TrustWatch™

Enterprise USB-Flash Drive Management

Corporations, financial services companies, and government agencies fear information leakage through network endpoints, such as desktop and laptop PCs. The recent proliferation of USB flash drives approaching 8 gigabytes and MP3 players with hard drives bigger than many laptop PCs has made it easier for uncooperative users and malicious parties to copy vast quantities of private information in just a few moments. Much like the floppy drives in early PCs, USB flash drives offer significant advantages, such as the convenience of file portability and improved productivity. However, fear of information leakage is forcing some executives to order that all USB ports be filled with epoxy cement to disable them. But to stay competitive, enterprises need to allow the use of USB flash drives and the remote access that they enable to their key information resources, even from uncontrolled computers.

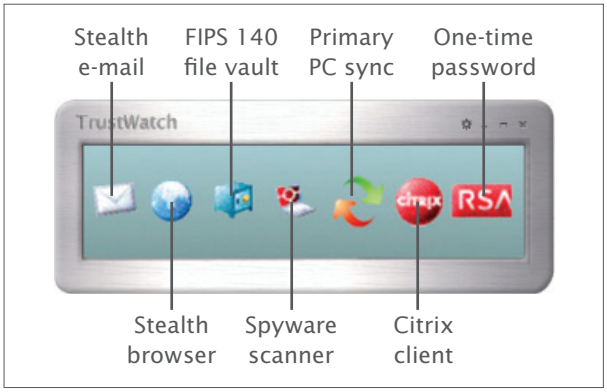

Figure 1. SanDisk TrustWatch Suite transforms any SanDisk USB flash drive into a trusted device for mobile storage or remote access.

SanDisk, the leading supplier of flash memory storage devices, offers TrustWatch™, an integrated solution that prevents information leakage while facilitating remote access to corporate applications and information resources. This solution offers significant advantages, such as the convenience of browser-based access, improved productivity, and high-capacity storage in an enterprise issued and managed pocket-size device.

SanDisk TrustWatch

As storage capacities grow to multiple gigabytes, it is imperative that companies gain control of USB storage devices that are able to copy entire databases or the contents of multiple PCs. Most IT organizations do nothing to manage USB devices, and those that do take a shotgun approach rather than implementing granular control. Security-conscious companies attempt to manage mobile devices while within the sphere of their network, but lose control as soon as the devices leave the company premises. The SanDisk® TrustWatch suite not only manages end-user devices, but also provides a complete record of all device activity.

The TrustWatch solution combines the power of instant endpoint security and mobile encryption with an enterprise-grade management system through an integrated suite of components that run on servers within the data center, on enterprise PCs, and on SanDisk USB flash drives.

The TrustWatch suite delivers a policy-driven environment for complete USB device life-cycle management, from provisioning to password reset to remote data destruction. TrustWatch Suite extends security policy beyond the network perimeter. An ultra-thin client running on a USB flash drive instantly secures and sanitizes any PC, anywhere. The TrustWatch suite extends security policies beyond the network perimeter, allowing policy enforcement to travel with the user. The suite supports access and authentication from

SanDisk®

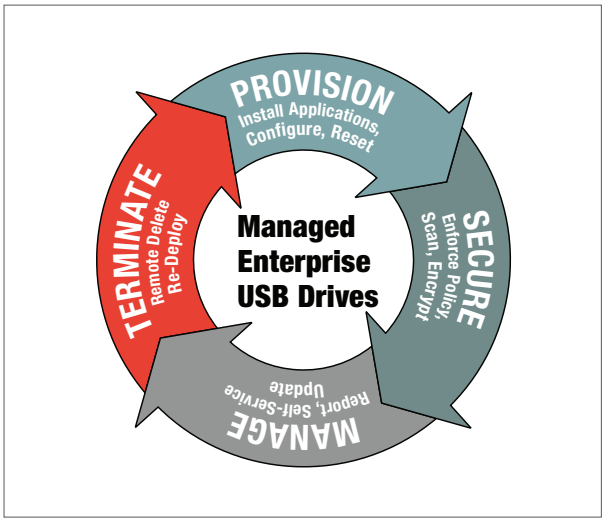

Figure 2. The TrustWatch suite offers complete lifecycle management for USB flash storage devices

strategic partners, including Citrix®, OATH® (Open Authentication), and RSA®, in addition to implementing best practices for document storage and encryption. The TrustWatch suite enables secure remote access to enterprise applications, while leaving no trace of user activity on the host PC.

