

Prevent Data Breach & Define
The Predator With Our **Customized**

WATERMARK SOLUTION

Version is 2.1
Last revised: 06-06-022

Datasheet
June 2022



Security and privacy for company's data and information.

In a world where data is becoming more and more a valuable asset, organizations have realized that they do not only need to protect their proprietary information from external attackers, but also from internal ones.

Investing with reliable state-of-the-art security measures and tools to prevent sensitive data breach is essential. However, these measures cannot prevent the breach of sensitive data if insiders can take pictures of the computer screens! Taking pictures leaves no log trail that identifies the perpetrator.

Whilst the number of Insider-Related breaches rises every year, the Verizon 2019 Data Breach Investigations report states that 34% of all breaches in 2018 were caused by Insiders. Here comes the necessity for a solution that can minimize the risk of internal threats and solve the continuous struggle of protecting all company's owned data and information.

Data security is our topmost concern, therefore DataPatrol provides innovative and user-friendly solutions to secure sensitive and confidential internal data from unauthorized disclosure.

You can use and rely on our software even if you are not an IT specialist!



SOLUTIONS



DIGITAL SCREEN WATERMARK

Our solution applies a watermark to all end users machines and servers with detailed information about the logged-in user, IP Address, time, and other metadata that you can fetch from your AD. This feature allows you to set up granular policy control for different groups, and this watermark layer is always on top of the screen.



PRINTING WATERMARK

This feature alters all printed documents to have a dynamic watermark containing user data. This can be applied to any printed document whether printed via a physical printer or into a PDF/XPS document.



ANTI COPY

The AntiCopy feature from DataPatrol allows administrators to control (Enable & Disable) the Copy of texts feature on all windows based machines. When enabled, the feature won't allow users to utilize the copy of any texts, and this can be enabled only when a specific process or application is running.



PrtSc PREVENTION

Anti-PrtSc feature controls and prevents data exfiltration through screen capturing using the Print Screen button or snipping tools. This feature will also log attempts to access the information with the appropriate user's logon name and timestamp.

KEY BENEFITS

IDENTIFY OWNERSHIP OF YOUR DATA



By applying digital watermarks on the screens and printed documents, you make a statement that any data belongs to the company only.

ALERT



Having permanent watermarks on the screens and printed documents, you assure all insiders that these data are confidential, and any exfiltration will be tracked.

FORENSICS



Metadata information will appear on all the screens, so you can track and investigate any publicly shared information.

COMPLIANCE

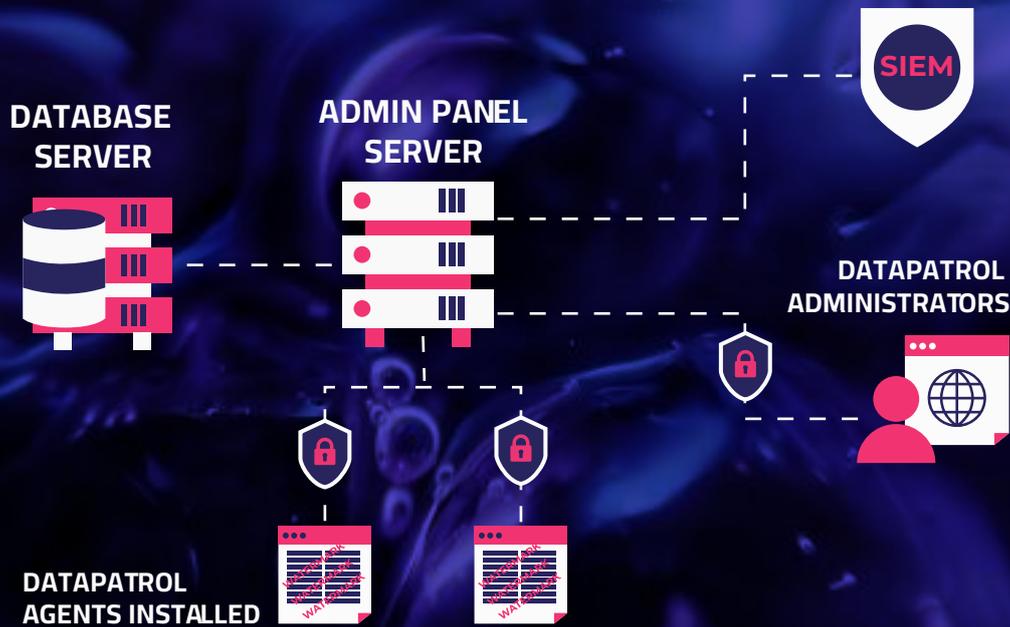


Utilizing the AntiCopy feature which forces Data Entries to write genuine content rather than copying it.



DATAPATROL SYSTEM

HOW DOES IT WORK?



HIGHLIGHTS

- Very light-weight agent, less than 20 MB RAMs and 4% CPU utilization.
- All secured communication between agent/administrator & server side.
- Agent Auto-Start after installation
- Supports Multi-Session for Windows Servers.
- All Administration tasks done through the web interface (GUI).
- Requires a Help-Desk password when uninstallation.
- Supports multiscreen watermark.
- AD Integrated for advanced meta-data.
- Granular Policy Control with policy routes and time scheduler.



**START SECURING
YOUR DATA TODAY**

Get in touch with our Sales Team to learn more about DataPatrol and its features: Sales@datapatrol.com

