

## Securing Citrix® Metaframe® and Microsoft® Terminal Server Environments with Digital Guardian™

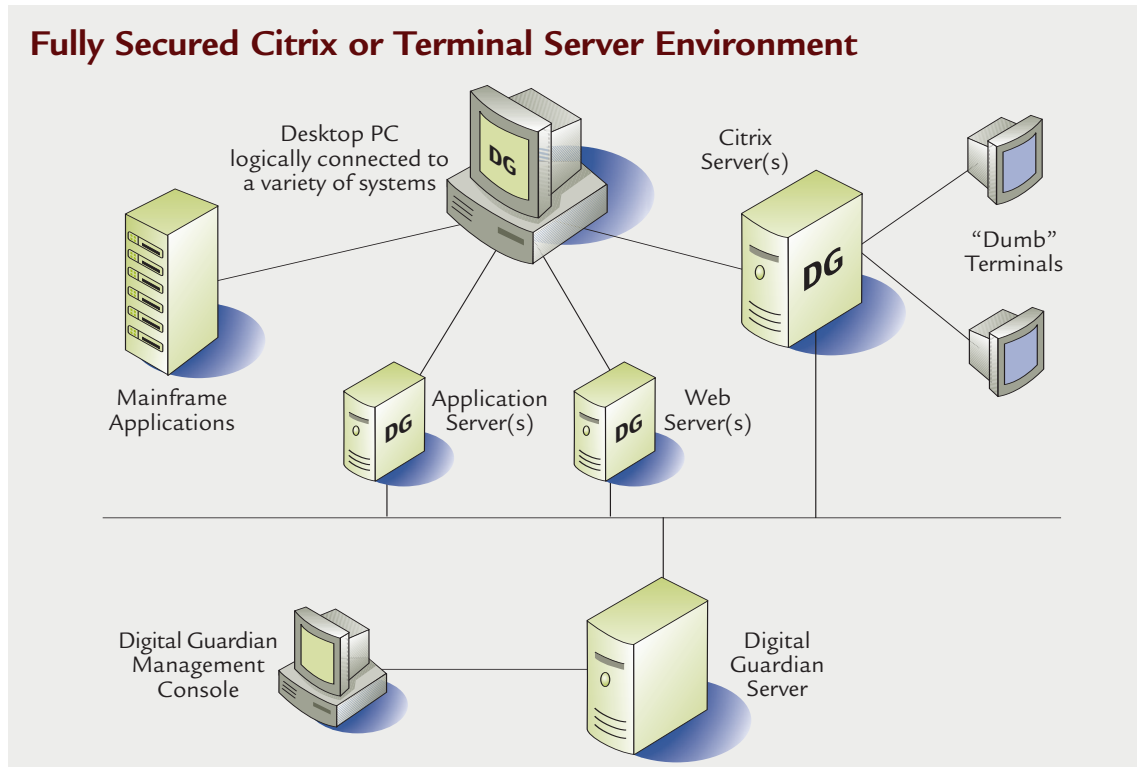
### OVERVIEW

Remote desktop client technologies have become an extremely powerful and cost-effective way to provide access to enterprise applications. Products such as Citrix MetaFrame Access Suite and Microsoft Terminal Server allow companies to centrally deploy business-critical applications and enable secure access by authorized users over a network connection. The remote access client software facilitates a virtual user session into the server where the application is running and remote users employ the published application as if it were running on their local computer.

Although these systems provide a secure way to access and communicate with the application server, they may create security gaps on the remote client. This risk is particularly high in the case of custom or internally developed applications that were not designed with remote deployment in mind. Typical application functions can present a host of unexpected vulnerabilities that can lead to the leakage of sensitive or regulated corporate data:

- A published application requires connectivity to network shared directories, which allows users to access data files directly.
- **Risk:** Users may access shared directories indirectly.
- A published application requires open network ports to access data.
- **Risk:** A user may initiate a virtual session as an unauthorized jump point to internal network resources.
- A published application requires the command line to run external commands.
- **Risk:** Users may start unauthorized programs from the command line.
- A published application serves as a front-end to other programs.
- **Risk:** The launched programs may not be under the same information security controls as the main application.
- A published application offers built-in web browsing capabilities.
- **Risk:** Users might gain access to intranet resources that were not intended to be reached from remote networks.