Business users demand convenience, zero downtime, and instant restoration whether they are accessing their own files at home or remotely accessing corporate applications from the road. Growing user demands for new devices puts increased pressure on already overtaxed IT departments. The TrustWatch suite was designed to get end users set up quickly, easily, and reduce time spent administering users and devices.

The TrustWatch suite secures mobile files and identity data even if the device is lost or stolen. If the device is subject to physical attack, policy-driven management enables IT to remotely disable the device or destroy the information on it at the press of a button. TrustWatch significantly reduces the risk of data leakage from mobile devices especially when TrustWatch devices are issued as the corporate standard USB flash drive.

The TrustWatch components—TrustWatch Access, TrustWatch Vault, TrustWatch's support for endpoint port protection and TrustWatch Manager—are described in the following sections.

TrustWatch Access

Although most IT organizations work diligently to protect access to their networks, the common network defenses, such as anti-virus software, firewalls, and anti-spyware can only protect users operating within the sphere of their control. The weakest link in remote access has always been the endpoint. Until TrustWatch Access, there was nothing an IT organization could do to manage access from uncontrolled computers.

Provides Trusted Remote Access

SanDisk TrustWatch Access is the premier solution that combines the power of instant endpoint security, centralized monitoring and reporting, and enterprise access software on a highly secure personal mobile device. TrustWatch Access integrates a spyware scanner, stealth browser, portable RSA SecurID™ token, Citrix nFusion™ client, stealth email, and a secure data vault with push functionality. These integrated security applications work together to transform instantly an untrusted workstation into a trusted platform from which users can remotely access their enterprise applications.

Lowers IT Expenditures

The seamless integration of Citrix, one-time password, and web clients within a protected USB device

TrustWatch Suite

- Stores multiple authentication tokens on one device
- Reduces mobile storage data leakage risk
- Demonstrates regulatory compliance
- Distributes media automatically for business-critical content
- Provides trusted remote access to enterprise applications
- Extends strong authentication
- Retains usage and access
- Controls data leakage from Internet cafes and kiosks
- Minimizes the risk of malware from untrusted PCs damaging the enterprise network

TrustWatch Access Features

- Launches automatically
- Requires no software installation on the host PC
- Supports policy-based controls
- Leaves no trace of user's information on a PC host
- Integrates file and email synchronization and Citrix, RSA SecurID, and email clients.
- Provides on-demand VPN access

makes TrustWatch Access the ideal remote access solution, eliminating the need to travel with a laptop and even eliminating the need to deploy a laptop. This capability gives enterprises an economical means of providing secure remote access to anyone at anytime on any USB-enabled Windows workstation anywhere in the world.

Improves Mobility and Productivity

With TrustWatch Access, remote users never have to install software or drivers to access enterprise resources because dual-factor authentication, VPN software, and other clients are always in their pocket on a convenient and secure personal security device. TrustWatch Access protects the enterprise network from security threats, allowing most USB-enabled computers to host safe remote access.

Assures User Identity Through Standards-Based Authentication

TrustWatch Access integrates one-time password technology from RSA and OATH (Open AuTHentication) to provide two-factor authentication. It can even be used to safeguard digital certificates for Public Key Infrastructure (PKI)–based authentication.

Supports User Self-Service

When employees are ready to provision their TrustWatch device, they follow the instructions and web page link sent to them in a private email. The software is installed and configured on the device, policies are downloaded, and the user creates a device password that meets the company's security policy. User self-service extends to password management and reset, which eliminates the single largest cause of Help Desk calls.

