

Data Turnover Protection

Protecting your organization from e-mail data leakage or orphaned data during times of workforce turnover

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Table of Contents

The workforce is fluid – data doesn't have to be	1
Data needs to be retained	2
Productivity tools can become counterproductive	3
Businesses need to remain flexible	4
Data Turnover Protection	5
Shield Your Data from Turnover with SonicWALL Data Turnover Protection	6
SonicWALL Email Security	7
SonicWALL Continuous Data Protection	8
SonicWALL Network Security	9
SonicWALL Secure Remote Access	10

The workforce is fluid – data doesn't have to be

In times of workforce turnover, you need to retain mission-critical data to keep your business teams productive. People are the lifeblood of any organization and the work they produce is critical. Workforce turnover is an everyday occurrence and an ongoing challenge that's especially significant in today's economic climate.

Do you risk losing intellectual property whenever an employee exits your organization?



Departing employees frequently don't end-up forwarding their crucial data, e-mail and voicemail to their replacements. Sometimes there is no designated replacement or sometimes a transition is ill planned. Whatever the reason, workforce turnover can threaten the security of mission-critical data and corporate intellectual property, bottleneck productivity, and result in lost business opportunities and lost revenue.

Data needs to be retained

Whenever people leave any organization, productivity is threatened. Continued productivity depends on seamlessly retaining every team member's intellectual property, such as prospect lists, business plans, research or financials, and withholding it from unauthorized disclosure. In order to retain such mission-critical intellectual property, your organization needs to be able to enforce policy to capture and protect any potential orphaned data.

Orphaned data is any business information, application or intellectual property that has become unrecoverable because it was left on no-longer-accessible edge devices that were not backed up such as laptops, smartphones or PDAs.



For IT, this means demanding backup and recovery solutions that deliver full functionality at the most affordable price-point, to clearly demonstrate the greatest return on investment. At the same time, businesses need to choose solutions that streamline and automate management overhead, to reduce total cost of ownership.

Productivity tools can become counterproductive

It is not uncommon for employees to be unaware of corporate policy and for them to try to e-mail sensitive documents to themselves or other third parties without company authorization—and without any policy controls put in place to prevent it.

Productivity tools like e-mail become counterproductive when they transmit business plans, company financials, product roadmaps and other confidential documents outside the corporate network.



A recent IT security study demonstrated that 56% of workers surveyed feared layoffs, and over half had downloaded competitive corporate data in anticipation of getting another job. And ComputerWorld reports that layoff rumors can lead sales reps to download customer, order, and payment histories to their personal e-mail accounts. Finally, Forrester Research reports that the most common threat today is that an employee may take intellectual property, including strategic plans or customer data, before or soon after that employee is let go.

¹ Cyber-Ark Software Inc. 2008 (as reported in Computerworld, March 2, 2009)

² March 2, 2009

³ Jonathan Penn, as reported in Computerworld, March 2, 2009.

Businesses need to remain flexible

Fluctuations in today's market can mean the sudden need to expand your organization to newly acquired, added, or more widely distributed locations, or identify cost-savings in the form of reorganization or consolidation.

Businesses must be able to respond flexibly to rapid shifts in workforce requirements.

Businesses may need to quickly add or subtract new and returning employees, contractors, consultants or outsourcers.



SonicWALL's Data Turnover Protection – Provides Critical Dual Protection

1 Locks down potential leaks of sensitive information over corporate or private e-mail

During turnover, organizations need to be mindful of controlling outbound transmittal of confidential and sensitive intellectual property like business plans, research, prospect lists, financials, or product roadmaps, whether over corporate e-mail like Outlook® or even private e-mail accounts like Gmail®.

Data Turnover Protection establishes granular policy for in-house, remote, and mobile employees, contractors and consultants, which can enforce restrictions with automatic responses ranging from gentle reminders to blocked e-mails.

2 Ensure productivity after turnover by easily recovering important information to ensure productivity after workforce turnover

Businesses need to ensure the backup and recovery of all potential orphaned data left behind in the inevitable “black hole” of laptops, smartphones, at-home laptops or personal folders whenever staff members leave during workforce turnover.

Data Turnover Protection automatically saves data, applications and settings every time they are updated, from servers, desktops—even mobile laptops—continuously whenever employees are on the network, instead of only once a day like tape backup. You know the data you need is available when you need it.

