Screenshare Interceptor

Protirus Information Protection eXtensions

INTEGRATE YOUR DLP CONTROLS WITH COLLABORATIVE SCREEN SHARE APPS

Prevent accidental or malicious sharing of sensitive content during a screen share

Detect a user trying to share a screen with a sensitive document already open and detect a user trying to open a document when the screen is already shared

Major app support

Supports the three most popular collaborative screen share applications used by enterprise businesses: Microsoft Teams, Cisco WebEx and Zoom.

Influence security awareness at home

Warn a user, with a custom message, that they are about to display sensitive content to a wider audience and force them to think twice about the risk they may be taking.

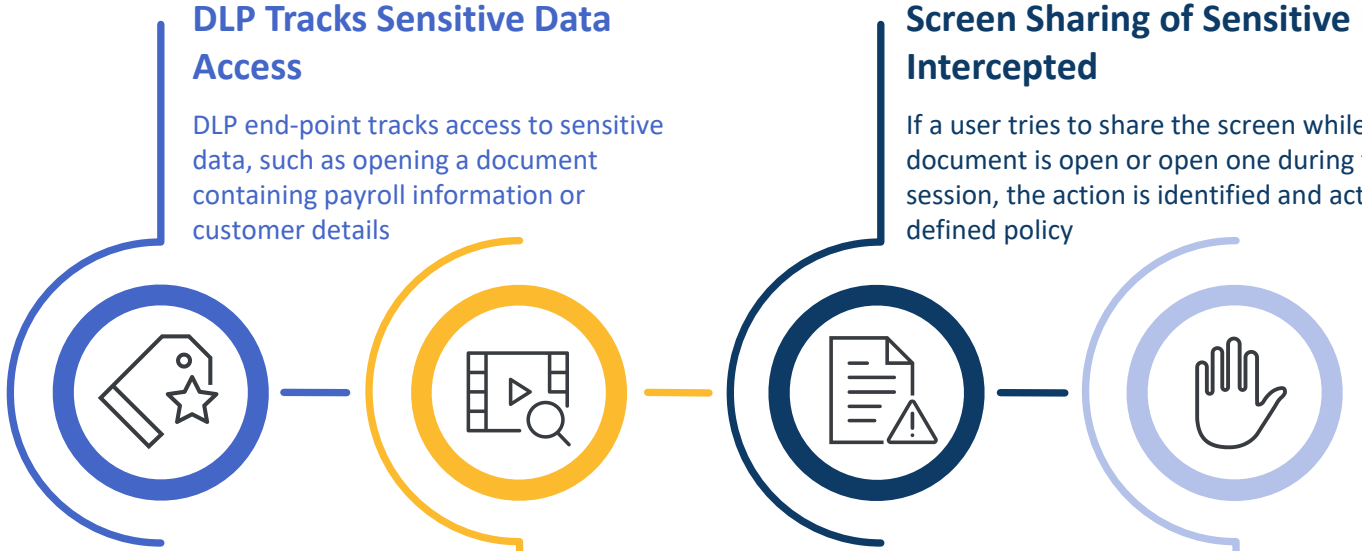
Record and track levels of risk taken

Track the sensitivity and volume of incidents centrally to help assess the risk that screen sharing poses

PROTIRUS

PIPeX Screenshare Interceptor

How It Works



DLP Tracks Sensitive Data Access

DLP end-point tracks access to sensitive data, such as opening a document containing payroll information or customer details

Screen Sharing is Monitored

Screenshare Interceptor monitors the use of collaboration tools and identifies screen sharing activity

Screen Sharing of Sensitive Data is Intercepted

If a user tries to share the screen while a sensitive document is open or open one during the screen sharing session, the action is identified and acted on based on pre-defined policy

Block or Warn

Screenshare Interceptor records the event and enforces the pre-defined action - Block or Warn – notifying the user through a pop-up notice

PROTIRUS

PIPeX Screenshare Interceptor

How It Addresses Your Risk of Sharing Sensitive Data Via Collaboration

Challenges

Remote working or **working from home** most often requires the use of **collaboration tools** to conduct business. When using these to support interaction with third parties, **accidental or malicious oversharing** should be considered – eg, an employee accidentally shared a screen containing sensitive data such as payroll or customer details.

The end-user may have opened the sensitive file hours before the collaborative meeting and accidently shared it on screen or accidently opened it during the screen sharing session.

Users at home have been found to be far more relaxed with adhering to good security practice. This leads to further likelihood of accidental risks being taken.

Solutions

PIPeX Screenshare Interceptor leverages the power of your **End-Point DLP** to identify access to sensitivity data, and combines it with **tracking the use of collaboration tools**. This allows it to detect undesirable behaviours and act on those.

The security administrator defines the policy for when a risk combination (screensharing while having a sensitive document open) takes place, and may choose to have the tool step in to **warn the user of the event, or to block the action**. In either case, the **event is recorded and tracked**.

The use of **pop-ups** directly influences home users to **adopt good behaviours**. By centrally tracking the events and pro-actively warning high risk users, your security team can drive good security practice amongst homeworkers.

PROTIRUS