TrustWatch Vault

TrustWatch Vault combines the power of U.S. government–certified software encryption and centralized management on a highly mobile personal storage device. It ensures that privacy is maintained by automatically encrypting all files and enabling lockout or erasure if the device is lost or stolen. TrustWatch Vault automatically encrypts and compresses all files on the mobile storage device. Users simply drag-and-drop files into the secure vault. TrustWatch Vault provides standards-based, military grade software encryption and storage, certified to meet FIPS 140-2 compliance for software encryption.

Protects Information

TrustWatch Vault provides the convenience of mobile storage while controlling and ensuring confidentiality of sensitive information. If the device is lost or stolen, the data can be deleted remotely, or the user can be locked out temporarily or permanently.

Eases Regulatory Compliance

All files in the TrustWatch Vault are automatically encrypted, and the log of all files moved to or from the device demonstrates that sensitive information was adequately protected as set forth in HIPPA, SOX, and other compliance regulations. Furthermore, this unique functionality alleviates the need to disclose lost or stolen devices because companies can prove that private data was never exposed.

Port Protection

Experience shows that management controls over installed executables and removable storage devices on laptops, desktops and servers are effective in reducing exposures to threats, such as root kits, spyware, malicious code and information loss. Information security officers cannot control what the next worm looks like, but they can control the computer's operating policy. TrustWatch works with multiple port protection solutions which can be tailored to your enterprise's requirements. Port control ensures that only approved devices are allowed to connect to your corporate endpoints, controls what those approved devices are allowed to do, and keeps centralized logs of all actions.

Port protection blocks all ports and opens a secure tunnel for approved devices only. It detects and allows restriction of devices by device type, model, or even specific device serial number. For storage devices, port protection allows security administrators to either block all storage devices completely or permit read-only access. Wi-Fi controls are based on MAC address, SSID, or network security level.

Port protection solutions work in concert with TrustWatch Access to ensure that corporate data can be accessed only by company-provided (or approved), fully encrypted USB flash drives, without the fear of data leakage or theft.

Eases Regulatory Compliance

Organizations now can be assured that only those devices provided to employees will work on the employee's specific PC. Any attempt to connect the USB drive to other PCs in the company, or to connect other devices to that same PC, will be blocked unless specifically approved by the company. When combining this capability with TrustWatch Access USB flash drives, the solution is complete. While employees continue to enjoy mobility and portability, organizations can reap the benefits without comprising regulatory compliance.

Supports Granular Controls

The granular management present in port protection solutions grants access to devices based on the unique User IDs (UIDs) or the unique serial numbers of the device. Administrators can grant access to individual devices based on their UIDs. Thus, an organization can create a "whitelist" of all the secure drives allotted to specific employees, granting unrestricted access of corporate data to authorized users on authorized machines only. In the event of theft or loss of the drive, it can be erased from the whitelist, thus preventing future access to the network. With its secure encryption, the data on the drive remains safe and inaccessible to any malicious user.

Creates Activity Logs

All port protection solutions create forensic logs of all data moving in and out of the organization, allowing administrators to create policies that don't necessarily restrict device usage, but allow full visibility device activity and content traffic.

Through a built-in and flexible management console, port protection enables administrators to create comprehensive and granular endpoint security policies. Policies are exported directly to the Active Directory as Group Policy Objects (GPOs), ready to be assigned to relevant Organizational Units (OUs) and silently installed on clients.

With built-in alerting capability, administrators can get immediate notifications of any activity that needs immediate response. Alerts are available via email, SNMP, Syslog, Windows Event Viewer, pop-up messages, and even custom scripts.

Port Protection Features

- Logs data written to devices (shadowing)
- Supports and manages context-sensitive permissions for each device
- Controls Wi-Fi network access
- Blocks PS2 ports
- Manages other writable devices, such as CD-RW and DVD-R
- Authorizes media

TrustWatch Manager

Centralizes Deployment and Management

TrustWatch Manager enables enterprises to deploy, administer, and audit thousands of TrustWatch devices from a centralized management console whether connected directly to the enterprise network, or anywhere on the Internet. Any number of TrustWatch devices can be deployed, updated, tracked, disabled, locked out, and contents destroyed remotely. Further, TrustWatch Manager tracks and logs all file activity, establishing a clear forensic trail. Flexible reporting helps understand and analyze mobile storage usage.