### Fully Secured Citrix or Terminal Server Environment



The Verdasys information security platform, Digital Guardian, secures remote desktop client technologies by providing complete monitoring and control over application and data access and usage. Easily put into service across a distributed infrastructure, the solution can be implemented in centralized, server-based environments, desktop/laptop-based personal computing environments or hybrid environments.

With Digital Guardian, corporate information usage policies are translated into a set of business rules. Covering anything from prohibited user actions to file, application and network privileges, these rules are actively enforced in real-time by Digital Guardian "agents" that monitor and track all activity and block unauthorized actions. This comprehensive management of activities by remote and onsite users alike enables organizations to prevent the accidental or intentional misuse of valuable data.

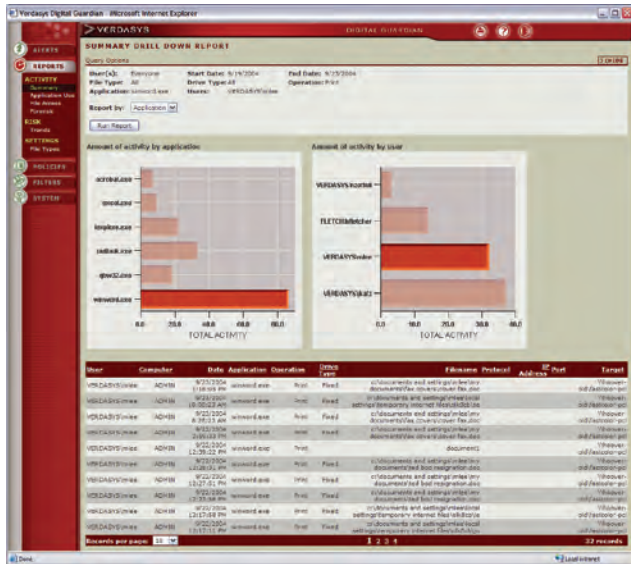
## IMPLEMENTATION

Digital Guardian makes it possible for companies to harden each Citrix or Terminal Server virtual session that publishes enterprise applications. By deploying Digital Guardian at the publishing server, companies can ensure that applications running within a virtual session only perform operations that are in line with normal application usage.

### Agent-Based Deployment

In a typical remote access scenario, an enhanced Digital Guardian agent is installed on the Citrix server or Terminal Server. This "session-aware" agent keeps track of each virtual session and treats each session as though it were an independent computer system. This provides complete control over each user using a "dumb terminal," even though Digital Guardian is not directly deployed on their device.

Issue	Solution
A published application requires connectivity to network shares to operate.	Implement a Digital Guardian policy that blocks connections to network shares and specific file types not needed or not accessed by the published application process. The policy should specify the combination of file types to be blocked and the off-limit network shares.
A published application requires open ports to access data.	Implement a Digital Guardian policy that blocks any network connection not needed by the published application. The policy should specify the combination of the published application process identifier, remote address and remote port to be allowed and should block everything else.
A published application requires the command line to run external commands.	Implement a Digital Guardian policy that allows only specific batch files, scripts and executables to be launched from the published application and blocks everything else.
A published application is a front-end to other programs.	Implement a Digital Guardian policy that controls use of launched applications and specifies what applications can be launched by the published application.
A user of a published application attempts a clipboard operation or file save to a removable media such as a CD burner or USB drive.	Implement a Digital Guardian policy that blocks this activity or warns users that their attempted activity violates corporate policies.



Detailed activity reporting combined with high-level aggregate reports provide a comprehensive view of enterprise information usage and risk trends as well as easy navigation to forensic quality detail.

### Policy-Driven Data Security

Digital Guardian's advanced user activity control capabilities provide the flexibility to secure even the most complex environments, including custom-developed applications and legacy applications. Digital Guardian can support any number of policies designed to reduce vulnerabilities specific to applications running within a remote access environment.

