



Achieving Basel Compliance with Safend Protector

www.safend.com

TABLE OF CONTENTS

Introduction 1

New technologies and business practices 1

- Laptop computers 2
- Removable storage 2
- Wireless Networks 2

Using Safend Protector to plug the gaps 2

Conclusions 7

Introduction

In the banking profession, management of risk is the name of the game. Risks to bank assets can come from a variety of sources such as credit risk (loss due to non-payment), and market risk (loss due to market investments). But operational risk is an area that is the latest to earn increased attention. Operational risk is defined by the Basel Committee as "...the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events".¹

Attention from bank executives and risk managers for this type of risk is not new. What is new is a formalized approach to addressing, mitigating, and reporting operational risk.

"...management of specific operational risks is not a new practice: it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk in principle, if not always in form. The (industry) trends combined with the growing number of high-profile operational loss events worldwide, have led banks and supervisors to increasingly view operational risk management as an inclusive discipline..."²

Recognizing the importance of operational risk, the Basel Committee on Banking Supervision will require banks to set aside regulatory capital for operational risk in 2007. Therefore, all those in the financial service industry must explicitly and formally manage operational risk - meaning they must identify, assess, monitor, and control risks from inadequate system controls.

Herein lies the challenge: Traditional approaches to managing system risk (a component of operational risk) focus on old technologies and threats. Organizations and companies need new approaches and controls to properly address and manage system risk, approaches based on new technologies such as mobile devices and new threats such as wireless access.

New technologies and business practices

A well-defined physical perimeter is the principal requirement for a traditional approach to securing electronic information. An organization first defines a security perimeter and then positions all systems inside to guarantee restricted access. An access device, usually a firewall, controls the access across the perimeter for every system. This strategy assumes that the perimeter prevents all other information transfers and a bastion firewall provides the only access.

¹Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, Bank for International Settlements, February 2003.

²Ibid.

This model worked very well, but only in the world of wired networks and limited storage devices. In that world, workstations were tethered by their network connection, so they could not be transported easily. The physical limitations of the equipment enforced access control. Furthermore, most of these workstations did not contain removable storage and were further physically constrained. The corporate firewall represented the only way to transfer data between these endpoints. The main concerns of security professionals were to ensure the firewall was well-maintained and attacks from the outside were contained.

But now several new technologies have emerged to change this landscape. Newer corporate IT environments make it very difficult to base security on a single access point.

Laptop computers

More and more, the convenience of laptops outweighs the cost differential of desktops. What's more, laptops come with an additional advantage: They can be used in many locations outside the office. In many instances they are now the preferred platform, no longer reserved for executives and road warriors. Laptops represent a new access point which must be secured.

Removable storage

Although the removable trend began with floppies, those storage devices did not present major issues, because the floppy disk format limits the amount of data that can be stored. Then storage amounts increased, first with writeable CDs and other removable media. But removable storage was still limited by cost and complexity of the devices. Within the last two years, however, the cost of removable storage has dropped dramatically as the devices have become easier to use. A 1 GB "thumb drive" of USB memory is not only cheap, but it automatically installs as a drive in most operating systems. Plus, other sources of removable media such as MP3 players connect easily to store data.

