OPSWAT™

Secure Virtual Desktop

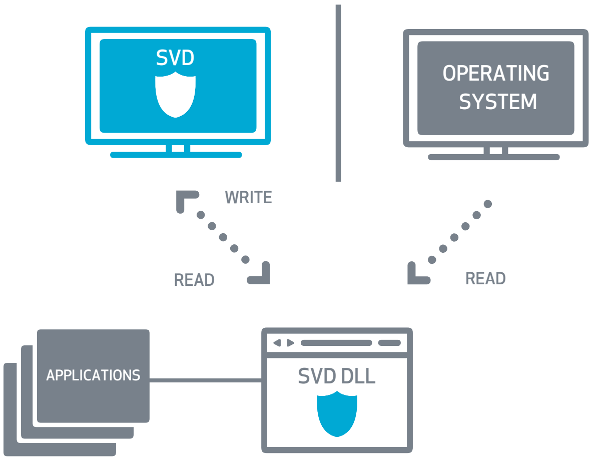
Extending the corporate security policy

OPSWAT's Secure Virtual Desktop (SVD) protects users when accessing corporate applications, networks or data from unprotected devices such as home computers, public kiosks and guest laptops.

The accessibility of web-based applications has changed the way employees and business partners access and utilize sensitive information. On remote systems, corporate security departments cannot ensure the integrity of endpoints or prevent the compromise of enterprise assets such as company financials, customer information, and intellectual property. OPSWAT's SVD is able to extend the corporate security policy by creating a secure environment inside an isolated clone of the file system. The secure environment ensures data security by erasing all activity and changes at session termination, as well as by enabling control over additional settings related to data security.

How It Works

SVD is a virtual clone that sits between a machine's installed applications and its hardware (hard drives, registry, copy/paste buffers, external media, printers, etc.). As applications try to read or write to these sensitive areas, SVD applies security policies from a configuration file, providing control over user access to system resources and over data sharing to and from the isolated environment. For additional security within the session, administrators can create a whitelist to allow only approved processes within the secure session, can configure SVD to utilize third-party encryption libraries, and can set up a proxy to be used within secure sessions.



Secure Virtual Desktop

Key Benefits

- Enables the secure deployment of web based applications
- Protects customer, employee and corporate data accessed by and edited on unmanaged devices
- Enables secure, private browsing with no history or cookies saved, and with a masked IP address

Why should I incorporate SVD into my solution?

SVD is ideal for protecting data accessed over an internet connection. Use SVD to:

- Increase security for users accessing important resources via SSL VPN
- Increase security for users at WiFi hotspots, business centers, airport kiosks, conference centers, hotels, cafés, etc.
- Ensure that users are protected on websites containing sensitive data (banking, accounting, etc.)
- Incorporate data leak protection into your workflow

What can SVD manage?

SVD has many configuration options, allowing the following controls as well as many others:

- Whitelist/blacklist specific applications
- Isolate the copy/paste buffer to exist only within the virtual environment
- Limit access to network drives on the endpoint
- Limit access to external media (USB drives, DVDs, etc.) on the endpoint
- Control which processes are launched at startup
- Control printer access

Features

- Able to use a configuration file located on the local computer or on a server
- Does not require special user privileges: file deletion can wipe anything the user can access
- Preserve or delete resources upon exit
- Supports third-party encryption libraries
- Auto termination after a specified period of inactivity
- Messaging can be localized to user environment
- Accommodates proxy configuration
- Able to specify different configuration settings for specific groups

Available Packages

SVD On-Demand for ISVs

- Simple CLI configuration
- OPSWAT branded "drop and go" executable
- Active X and Java applet code samples

SVD SDK for OEMs

- Robust CLI
- Fully brand-able by OEM

Supported OS

- Windows XP
- Windows Vista
- Windows 7

Licensing SVD

To learn more about commercial licensing of SVD please contact sales@opswat.com.

Learn more and try the demo at www.securevirtualdesktop.com.