Shield Your Data from Turnover with SonicWALL Data Turnover Protection

Responding to the ongoing challenge of mitigating the business risks of workforce turnover, SonicWALL® Data Turnover Protection unites four award-winning SonicWALL technologies into a comprehensive, aligned solution, featuring:

- Email Security
- Backup and Recovery
- Network Security
- Secure Remote Access/SSL VPN

The combined multi-layered protection of the SonicWALL Data Turnover Protection solution means you don't have to downsize productivity because of leaked or lost intellectual property due to employee turnover.



SonicWALL Email Security

SonicWALL Email Security (SES) is an award-winning anti-spam, anti-virus, anti-phishing, policy, and compliance management solution offering high-performance e-mail protection. As a component of SonicWALL Data Turnover Protection, SonicWALL Email Security controls leaks of sensitive information with robust inbound and outbound policy enforcement, including scanning for specific sensitive words or phrases in e-mails—or in over 300 attachment types like Word, PowerPoint and PDF files—and responding with appropriate actions.



SonicWALL SES controls e-mail leaks of sensitive information and intellectual property via e-mail content and attachments.



SES offers an easy-to-use Web-based administrative interface, allowing easy implementation of a wide range of policy management rules for both inbound and outbound e-mail, applied company-wide or to specific users or LDAP groups. Additionally, SES enables central monitoring of policy impact by placing all matching e-mails in a named Approval Box for review.

SonicWALL Continuous Data Protection

SonicWALL Continuous Data Protection (CDP) offers complete end-to-end disk-based backup and recovery all in a single, easy-to-use, reliable solution, featuring flexible options for Offsite Data Backup, Site-to-Site Data Backup, Local Archiving and Bare Metal Recovery. CDP enforces reliable, automated backup policy, even for traveling or remote laptop users whenever they are on the network.

SonicWALL CDP protects loss of mission-critical information during workforce turnover.



As a component of SonicWALL's Data Turnover Protection, SonicWALL's automatic disk-based backups are worry-free, continually backing up every time a file is updated, unlike once-a-day and human-error-prone tape-based solutions. End users can easily recover data for themselves in just a couple minutes and with no IT intervention. Administrators can easily recover whole workstation or server systems, including operational settings and applications like Exchange, SQL Server and Active Directory.

SonicWALL Network Security

SonicWALL Network Security combines patented high-speed Reassembly-Free Deep Packet Inspection™ (RFDPI) technology with robust Unified Threat Management (UTM) security services. As a component of SonicWALL's Data Turnover Protection, SonicWALL Network Security mitigates Web-mail and data loss over services like Yahoo® or Gmail by enabling Application Firewall policies that can detect and block any outbound e-mail that contains sensitive or confidential information. It can also scan and block transmittal of documents in attachments with e-mail applications like Microsoft® Outlook.

SonicWALL Network Security restricts unauthorized dissemination of sensitive and proprietary corporate information during workforce turnover.



SonicWALL restricts unauthorized file transmittal by limiting or disallowing FTP privileges to particular users, and blocks transmittal of specific file types prone to containing confidential or proprietary information, such as Word, PowerPoint or Excel files. It can also eliminate file sharing over peer-to-peer applications.

SonicWALL Secure Remote Access

As a component of SonicWALL's Data Turnover Protection, SonicWALL Secure Remote Access (SRA) offers SSL VPN secure remote access to mission-critical resources from virtually any endpoint—including desktops, laptops, PDAs and smartphones, as well as optional remote help desk support to non-IT-managed laptops and PCs.



SonicWALL SRA provides granular access control to protect intellectual property from unauthorized access over remote or mobile devices.

As a component of SonicWALL Data Turnover Protection, SonicWALL SRA delivers automated policy enforcement based on pre-authentication endpoint criteria, such as the detection of a valid client certificate watermark. SRA's policy-based endpoint control can detect and restrict attempted access from unmanaged PC kiosks at office service centers, cafés, airports or hotels. SonicWALL's Secure Desktop function creates a virtual encrypted environment that prevents sensitive information from being left behind. SonicWALL SRA can block suspect e-mail attachments in Outlook Web Access or Lotus iNotes, or block access to financial data or patient records. With a closed-by-default VPN platform, SRA provides "deny all" firewall-style protection.

How Can I Learn More?

Visit the SonicWALL Data Turnover Protection Website.

Click here to opt-in to receive SonicWALL Newsletters.

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to **feedback@sonicwall.com**.

Forward to a Friend

About SonicWALL

SonicWALL[®] is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high-performance business network. For more information, visit the company Web site at **www.sonicwall.com**.