




Trend Micro™ LeakProof™

Trend Micro, Incorporated 

 Leveraging Data Leak Prevention Technology to Secure Corporate Assets

A Trend Micro White Paper | January 2008

Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

➔ TABLE OF CONTENTS

- I. EXECUTIVE SUMMARY: ADDRESSING THE INSIDER THREAT.....3
- II. THE HIGH COST OF DATA LEAKS.....4
- III. CONVENTIONAL DLP SOLUTIONS.....6
- IV. TREND MICRO LEAKPROOF DLP SOLUTION.....7
- V. LEAKPROOF 3.0 FEATURES.....9
- VI. SUMMARY.....11



Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

I. EXECUTIVE SUMMARY: ADDRESSING THE INSIDER THREAT

According to the Ponemon Institute, 78 percent of data breaches come from authorized insiders of an organization. Loss of proprietary information and intellectual property can trigger fines, litigation, brand damage, and bad press. Enterprises have deployed protective measures—such as VPNs, firewalls, and network monitors—to provide audit trails and prevent unauthorized external access to proprietary information. However, these solutions don't address the rising threat from internal users. Because they have access to data assets, insiders are a major channel for information leaks, whether through deliberate policy breaches or accidental data loss (such as losing a mobile device containing personal records).

To protect sensitive data, enterprises need an effective data leak prevention (DLP) solution that monitors potential information leaks at the point of use. However, the explosion of messaging systems, wireless networking, and USB storage devices has made the protection of critical enterprise data difficult. As a result, enterprises are experiencing an increase in the loss or theft of data assets by employees or contractors who accidentally or maliciously leak data.

In today's virtual enterprise, it's rarely practical or cost-effective to search employees for iPods or other USB devices. A more comprehensive, effective system for preventing data leaks is required at every port, on every endpoint in the enterprise, and on any network whether corporate, public, or WAN.

Since most breaches are accidental, companies have an opportunity to better protect enterprise data by educating employees on the proper handling of information. Data leak prevention technology should not only monitor and prevent leaks, but help to educate and raise awareness of employees about companies' policies and procedures for handling sensitive data. Plus, meeting compliance regulations such as SB-1386, GLBA, EU DPD, Sarbanes-Oxley, and HIPAA requires intelligent content filtering solutions that enforce security policies.

ASK YOURSELF THESE QUESTIONS

1. Do you worry about your intellectual property leaking out such as contracts, schematics, source code, or diagrams?
2. How do you prevent your customer or employee information such as IDs, credit cards, account names/numbers from leaking?
3. Have you had a recent breach of sensitive information? How did it leak? Through what channel—e-mail, USB?
4. Have you evaluated any products to protect your data, such as encryption, digital rights management, DLP, email filtering? If so, what, when, where, who, why?
5. Do you have any regulatory compliance initiatives where protection of sensitive information and/or education of employees is critical?

II. THE HIGH COST OF DATA LEAKS

Never before has the threat to corporate data assets been so great—and so costly. According to Attrition.org, an industry monitoring organization, in calendar year 2007, more than 162 million records such as credit cards and Social Security numbers were compromised through December 21—both in the U.S. and overseas. By contrast, Attrition.org reported that 49 million records had been compromised in the previous year. Additionally, the Identity Theft Resource Center lists more than 79 million records compromised in the U.S. through December 18, 2007. That's nearly a fourfold increase from the 20 million records reported as compromised in 2006¹.

The average amount lost in each case of identity theft in the U.S. is more than \$31,000², counting losses to companies as well as individuals³. Moreover, every year U.S. companies suffer billions of dollars in intellectual property losses when software, product designs, games, drug formulations, business plans, and other trade secrets are illegally copied. Beyond the sizable loss of profits, data leaks can also lead to bad publicity, public distrust, damage to brand image, and weaker competitive positions. The following are three recent examples of typical data thefts:

⊕ **Boeing Breach**

"Police reported [of a Boeing employee stealing data] finding a thumb drive that was connected to his computer terminal via a USB cord that ran along the back of the terminal to the storage device that was 'hidden in a drawer' in his desk."⁴ Clearly, with the proliferation of removable storage devices and mobile systems, it is becoming more difficult to prevent the leak of sensitive data.