Digital Guardian also provides critical data and application protection capabilities when personal computers are used for remote access. Often these desktops or laptops are used for multiple purposes with an occasional or simultaneous connection into the Citrix or Terminal Server environments. To provide complete control over this hybrid environment, a Digital Guardian agent should be also be deployed on the remote PC. With this approach, any activity is monitored, recorded and controlled at the desktop itself, eliminating the potential for information leakage at the point of use.

### User-Level Control

Since Digital Guardian policies are user-based, each time a user logs onto a Citrix or Terminal Server environment and launches applications or attempts to access resources, the policies developed for the user's group and for that specific user are applied. Even if multiple employees use the same computer terminal to log onto a Citrix or Terminal Server environment, the appropriate policies for each individual user are applied.

### Consistent Enterprise-wide Reporting

Digital Guardian agents collect extensive usage data that is provided in high-level reports that offer an aggregated view of user activity as well as query-based, more detailed reports sorted by parameters such as application name, user name, type of policy violation, etc. With Digital Guardian, this data is consistently captured, archived and presented whether sourced from a desktop, laptop, IBM 3270 or "host on demand" application or thin client, Citrix MetaFrame or Microsoft Terminal Server environment – giving security managers comprehensive insight into data and application usage across the entire enterprise.

### SUMMARY

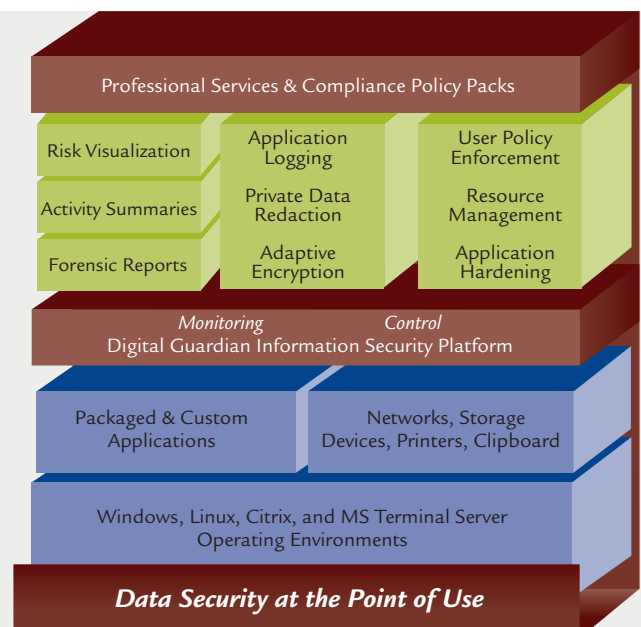
To give workers on-demand access to the information they need to do their job, many organizations implement Citrix MetaFrame and Microsoft Terminal Server environments. These solutions present an effective way to connect remote users to enterprise applications, but may introduce potential information security risks. Verdasys Digital Guardian effectively plugs these remote access-based security holes and provides seamless control over information flows within a department or across the enterprise.

## VERDASYS INFORMATION SECURITY SOLUTIONS

Verdasys delivers information security solutions that address business-driven requirements for assuring compliance with a broad range of regulatory mandates; safeguarding the privacy of client and patient records; and preventing the misuse and theft of intellectual property.

Offering a compelling set of solutions for a wide array of data containment, global outsourcing and information protection challenges, the Verdasys Digital Guardian platform offers real-time, autonomous data-level monitoring and control. In addition to minimizing the information security risks posed by technologies such as e-mail, IM and USB drives, Digital Guardian detects and interdicts violations of information usage policies – thus creating a corporate culture centered on accountability.

Verdasys clients include Fortune 500 corporations – in industries ranging from insurance and financial services to multimedia and pharmaceutical – who are setting industry benchmarks for information security. To join them, contact us at [compliance@verdasys.com](mailto:compliance@verdasys.com)



## VERDASYS

950 WINTER STREET, SUITE 2600 WALTHAM, MA 02451  
781-788-8180 TEL 781-788-8188 FAX

COMPLIANCE@VERDASYS.COM WWW.VERDASYS.COM