Enforces Policy-Based Controls

TrustWatch Manager's foundation is a policy-based engine that matches the functionality and attributes of each TrustWatch device to the user's role or individual requirements. This policy enforcement protects enterprise networks from malware, including key loggers and trojans, by prohibiting

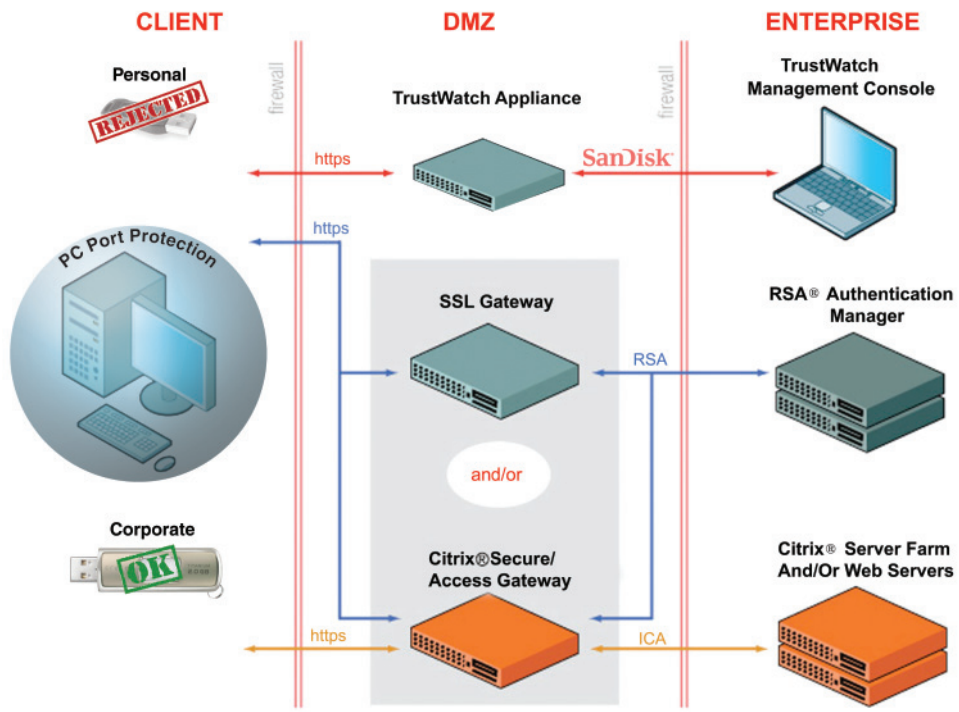

Figure 3. TrustWatch Manager seamlessly integrates with your existing infrastructure to centralize control of USB flash drives.

TrustWatch Manager Features

- Secures content on USB flash drives
- Manages device life-cycle
- Deletes confidential information from the device if it is lost or stolen
- Improves productivity with user self-help

contaminated PCs from accessing the corporate network. The policy-based engine includes control of the following:

- Centralized logging and reporting
- Mobile storage
- Change management
- Activation and deactivation
- Self-destruction and lockout
- Password policy and recovery
- Reporting

Secures Application and Document Updates

TrustWatch Manager securely pushes content and applications to managed devices. This means no more running obsolete versions of software or using outdated documents, such as price lists and customer information. TrustWatch Manager can automatically deliver updates to some or all devices through any Internet-connected PC.

Demonstrates Regulatory Compliance

Using the logs maintained by TrustWatch Access and TrustWatch Vault, TrustWatch Manager keeps a complete history of all USB device activity, even when the devices are offline or connected to untrusted PCs. Managers are able to define the level of tracking on a role or device basis, which is kept in an online log. The same technology that ensures that TrustWatch devices have the latest anti-spyware also is used to constantly update the TrustWatch Manager with the latest logs from each device.