⊕ **Fidelity NIS Theft**

"To avoid detection, [an administrator committing data theft] appears to have downloaded the data to a storage device rather than transmit it electronically."⁵ This theft, at Certegy Check Services, a subsidiary of Fidelity National Information Services, illustrates how employees are becoming increasingly sophisticated in their attempts to steal data. In this case, the administrator assumed that the company had email and network filtering solutions in place, and sought other means to get data out.

CUSTOMER PAIN POINTS

Executive Concerns

Prevent bad publicity and lawsuits from data breaches or accidental or intentional leakage of sensitive customer, patient, or employee information.

Business Concerns

- Safeguard customer, patient, and employee data by preventing leaks that can be used for identity theft and other criminal abuses
- Prevent financial losses and expenses for remediating breaches
- Protect competitive position by preventing the compromise of intellectual property
- Preserve good brand name/image

IT Concerns

- Provide effective IT controls to keep data from leaving an organization's network either by accident or intentionally due to direct criminal behavior
- Reinforce IT security and risk management policies through awareness and education

1 "Groups: Record Data Breaches in 2007," by Mark Jewell, AP, <http://attrition.org/news/content/08-01-03.001.html>

2 "Identity Fraud Trends & Patterns," October 2007, Center for Identity Management and Information Protection (CIMIP) at Utica College, NY, <http://www.utica.edu/academic/institutes/cimip/publications/index.cfm>

3 "Identity Theft: Costs More, Tech Less," Information Week, Oct. 22, 2007, <http://www.informationweek.com/news/showArticle.jhtml?articleID=202600312>

4 Information Week, 7/11/07

5 CSO Magazine, 7/03/07

Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

⊕ UK Government Breach

CDs containing the confidential personal details of 25 million child benefit recipients have been lost by HM Revenue & Customs (HMRC). The records contain the names, addresses, dates of birth and National Insurance numbers of the entire HMRC child benefit database, which also includes the bank account details of more than seven million parents, guardians and care givers.⁶

As internal security threats abound, current market research data shows the extent of this very serious problem.

- ⊕ Based on PricewaterhouseCoopers's "Trends in Proprietary Information Loss" report, the Fortune 1,000 corporations and 600 other companies experienced proprietary information and intellectual property (IP) losses of between \$53 and \$59 billion in one year alone. Other studies have put the cost of IP losses and identity theft at \$85 billion annually in the U.S.
- ⊕ According to the Computer Security Institute's latest annual survey of cyber-crime and security, published in September 2007⁷, the average cost to companies from computer crime is \$345,000 per respondent, up from \$167,700 in 2006, for a total of nearly \$67 million. Of this amount, confidential data theft and insider abuse totaled \$13.6 million, the second-largest share after financial fraud (\$21 million). This outranked the losses caused by viruses, worms, and spyware (\$8.4 million) and system penetration by outsiders (only \$6.9 million). About a quarter of the companies surveyed said the majority of their losses were due to insiders.

According to industry analyst Enterprise Strategy Group in a June 2007 survey:

- Nearly one-third of organizations have experienced a data breach within the last 12 months. More alarming still, another 10 percent of the security professionals surveyed responded that they "don't know" if they've experienced a data breach in the last 12 months.
- More than 40 percent of users say that data breaches cause business ramifications such as lost data, application downtime, and dissatisfied customers. Alarmingly, 30 percent of survey respondents say that their organizations' data breaches resulted in a "direct loss of revenue."

If these risks aren't enough to motivate businesses to strengthen their data protection measures, the government is adding pressure. There are now extensive legal requirements to protect customers' data and make business processes auditable, with precautions against intrusion and fraud. The U.S. federal Sarbanes-Oxley and Gramm-Leach-Bliley Acts, California's pace-setting Security Breach Information Act (SB-1386), HIPAA, the European Union's Data Protection Directive, and other regulations pose stringent requirements regarding confidential and customer information, and create added burdens for network security managers.

