



## Protect Your Business

Dealership-wide Solutions

U.S.

Fight one of the biggest threats to your business with a networked antivirus solution created specifically for automotive dealerships. Reynolds' solution enables you to protect your networked Windows®-based PC desktops by utilizing a managed distribution server.

### A Growing Threat

Computer malware is more than a nuisance. It is a potential threat to your business, your customers, and your bottom line. Desktop security can be a time and resource-consuming headache for your dealership. The stakes are high and today's threats can't be ignored. Hackers are designing increasingly deceptive and destructive malicious software in the form of viruses, worms, spyware, and Trojan horses.

The U.S. National Institute of Standards and Technology reports that software vulnerabilities are rapidly increasing.<sup>1</sup>

Such exploited vulnerabilities may allow:

- Access by criminals to sensitive information.
- Outsider control of internal IT resources.
- Slow PC and network performance.
- Denial of services.
- Network failure.

Such attacks are on the increase, especially among small to medium-sized businesses that are generally not fully prepared. A solid business reputation and secure bottom line are critical to a dealership's continued success. In fact, the Ponemon Institute reports 70% of Americans fear becoming victims of identity theft.<sup>2</sup> Businesses like yours, with personal information stored within their computer network, must take action to make the information secure.

### Peace of Mind

Protecting your dealership's Windows PC network with Desktop Security couldn't be simpler. Reynolds' solution provides a central management console running on a distribution server equipped with industry leading security software. Though the solution requires little management, the console allows the network administrator to easily manage the dealership's desktop security program from one location. To

keep your protection current, Desktop Security allows PCs to automatically poll the centralized distribution server for new security definitions, not the Internet, thereby reducing PC dependence on Internet bandwidth.

**The Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry-Data Security Standard (PCI-DSS) require dealerships to safeguard customer information.**

# Desktop Security

## What Desktop Security Can Do For You

According to some sources, the virus problem doubles every 14 months, so it's vital to install antiviral software on every PC in your network—and just as important to keep it updated as new virus threats are identified. You can rely on Desktop Security for effective, continually updated network protection that saves you time and helps shield you from danger.

- Networked PCs automatically pull virus definition updates every hour from the distribution server instead of the Internet, keeping normal business activities uninterrupted.
- Enables one administrator to manage network-wide antivirus protection from a single PC, and automates most tasks to minimize the time required to manage them.
- Cleans or quarantines any file infected by a virus.
- Helps protect your network from the most common types of malicious software such as viruses, spyware, Trojan horses, and worms.

<sup>1</sup> <http://csrc.nist.gov/>

<sup>2</sup> <http://www.ponemon.org/>

*Desktop Security is designed to protect your networked PCs from these common types of malicious software:*

- **Viruses** can make copies of themselves and then attempt to infect other computers that are exposed to them. Viruses can be transmitted as e-mail attachments, downloads, or through sharing computer disks or files.
- **Spyware** is secretly installed software used to intercept or take partial control of a PC without the user's consent. Spyware can secretly monitor system activity on an infected PC, capturing information and exploiting the infected computer for commercial gain.
- **Trojan horses** are programs that are not what they appear to be, but in fact contain harmful code. They often leave a "back door" into the network, allowing hackers to access the system in the future or start programs when an infected PC is started.
- **Worms** are usually self-replicating programs, but some also carry malicious code. Generally they do not alter files, but their uncontrolled replication consumes system resources, slowing or halting other tasks—potentially bringing your network to a standstill.

*Important User Notice: Antivirus protection such as Desktop Security is a critical component of an information security program. It is important for users to understand that no virus protection technology can guarantee detection and treatment of all viruses and any virus protection technology should be implemented in the context of a comprehensive information security program. Desktop Security can provide protection to any automotive dealership independent of the DMS provider.*

**For more information on Desktop Security, please contact your Reynolds Account Manager, call 800.767.7879, or e-mail [marketing@reyrey.com](mailto:marketing@reyrey.com).**



MAKING BUSINESS BETTER.