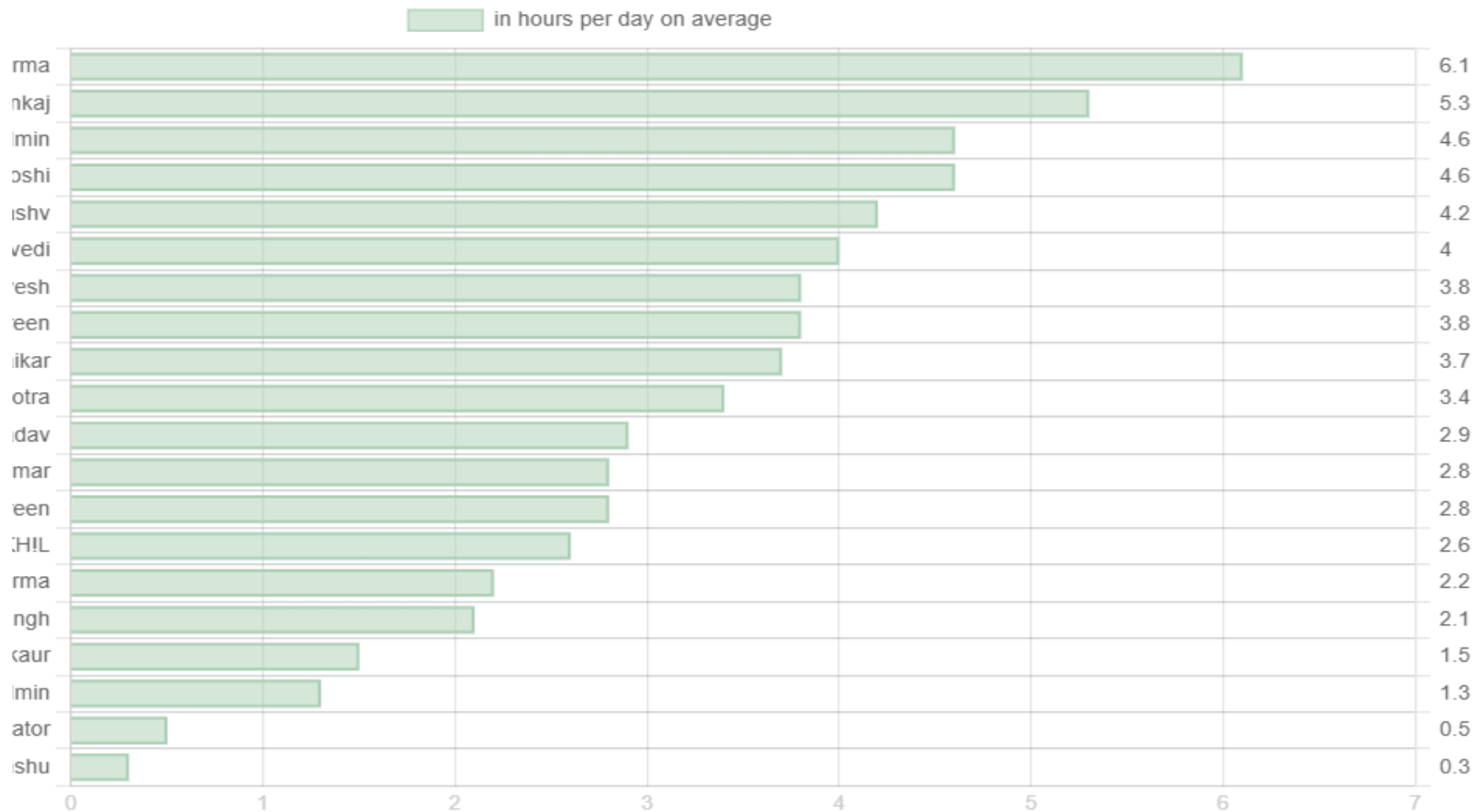
View by all (3,114)

Page 1 from 1



1





Harmful	Unproductive	Productive	Other
0h00m0% ! 1	2h01m8%	8h05m30% ! 28 3h06m12%	1h24m6% 6h36m25%
0h00m0% ! 1	0h11m1% 0h19m2%	6h37m25% ! 26 6h00m34% ! 2	6h38m25% 0h08m1%
		3h20m19%	0h21m2%

Σ 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%\TalkPrimeEditor\talkprime.exe"	 1h10m	32h21m	

View by all (268) ▾

Page 1 from 1



1 ▾



Σ 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)