Most existing security solutions focus on securing the perimeter of the organization. By doing so, they reduce the risk from eavesdropping and hacking initiated from outside, but do almost nothing to prevent breaches from internal sources or the accidental leaking of information. Employees, partners, consultants and contractors with access to a secure network have several mechanisms with which to obtain key

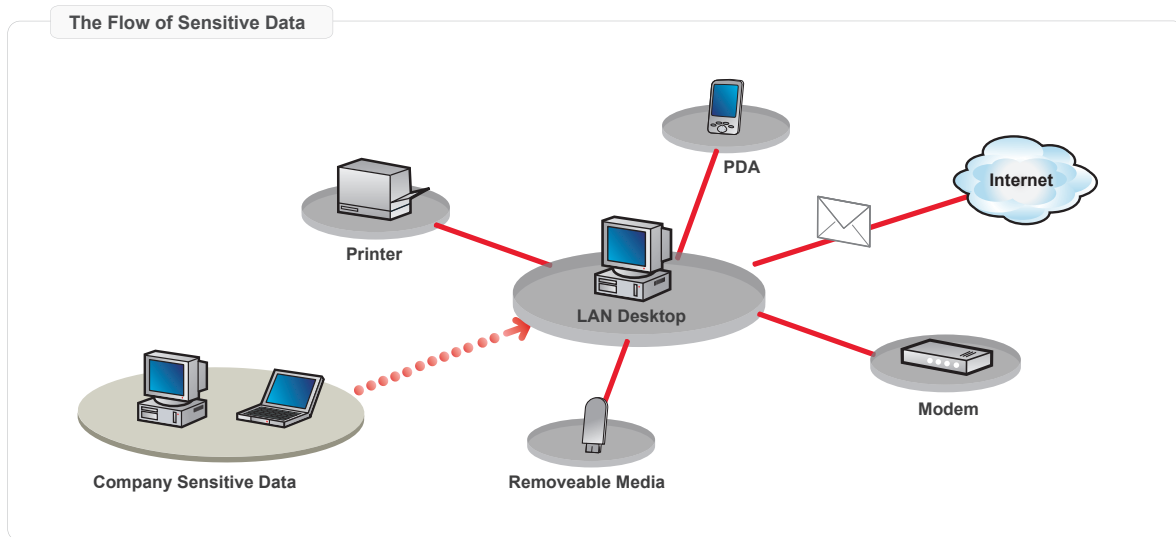
⁶ ComputerworldUK, 11/20/07

⁷ "2007 CSI Computer Crime and Security Survey," Robert Richardson, CSI Director, September 2007.
<http://www.gocsi.com/press/20070913.jhtml>

Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

information and documents and proliferate that information outside the secured enterprise. Whether they use email, ftp, IM, IrDA, WiFi, USB-disks, digital cameras, phones, recordable CD/DVDs, or simply print information, there are too many unsecured network exits creating opportunities for the accidental loss or intentional leaking of data.

The most effective solution requires closing and securing all network exit points, as shown in the diagram below.



III. CONVENTIONAL DLP SOLUTIONS

Security vendors have created a number of products to solve pieces of the information theft and data leak problem. Firewalls, VPNs, network traffic monitors, email content filtering systems, and security agents have been deployed in the enterprise. Unfortunately, they're only part of the solution.

While each of these solutions serves a vital purpose when securing the network against external threats, they do little to:

⊕ **Intelligently scan and filter content.**

Most of the solutions use simple keywords or other rules to detect confidential information, and these rules can be easily manipulated and defeated by a motivated user.

⊕ **Protect every network exit point.**

Most of the systems use network-based approaches that cannot lock down every port on every PC—making it easy for a motivated insider to circumvent the protective measure in place.

⊕ **Prevent the breach in real time.**

Most systems only monitor and audit user behavior, resulting in a passive solution that enables a security administrator to discover breaches only after the information leak has occurred.

KEY POINTS

LeakProof addresses the primary concern for most customers with data leak prevention at the endpoint:

- Does not impact employee productivity or system performance
- Easy to install with minimal tuning needed
- Full compatibility with single and double-byte languages
- Sold in all major regions where Trend Micro operates

Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

⊕ **Protect laptops and other disconnected endpoints.**

Most solutions are only fully effective for devices that are connected to the corporate network, rendering a laptop at Starbucks or a stolen laptop a huge and uncontrolled liability.