Eases Implementation

The TrustWatch Manager arrives already installed on a turnkey appliance and is ready to transform any SanDisk USB flash drive into a trusted, managed device, thus allowing companies to reduce capital expenditures by taking advantage of promotional retail pricing. The appliance typically can be deployed in less than an hour. Simply connect the TrustWatch appliance to your network's Demilitarized Zone (DMZ) LAN and configure the network connection. After optional linkage to your Microsoft® Active Directory, RSA authentication server or OATH-compliant authentication server, and Citrix remote access server, you are ready to deploy security policies to company-approved devices.

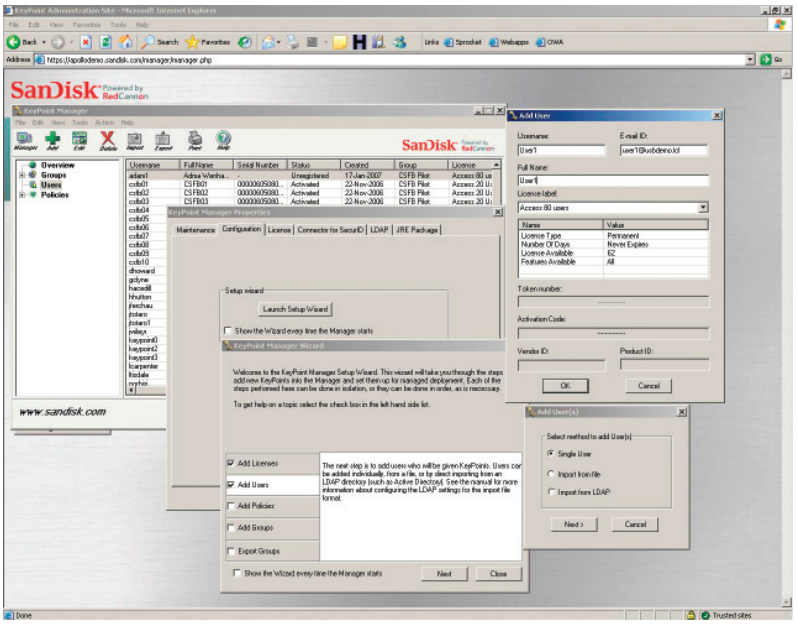

Figure 4. TrustWatch Manager enables full life-cycle management for USB flash drives.

Specifications

TrustWatch Access
Host PC Requirements
Windows 2000 or Windows XP
(Home Edition or Professional)
Intel Pentium II or later processor
Open USB port 1.1 or later
Internet Explorer 5.01

Server Requirements
Windows 2000 or Windows XP Professional
Intel Pentium II or later processor
Network access

Optional Server Requirements
Citrix ICSA-certified server
RSA SecurID server
Microsoft Active Directory Server

TrustWatch USB Flash Drives
1–8 GB of secure storage
32-bit cryptographic co-processor
AES 256-bit software encryption
FIPS 140-2 certified file vault

Disclaimer: Security safeguards, by their nature, are capable of circumvention. SanDisk cannot, and does not, guarantee that data will not be accessed by unauthorized persons, and SanDisk disclaims any warranties to that effect to the fullest extent permitted by law.

For more product information, including pricing and distributors, email TrustWatch@sandisk.com

USA
Tel: +1-408-470-4440
Fax: +1-408-470-4470
OEMinfo@sandisk.com

Japan
Tel: +81-3-5423-8101
Fax: +81-3-5423-8102
OEMJapan@sandisk.com

Taiwan
Tel: +886-2-2515-2522
Fax: +886-2-2515-2295
OEMAsia@sandisk.com

China
Tel: :+86-755-8348-5218
Fax: +86-755-8348-5418
OEMChina@sandisk.com

Korea
Tel: :+82-2-3452-9079
Fax: +82-2-3452-9145

Europe
Tel: +33-(1)-43-37-2131
Fax: +33-(1)-43-37-2111
OEMEurope@sandisk.com

Rest of the World & Israel
Tel: +972-9-764-5000
Fax: +972-3-548-8666

For more information, please visit www.sandisk.com/trustwatch

SanDisk®