safend
a SuperCom company

PROTECTOR

MARKET OPPORTUNITY

- Compliance: Safend encrypts external media which is a requirement of standards like GDPR EU or HIPAA
- Safend helps prevent organizational mistakes. Good people doing bad things.
- Safend protects against external threats from endpoints.
- Safend limits Wi-Fi connectivity to secure networks only.

KEY FACTS

2016 Data Breach Statistics

- 3.04 million recorded breaches per day.
- 126,936 recorded breaches per hour.
- 2,116 recorded breaches per minute.
- 35 recorded breaches per second.
- The most common type of breach is identity theft.
- Most breaches were from external sources.
- Government has the most lost/stolen data.
- Healthcare has the most breaches.
- USA is the most targeted country.
- In 2016 costs related to data breaches = $4 million, up from the $3.8 million in 2015. (IBM Survey 2016).
- 71% of employees reported that they can access data they should not see. Over half say that this access is frequent or very frequent.

CUSTOMER PAIN POINTS

- Implementing compliancy requirements like GDPR EU.
- Support and secure more and more removable storage devices, smart phones, physical and wireless interfaces
- Control users with access to sensitive information via endpoints, to avoid both accidental and malicious data leakage.
- Preventing employees / partners / others from connecting a smartphone, USB thumb drive or removable memory stick to an enterprise endpoint and walking away with sensitive data.
- Avoiding network connections to Wi-Fi, Bluetooth or 3G/4G and bridging classified internal networks to open external networks that may lead to loss of data. loss of data.
- Identify and implement easy-to-use and quick deployment solutions.

SOLUTION OVERVIEW

- Protector is an easy-to-use endpoint data protection and data breach prevention solution for controlling endpoints.
- Protector allows IT to set policies to encrypt data that is written to removable media and to enforce port and device control.
- Protector monitors and applies customized, highly-granular security policies over physical / wireless interfaces and external storage devices.
- Protector can detect, allow and restrict data according to device type, model or specific device serial number.
- Storage devices: Protector allows security administrators to block all storage devices completely, configure read-only permissions or to encrypt all data. It also monitors, blocks and logs files that are sent to or retrieved from these devices.

UNIQUE SAFEND DPS SELLING POINTS

- Probably the best providers of portable device control solutions.
- A flexible and highly granular solution for administrators.
- Easy to install, use, manage and transparent to end-users. Doesn't interfere with daily work activities.
- Light-weight agent: deploys a single agent that protects, inspects and encrypts data.
- Licensing flexibility: customers can purchase other Safend module licenses with zero deployment.
- Granular port and device control by model and device ID with easy to manage black / white lists
- Granular Wi-Fi control by SSID or the security level of the network.
- Anti-bridging: prevents hybrid networks bridging by blocking Wi-Fi, Bluetooth, modems or IrDA while the PC is connected to a wired corporate LAN.
- Anti-hardware keylogger: blocks or detects both USB and PS/2 hardware keyloggers.
- U3 and autorun control: turns U3 USB drives into regular USB drives when attached to organization endpoints, protecting against auto-launch programs by blocking autorun.

COMPETITIVE ANALYSIS

Capabilities	Safend Protector	McAfee	Trend-Micro
Protection Before User Login (PBUL)	Yes	No	No
Anti-hardware key logger	Yes	No	No
Port lock – fully blocks port activity	Yes	No	No
Wi-Fi white listing	Yes	No	No
Anti-bridging	Yes	No	No
File contact logging (file shadowing)	Yes	No	No
Removable media encryption	Yes	Yes	No
One time access key for encryption of removable media	Yes	No	No
Built-in policies for regulatory compliance	Yes	No	No
Supports up to 1000 users on one embedded internal database	Yes	No	No

CUSTOMER BENEFITS

- Minimizes loss: protects all sensitive data like enterprise IP and electronic assets from accidental loss and intentional theft.
- Security: mitigates malware and virus outbreaks via removable storage devices. Provides policy-driven port and device control and removable media encryption.
- Compliance: customers fit compliance with privacy regulations. Policies are preconfigured for specific regulatory compliance standards, such as PCI, HIPAA, SOX, and GDPR.
- Generates logs of all data moving in and out of company endpoints.
- Cost: minimizes IT overhead and help desk costs associated with the setup, deployment and maintenance of removable media encryption and port and device control.
- Flexible and intuitive management: IT-familiar interface. Automatically synchronizes with Microsoft Active Director.