I AM NCR
THREAT DEFENDER

Protect against threats that find their way through network-level defense

Threat Defender is part of the NCR Network and Security Services suite. When it is installed, it is designed to safeguard your computer systems. The software agent helps control what applications may or may not run on your system to minimize disruptions due to a virus infection, a network compromise or a self-inflicted problem. Threat Defender can help increase productivity and protect from malicious threats for your business.

Safeguard your computer system

An approach to securing systems by restricting which software is allowed to run on them to drastically decrease the opportunity for malicious programs to infect the protected computer is known as application whitelisting.

Traditional antivirus tools allow software to run unless it is considered malicious, which often allows malware to evade detection. Application whitelisting allows only trusted applications to run, blocking other software from executing under the assumption that it's malicious or undesirable.

Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 300 million transactions daily across the retail, financial, travel, hospitality, telecom and technology industries. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 26,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

Additional layers of security

Threat Defender includes host intrusion prevention system (HIPS) capabilities, which offer an additional layer of security to the system. HIPS accomplishes this using real-time behavioral techniques through:

- Kernel-level protection against applications that attempt to modify important operating system files, processes and registry keys.
- Protection against exploits that place code inside a process' data segment.
- Overseeing of the programs that attempt to run during the system's startup.
- Watching the system for unusual file access activities.

Key features

- Increase productivity by limiting employee access to non-business related applications.
- Protects system by not allowing malicious programs to run.
- Lower your IT costs by preventing malware and viruses from affecting your systems stability.
- Safeguard your system by preventing the unauthorized installation of programs.