IV. TREND MICRO LEAKPROOF DLP SOLUTION

Trend Micro LeakProof™ 3.0 protects customer and employee privacy, and intellectual property. LeakProof turns employees into security assets instead of liabilities, providing the broadest protection of any endpoint client including USB ports, CD/DVD burners, Bluetooth devices, desktop computers, offline laptops, Webmail, encrypted Webmail, IM, FTP, and HTTPS—whether on or offline—including:

- Mobile, branch, and corporate offices
- Online and offline endpoints
- Corporate networks
- Public networks
- WiFi and email

Trend Micro LeakProof enables companies to reduce the risk of data breaches and ensure privacy and compliance. The DLP solution “understands” the unique DNA of each data document and monitors and protects data at rest, in use, and in motion. LeakProof prevents enterprise data leaks with a unique approach that combines endpoint-based enforcement with highly accurate fingerprinting and content matching technology.

LeakProof provides the broadest coverage available for the network perimeter and endpoints. Built-in filtering modules inspect content before it is encrypted to protect activity through Web browser and email applications. IT managers can disable specific devices easily.

Through continuous monitoring, LeakProof provides corporate security and compliance officers with a radar-like capability to locate sensitive information and decrease the risk of data breaches. LeakProof discovers unauthorized information residing at endpoints, including laptops, desktops, and servers.

Interactive “alerts” enable IT managers to define content-sensitive dialog boxes that appear directly on an employee’s computer screen. These dialog boxes contain custom URL links that educate employees on the appropriate handling of confidential information. Unauthorized transfers are blocked, or employees can be required to use the built-in data encryption module to copy data onto USB devices.

LEAKPROOF DATA LEAK PREVENTION ADVANTAGE

Protect Privacy

Monitor and prevent improper use of customer and employee information

Protect Intellectual Property

Discover, classify, and protect critical company assets

Comply with Privacy Regulations

Monitor usage, scan endpoints, and educate employees to reduce risk

Educate Employees

Customize interactive dialogs for employee education and workflows

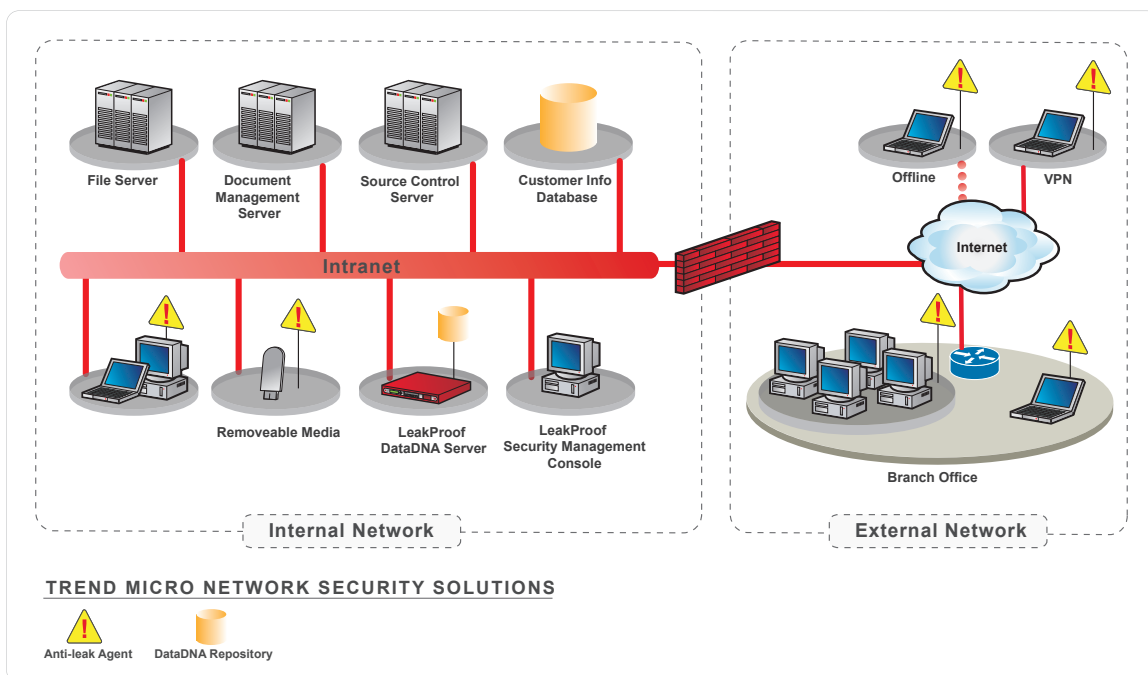
Discover Sensitive Data

Find sensitive data on laptops, desktops, and servers

Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

A software client and an appliance comprise the complete LeakProof solution:

- ⊕ **LeakProof DataDNA™ Server**—is an appliance that provides a central point for visibility, policy configuration, and fingerprint extraction from content sources. A Web-based interface supports an administrative workflow for discovery, classification, policy setting, monitoring, and reporting. Patent-pending technology detects sensitive data with the highest levels of accuracy and performance. Powerful algorithms extract information from content to create a unique DNA sequence or “fingerprint” for each document. This “fingerprint” enables endpoint-based enforcement online or offline.
- ⊕ **LeakProof Anti-Leak Client**—includes non-intrusive, powerful monitoring and enforcement software that detects and prevents data leaks at each endpoint. The client communicates with the DataDNA Server to receive policy and fingerprint updates and report violations to the server. A client-based device driver installed on the endpoints to monitor network traffic, I/O, and application activities performed at the endpoints, the Anti-Leak Agent locks down physical and virtual devices, which prevents the unauthorized copying or movement of sensitive data. Multiple matching engines provide real-time filtering using fingerprinting, regular expressions, keywords, and metadata. By employing Trend Micro’s patent-pending DataDNA technology, the Anti-Leak Agent can monitor application behavior and also prevent information leaks by encrypting sensitive information before it leaves the premises.



V. LEAKPROOF 3.0 FEATURES

LeakProof provides the following key features to help organizations protect valuable information and intellectual property:

⊕ Sensitive Information Matching

LeakProof identifies sensitive information and prevents data breaches using fingerprints, regular expressions, keywords, and metadata matching. Analysis of structured and unstructured data supports partial matching of text files and exact matching of binary files. Language independent, LeakProof produces results without geographical boundaries, perfect for multinational deployments.

⊕ Granular Security Policies

Using logging, server-side alerts, client-side alerts, blocking, encryption, justification, and education, you can set your company's security policies to align with your data protection policies. You can establish separate policies for online and offline violations, individual endpoint or group-based, and trusted/not trusted email domains.

⊕ Endpoint Topology and Sensitive Data Discovery

Discover, monitor, and manage endpoints with enterprise endpoint computer discovery, scanning for sensitive information, real-time map display of endpoint status, centralized client status monitoring and management, and discovery of unauthorized I/O devices at endpoints.

⊕ Device and Application Control

LeakProof performs control of all I/O devices: USB, CD/DVD, floppy, Bluetooth, IrDA, imaging devices, COM and LPT ports, and PrintScreen (PrtSc) function blocking.

⊕ Violation Monitoring and Reporting

Executive and operational visibility into violations with real-time dashboard and security violation reports summarized by endpoints and users. Also provides trend analysis and violation channel breakdown, scheduled and on-demand reports of security violations. Optional forensic capture feature logs the actual file violation on the DataDNA server for later inspection.