Wireless Networks

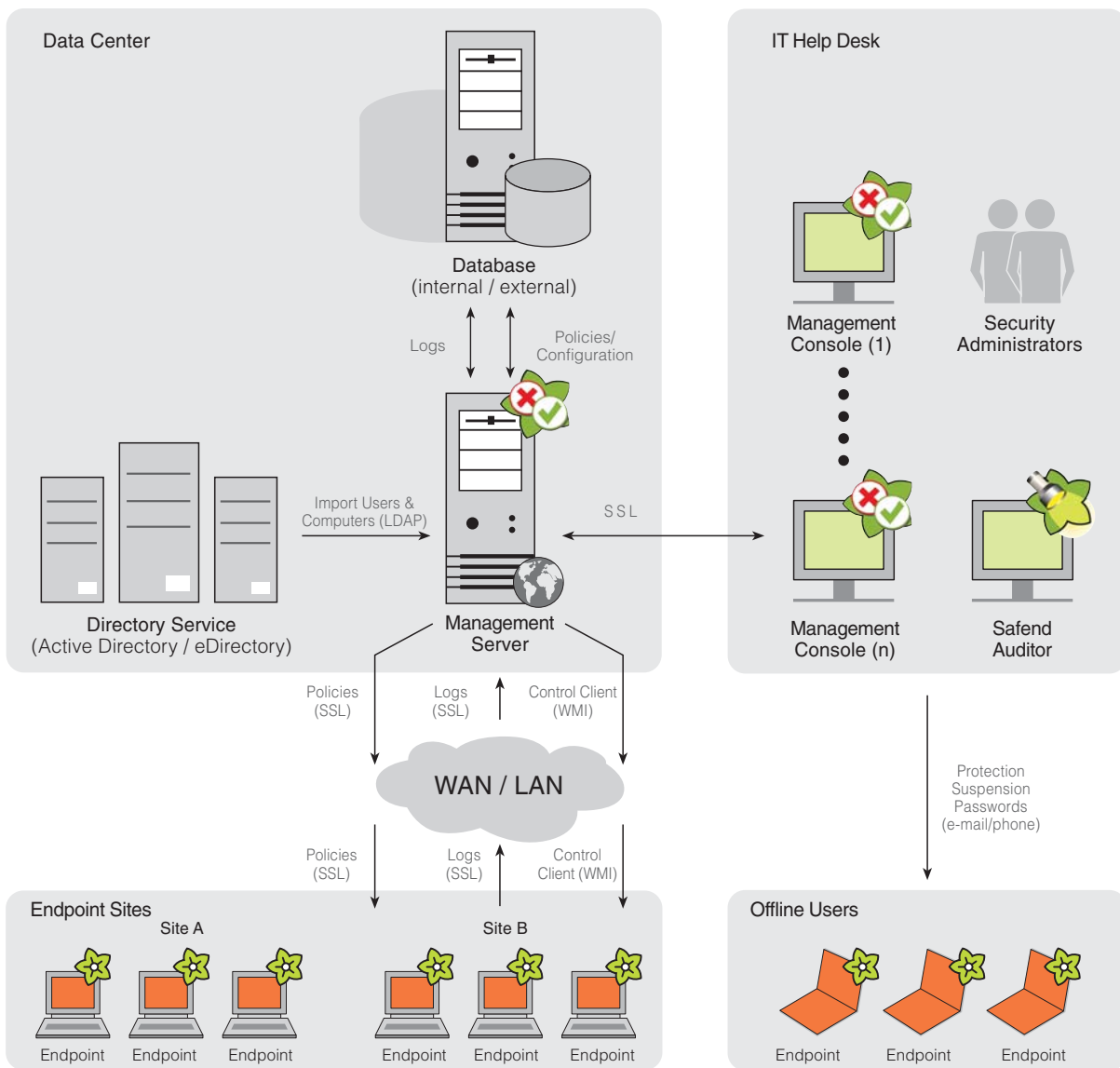
The standard access model was based on defined network connectivity, realized in physical connections. Cables connected users to central resources in a local area network. Today, wireless networks are not only inexpensive, they are very easy to get up and running. In many cases, laptop PCs come with wireless capability as a standard feature. The laptop operating systems use built-in hardware to automatically seek out and connect to wireless networks. Unfortunately, the standard wireless configurations deliver ease of use, but not automatic security.

Wireless networks permit information to be transferred outside the physical constraints of a wired network. All of these new technologies create virtual breaches inside the traditional security architecture. Information can now flow to and from the corporate environment without protection or security.

Using Safend Protector to plug the gaps

Safend provides a comprehensive set of access control products that is specifically designed to address these new challenges. These products deliver a high degree of control over the access mechanisms at the endpoint, i.e. they can prevent unauthorized information transfer or “data leakage.” The products have key capabilities to address this issue specifically - capabilities that address operational risk aid in meeting the Basel II Accord.

The overall system helps manage information flow at the endpoint. It integrates into existing corporate architectures and ensures that virtual security breaches are contained. The Safend solution breaks down into four parts as shown in the diagram below.



The first step in any security planning exercise is to evaluate the existing vulnerabilities within the network. The Safend Auditor allows the system administrator to collect information from each endpoint and deliver a comprehensive list of which devices, ports and connections are available for use. From this data, a specialized plan can be developed to allow access control for users.

