

# Protect Your Business

U.S.

Dealership-wide Solutions

## Reynolds Antivirus Service 2.0

### Ask Yourself...

- ❓ How often does productivity suffer because PCs are infected and consequently slow down?
- ❓ Is your business and customer data protected from malware designed to steal sensitive information?
- ❓ How susceptible is your network to newly-developed viruses?
- ❓ Are you manually administering antivirus updates? How can you be sure you've successfully updated every PC?

**Google reported that up to 1.3% of search results return at least one malicious URL.<sup>1</sup>**

### Expect Results

- Keep customers' personal information secure.
- Protect your customers and brand image by preventing the risk of embarrassing or infected email blasts.
- Detect and deny access to viruses before they infect PCs and affect business operations.
- Save time and rest assured computers are up-to-date with automatic virus definition updates.

<sup>1</sup> Google

<sup>2</sup> Symantec Internet Security Threat Report

### Are You Prepared?



286 million new Internet threats were detected in 2010, and this number is expected to rise each year.<sup>2</sup>

## About Reynolds Antivirus Service 2.0

Fight one of the biggest threats to your business with a centrally-managed networked antivirus solution created specifically for automotive retailers.

Reynolds Antivirus Service 2.0 is designed to protect your networked PCs from these common types of malware:



**Viruses** can make copies of themselves and then attempt to infect other computers that are exposed to them. They can be transmitted as email 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. It 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 and potentially bringing your network to a standstill.



**Fake Antivirus (AV)** deceives an unsuspecting user into installing other malware by posing as an antivirus software.

Survey results show 63% of small businesses expressed viruses as their greatest IT concern.\*

## Highlights

- One administrator can manage network-wide antivirus protection from a single PC.
- Networked PCs automatically pull virus definition updates at regular intervals from the central server instead of the Internet, keeping normal business activities uninterrupted.
- Cleans or denies access to any file infected by a virus.
- Behavior-based ("zero day") protection proactively detects and denies access to viruses before a fix has even been created for them.
- Quickly ensure each PC is protected with a "System Status" view.

Computer malware is more than a nuisance. Protect your business and your customers from potential threats with Reynolds Antivirus Service 2.0.



MAKING BUSINESS BETTER.

\*Trend Micro Survey