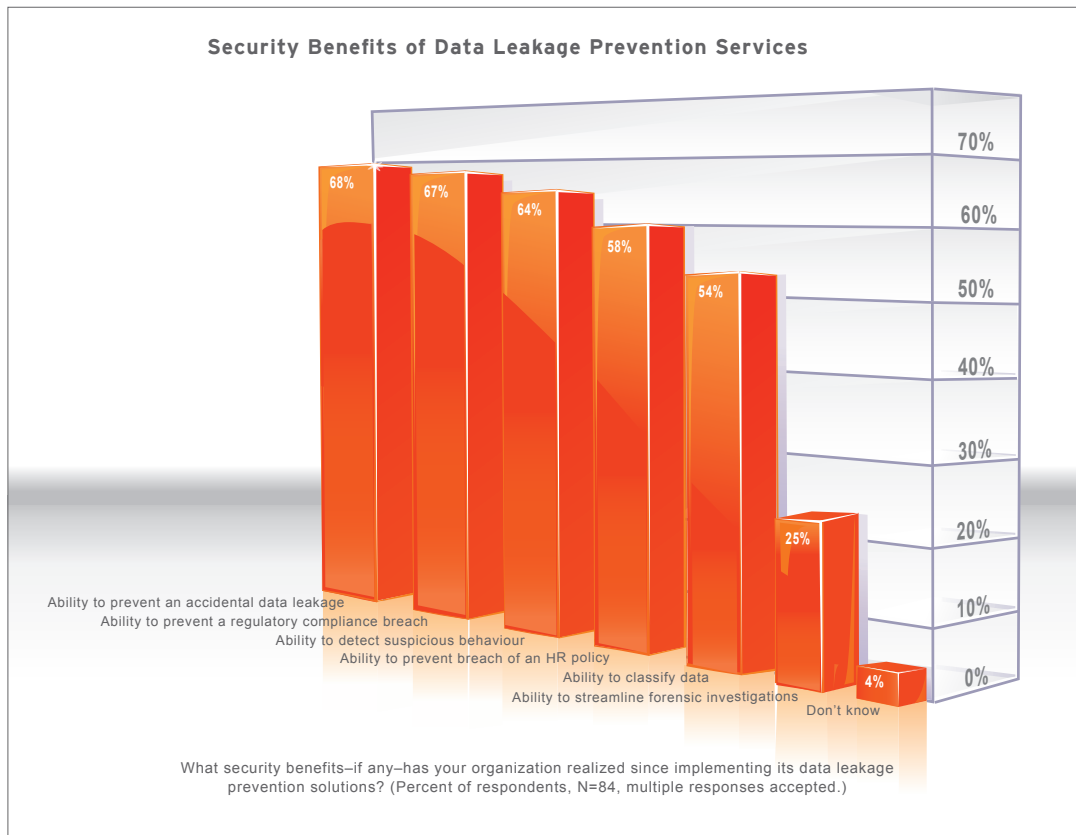
⊕ Compliance Templates

Comply with regulations with preconfigured classifications and policies supporting regulatory compliance such as PCI, GLBA, SB-1386, and SOX, with built-in rules and validation modules for entities such as Social Security, credit card, ABA routing, Canadian and Chinese National ID, American name recognition, and others.

Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

⊕ System Administration and Scalability

Enhance administrator productivity with a Web browser management interface, role-based administration and access controls to sensitive content. Integration with LDAP and Active Directory, management server clustering for enterprise scalability, and secure communication between endpoint and server via SSL.



Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets

VI. SUMMARY

Trend Micro LeakProof extends the broadest protection available at the endpoint for data at rest, in use, and in motion. It also helps educate employees on how to prevent data leaks with interactive alerts. Existing network security and intrusion detection products only solve part of the information theft and data leak problem. However, when deploying LeakProof, Trend Micro's comprehensive DLP solution, enterprises greatly improve the protection of sensitive business information on the desktop and on mobile devices. Trend Micro's patent-pending technologies enable the system to rapidly classify and filter information, accurately detecting sensitive content in files of various types. This real-time, proactive approach not only provides the monitoring capabilities that today's computing environments require, but also the capability to prevent information leaks from occurring at all. The protection continues even when the PC or laptop is disconnected.

LeakProof monitors every port on every PC, using unique pattern-matching technology that allows only authorized information to be copied or transmitted. The LeakProof security solution represents the state of the art in DLP, providing maximum protection for an enterprise's critical information.

By educating employees and safeguarding both the network perimeter and internal endpoints, LeakProof also helps employees become security assets by preventing data leaks, reducing accidental breaches, and enlisting the help of all employees to maintain a high degree of vigilance for the protection of company-sensitive data.

About Trend Micro Incorporated

Trend Micro, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. A transnational company, with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO™

Trend Micro, the Trend Micro t-ball logo, DataDNA, and LeakProof are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. [WP01_LeakProof_080123US]

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651

phone: 1 +408.257.1500

fax: 1 +408.257.2003

www.trendmicro.com