Aligning access control with the type of data the end user has available is the next step. Typically, an organization already defines classes of users, which are implemented for standard internal network access. Using the Safend Management Server, these existing policies can be extended to cover endpoint access channels. This effectively allows the data access control to be extended beyond the physical perimeter served by the wired network. Furthermore, organizations must assume responsibility for security of the critical and sensitive data leaving and entering the corporate environment, no matter what the physical location. As more mobile storage solutions become available, this is turning into a major nightmare for many organizations.

Once a set of policies is defined, Safend's Management Console deploys these to the various endpoints. The console also allows system administrators to check the access rights of users periodically within the system. Safend transfers these sensitive credentials using a secure SSL channel, so remote systems can be administered from a single location; only defined administrators can perform the actions within the Management Console. Safend Protector Client then enforces the policies at the endpoint. The client limits information flow from the endpoint to external data destinations. The transfer can be restricted as follows

- Do not allow write to the port
- Require Encryption
- Allow full access

Restrictions can be associated with a particular device or port and can also be defined on a per-file basis by linking to the policy manager from Websense (a Safend technology partner). Websense also provides content profiles and can be used in content filtering at the endpoint. Additionally, as part of the control, access to wireless networks is also enforced per the distributed policy. This ensures that only specified networks, with their associated encryption, are used.

Although the Basel II Accord has not specified how to implement operational security, or how to meet specific requirements, any operational security program will need to cover the general system security controls presented in the following section. The table below shows how the Safend product features assist with implementing or strengthening these controls.

General System Security Controls	Safend Features
Administrative Safeguards	
Information Policies and Procedures	The Management Server supports administrative policies and procedures with the deployment of access control policies for information sent outside the corporate network.
Information Security Roles and Responsibilities	Safend Protector defines administrators within the system. The Administrator can then develop and deploy policies that are used to control that access to financial information. Unless otherwise implemented, end users do not have the ability to change the policy once it has been deployed.
Independent Security Risk Assessment	Safend Auditor provides a full view of the ports, devices and networks in use by your organization's users, as well as a history of what was used previously. The Safend Auditor scan output can be used to select the devices and networks to control. Left uncontrolled, all of these devices present a vulnerability around the misuse of financial information.
Security Risk Management	Safend provides security measures that can be incorporated into a completed set of controls for managing the access to financial information. For example, Safend products include: Preventative: Controls data access at the endpoint Detective: Provides detective controls, in the form of auditing and alerts, to supplement preventative controls. Corrective: Detects and then blocks Hardware Key Loggers that are connected to a USB or a PS/2 port.
Physical Safeguards	
Manage removable media	The Safend Auditor delivers a complete listing for every endpoint, information that shows any external storage devices that have been connected or removed. The log also reports which files have been transferred to removable media. Administrators can query this file list to determine if the removable storage contains any financial information.
Manage media in transit	<p>Using the policy manager, user behavior is controlled at the endpoint. Depending on the connected device, Safend Protector can force all information directed to a specific device to be encrypted.</p> <p>As a rule, organizationally-encrypted removable storage devices can be used only when connected to computers protected by the organization's Safend Protector Clients. An optional function allows or prohibits content from being opened on non-organizational computers.</p> <p>For Non-encrypted Devices, policies can be deployed that determine behavior when a non-encrypted device is detected; the device may either be blocked, or permitted Read Only access.</p> <p>Wireless networks can be controlled at the endpoint. Two types of control are available:</p> <ol style="list-style-type: none"> 1 Specify which connection types are allowed access 2 Determine which specific networks are allowed access.
Technical Safeguards	
User Registration	One of the main strengths of Safend Protector is its deep integration with existing IT infrastructures. Once installed, the product automatically discovers the network, connects to Active Directory (AD) and synchronizes (read-only) with the existing organizational structure, including OUs, Groups, Users and Computers. The Safend products then utilize the directory's user identification to assign associated policies and identification in the audit logs.
User Account Management	Because Safend Protector is integrated with user access control, endpoint device and port access can be adjusted easily on a user-by-user basis. Furthermore, this can be done at the individual or role level using the Management Console to create and deploy access control policies.

