FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

Six Reasons VDI + Data Protection Can Strengthen Your Security Posture

Complete Data Protection Against Insider and Outsider Threats with One Agent

The Challenge of Security and Privacy

Virtual Desktop Infrastructure (VDI) brings many advantages to corporate and government IT departments. By separating the physical computer from the operating system and applications, VDI provides a consistent, familiar user experience for everything from a single application to a full desktop environment. VDI can also reduce downtime and data loss due to device failure.

VDI has advantages from a security standpoint as well. It can provide a more "hardened" operating system, limit the applications available to a user, and improve control of patches and versioning. It can also provide limited capabilities for device control and removing administrative rights. Data protection challenges remain in VDI environments however, specifically:

- Monitoring data usage and enforcing appropriate use policies, whether the VDI is accessed through a local network or remotely through a VPN
- Ensuring that data usage policies are enforced consistently across physical and virtual environments
- Maintaining controls for regulatory compliance
- Providing users with information needed to limit risk to data
- Covering all egress channels

Six Reasons Incorporating Data Protection in Your VDI Can Strengthen Your Security Posture

Reason #1: Effective Monitoring of Data Usage

Most data is not static. It moves between users, applications, and physical devices. VDI, while limiting application choices, does not prevent user errors or eliminate opportunities for data loss. The VDI may require Internet access for cloud applications such as file sharing, and allow copying data to physical devices. Data monitoring inside and outside the VDI provides organizations with improved visibility of data usage, and allows enforcement of organizational policies on appropriate use. When access to a physical device is needed, monitoring and enforcement in the VDI ensures that only appropriate data is moved.

Reason #2: Enforce Protection Policies Consistently Across Physical and Virtual Environments

In a VDI, the users can access their virtual desktop from any computer. In this environment, linking permissions to the computer is impractical. A data protection policy is required in the VDI that understands the operating environment, the context of the data, and the action requested by the user. This decouples permissions from physical devices, allowing users to work unimpeded, while the business benefits from VDI's flexibility.

Reason #3: Better Context = Better Compliance

Regulatory compliance standards, including PCI-DSS, HIPAA, NERC-CIP and Executive Order 13587 (addressing the WikiLeaks and Snowden events), require organizations to protect information from loss in VDI and non-virtualized environments. Effective data protection requires an understanding of the full context of the data, user, and action. By applying this intelligence and awareness in the VDI, a data protection solution can support normal business operations, protect data, and provide evidentiary quality logging to support regulatory audits.

Reason #4: Prompting Can Inspire User Compliance

Not all data loss is due to malicious users. Often, users make mistakes due to a lack of awareness of data protection policies, or simple inattentiveness (e.g., an email attachment sent to an unintended recipient). Some users may even operate under the false belief that they are protected from unsafe data handling simply because they are using VDI. Providing consistent and accurate information to users helps educate them to data protection policies, and prevent inadvertent data loss. By prompting users with policy warnings before allowing risky actions users can self-correct. If exceptions to policies are required, Data Protection can record this and maintain logs for auditing and forensics.

Forensic evidence can be lost if a VDI is rolled back or reset after a security event. Without proper forensic analysis, investigators cannot confirm the limits of a breach, potentially forcing broader public notifications. By using data protection in the VDI environment, events related to data usage are recorded in a separate system, and retained regardless of the VDI system state. This allows accurate

legal reporting, better information flow within the business, and effective incident response.

Reason #5: Enforcement of Data Policies Across all Egress Channels

Potential egress channels can be reduced significantly by incorporating thin and zero clients into VDI environments. However, this does not prevent egress through other channels such as email, print, or network uploads. Data protection solutions can effectively manage data egress policies across all channels including email (corporate and web-based), removable media devices, local and network printers, and network uploads.

Reason #6: Improving SIEM and Log Analysis Tools

SIEM and log management tools such as ArcSight and Splunk are great platforms for analyzing data. However, they are completely reliant on the data they receive from the monitored system. If the data forwarded to these platforms lacks context or proper details, the risk increases that events and incidents will be missed, or that false positives will be generated. By using a data protection solution in the VDI, actionable log data captured and sent to the SIEM that can be correlated with other events from network security tools such as firewalls, IPS, and MPS, immediately improving reporting and alerts.

Fill The Virtualization Security Gap With Digital Guardian

Fortra™'s Digital Guardian® supports and enforces multi-session and multi-user policies in VDI environments hosted on Citrix®, VMware®, and MS Hyper-V® servers.

Its agents continuously monitor and log all data interactions with evidentiary-quality forensics, inspect and tag sensitive data using automated rules or user input, enforce context-aware data access and control policies, and manage data egress across all data interactions. Data use and movement are managed appropriately for employees, third parties, and administrators.

Digital Guardian is the only data protection solution for VDI environments providing:

- **Full Data Visibility:** Real-time visibility of all data movement and data transmission methods across online, offline, physical, and virtual environments, including email, cloud storage, removable media, print, and FTP
- **Effective data-loss risk management:** Accelerates policy implementation based on data, user, and event context. Stops known threats, such as source code transmission via USB, and exposes unknown threats, such as synchronization of sensitive data to the cloud via Dropbox
- **Noninvasive, context-aware protection:** Automatically blocks and controls only those behaviors that pose a threat to your organization based on user, event, and data type
- **Privileged user monitoring:** Applies data protection policies equally to regular users and users with full local administration (roots access) privileges — independent of the operating system security model in place

VDI + DP =Strengthened Security Posture

VDI allows businesses to provide a more consistent and reliable user experience in today's world of BYOD. However, VDI does not eliminate the risk of data loss. By integrating a data protection solution across the physical and virtual environments, organizations can meet internal security goals, improve ROI on SIEM and log analysis investments, comply with regulatory standards, educate users effectively, and reduce the risk of data loss.

About Digital Guardian

At Fortra™'s Digital Guardian®, we believe in data protection. We know that within your data are your company's most valuable assets. The sum total of innovations, plans and potential. We protect your company's sensitive information like it's our own so you can minimize risk without diminishing returns.

For over 10 years we've enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.