



# RECAP

## REDiSAFE: Keep it safe, keep it secure

Do you know where your corporate data is? Locked away safely on banks of servers in climate-controlled secure facilities, backed-up hourly? But then your CEO spills a cup of coffee on his notebook, a virus cripples your call centre computers, an ex-employee wipes his harddrive. Months of work vanishes instantly, and all that's left - if you're lucky - are a few outdated CD and tape back-ups.

### 80% of corporate data is on your desktops and notebooks.

Corporate desktops and notebooks are notoriously difficult to protect. Physically scattered and under heavy daily use, they come in a dizzying multitude of hardware and software configurations. To securely back them up, IT departments need to track every unit and either handle tedious back-ups themselves, yet another responsibility for the IT department, or train users to do their own back-ups, and somehow enforce that discipline. Some companies force users to work off the central server, limiting mobility and security.

### The Big Four

There are four main threats to corporate desktops and notebooks:

- hardware failure
- external intrusion
- internal sabotage
- privacy

Check if your company's disaster recovery plan covers desktops and notebooks as well. Users need to have access to robust back-up hardware, from simple CD-burners to centralised tape back-ups. Mirrored back-up cuts the risk of a single hardware point of failure. While your company's network may be protected by firewalls and intrusion detection systems, find out if that extends to individual desktops and notebooks. With mobile executives, check if home or travel networks will expose them to vulnerabilities. Frequent backups mean a faster recovery from external attacks. When you're evaluating a back-up system, consider how robust it is. Look for a system that can be integrated within your own secure network.

A slip on the keyboard can accidentally destroy weeks of data, so make sure there's a



Extremely strong security can be simple: REDiSAFE's server tokens are the physical keys that keep hackers out, while allowing emergency corporate access

simple way for employees to recover lost data without having to involve the IT department. Disgruntled employees can deliberately wreck havoc. Look for multiple security measures such as emergency key tokens for your back-up system's administration to prevent unauthorized internal attacks. All back-ups are not equal. Look for a system that either lets you distinguish between highly-sensitive data and routine back-ups, or one that provides individual vaults for every user, ensuring no leaks and compliance with corporate and legal privacy regulations.

### The Preferred Solution

The best solution would offer ease-of-use and robust secure hardware with features like individual vaults, automation and tiered-security. REDiSAFE's appliance includes these and more. With its Linux-based operating system, end-to-end data security and encrypted transport and storage with full authorization, REDiSAFE delivers premium security that's resilient to virus and hacking attacks.



REDiSAFE is preferred by IT departments for its near-zero daily administration, thanks to its highly automated self-contained administration and web-based client application. Adding more disk space and disaster recovery mirroring is as simple as plugging another box into your network.

REDiSAFE has a strong support network across Asia, including China.

MHI South East Asia uses the REDiSAFE backup as a complete back-up for all the individual desktops simply and securely.

"We've been using it for more than two years," said Saravanan, System Manager at MHI. "We're very satisfied. It supports all the operating systems. It's the most secure and it's a good remote system."

MHI switched to REDiSAFE on the recommendation of their system vendor. "We use the back-up restoration maybe four or five times a year," said Saravanan. "It's very easy and fast, with recovery within a few minutes." His endusers find the REDiSAFE interface "easy to use", he said. Data privacy is a priority for MHI, and Saravanan pointed to REDiSAFE's strong encryption and integration with their internal security systems.