Technical Safeguards (continued)

User Rights Management	Safend Protector policies can be distributed or published using Microsoft's standard Active Directory GPO distribution feature. The policies are tied into the Windows authentication system. This authenticates the user, so the associated Safend policy can be enforced. The policy then allows or denies access to financial information on removable storage.
Access Rights Control Procedures	<p>The Management Server distributes policies directly to Clients via a secure SSL channel. It also supports an alternative distribution method which uses the Active Directory GPO mechanism. GPOs representing policies are written to Active Directory. After they are linked with the OUs of the organization, the policies are downloaded and applied to endpoints.</p> <p>When encryption is used, a decryption password is set on the file. The encrypted file can then only be opened by a user who has this password.</p>
System Access Control	Safend Protector enables access control by allowing full access, blocking or Read Only access by any device that is identified as a storage device. This includes removable media such as disk-on-keys, digital cameras and more, as well as traditional devices such as floppy drives, CD/ DVD drives, external hard drives and tape drives.
Network Access Controls	<p>Safend creates policies that specify how wireless networks can be accessed at the endpoint. Two types of controls are available:</p> <ol style="list-style-type: none"> 1 Specify which connection types are allowed access 2 Determine which specific networks are allowed access <p>Using these policies, Safend creates a white list of allowable networks to prevent any data transfer over unsecured or prohibited networks.</p>
Data Protection	<p>Using the policy manager, user behavior is controlled at the endpoint. Depending on the connected device, Safend Protector can force all information directed to a specific device to be encrypted.</p> <p>As a rule, organizationally-encrypted removable storage devices can be used only when connected to computers protected by the organization's Safend Protector Clients. An optional function allows or prohibits content from being opened on non-organizational computers.</p> <p>For Non-encrypted Devices, policies can be deployed that determine behavior when a non-encrypted device is detected; the device may either be blocked, or permitted Read Only access.</p>
Audit Logging	<p>Events that occur on endpoints protected by Safend Protector Clients are recorded in logs and/or alerts. An event may be a connection or a disconnection of a device, connection to a wireless network, tampering attempts or administrator login, as well as many more. These events are stored as Client logs. Logs and alerts - which record the name of a file read from or written to storage devices - are stored as File logs.</p> <p>The logs and alerts of Client and File Logging may refer to a computer or a user, depending on how an organization applies the policy that dictates them. In addition to events which occur on protected endpoints, Safend also creates logs and alerts for Safend Protector Management Server events, such as administrator login, publishing policies and performing backups.</p> <p>Client and Server logs and alerts are sent to a log repository and stored on the Management Server at the intervals defined in the Client's policy.</p>
Network Segregation	<p>Wireless networks can be controlled at the endpoint. Two types of control are available:</p> <ol style="list-style-type: none"> 1 Specify which connection types are allowed access. 2 Determine which specific networks are allowed access.

Conclusions

Mobile technologies have created new challenges for the management of operational risk. The traditional approaches to system security have serious limitations - an information perimeter with localized access control points cannot address all system risks. Newer technologies have been able to leapfrog this barrier and transfer any information without defined access controls. The result is a higher potential for failure to manage operational risk. This means that organizations are now more concerned than ever to ensure the thorough control of critical and sensitive data access, in all its forms.

Safend augments system security controls and integrates with organization access to control the flow of information from the endpoint. It tackles the difficult job of making sure that data leakage has minimal impact on operational risk. Safend also provides tools to manage the protective aspects and the audit requirements of the regulation. Plus, the technical controls can easily be integrated into existing policies and procedures - controls which can be quickly deployed. Without this type of security countermeasure, organizations face serious cracks in any infrastructure designed to address operational risk.

About Safend

Safend is a leading provider of endpoint information leakage prevention solutions that protect against corporate data loss via physical, wireless, and removable media ports while ensuring compliance with regulatory data security and privacy standards. Safend's solutions, available through resellers worldwide, are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe.

Founded in 2003, Safend is a privately held company funded by Elron Electronics (NASDAQ and TASE: ELRN), Intel Capital, and Walden Israel. Safend is headquartered in Tel Aviv with US headquarters in Philadelphia. For more information, visit www.safend.com.



Safend Ltd.

32 Habarzel Street
Tel-Aviv 69710, Israel
Tel. +972.3.6442662
Fax. +972.3.6486146

Safend Inc.

2 Penn Center, Suite 301,
Philadelphia, PA 19102, USA
Tel. +1.215.496.9646
Fax. +1.215.636.0251

Toll free from the US (to US and Israel):
1.888.225.9193 | info@safend.com

www.safend.com