safend
a SuperCom company

ENCRYPTOR

MARKET OPPORTUNITY

- Compliance: encrypts the hard disk which is a requirement of standards like GDPR EU or HIPAA.
- Protects theft of data on saved on lost / stolen devices.
- Fast, simple and transparent deployment, ideal for companies without the resources for complex solutions.
- Protects against data theft from within an organization. Bad people doing bad things.

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 are 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.
- 71% of employees reported they can access data they should not see. Over half say that this access is frequent or very frequent.

CUSTOMER PAIN POINTS

- The need to protect data at rest.
- The need to prevent data theft from stolen / lost devices.
- Time consumption of IT resources: laptop/PC encryption and employees training on product usage. Customers are looking for ease of use and quick deployment
- Usage of multiple passwords that people need to remember.
- The need for additional password recovery management.
- Slow encryption, leaving the machine unprotected during the encryption process.

SOLUTION OVERVIEW

- Encrypts all data on laptops and desktops: TOTAL DATA ENCRYPTION.
- Encryptor offers true Single Sign On (SSO) technology which is transparent to end users and help desk personnel.
- Encryptor is centrally managed and easily enforces policies and rules.
- Encryptor offers full visibility of an organization's encryption status.
- Encryptor offers stable and fault tolerant encryption due to its ability to maintain performance and minimize the risks of OS failure.
- Encryptor is easily integrated with Microsoft Active Directory or workgroup environments.
- Encryptor offers a mode where technicians can work on a computer without being exposed to sensitive data.

UNIQUE SELLING POINTS

- Flexible use cases: enables IT to set policies that encrypts data associated with Active Directory objects.
- Ease of use: transparent to end-users; doesn't interfere with daily work routines.
- Light-weight agent: deploys a single agent that consolidates all Safend capabilities including encryption.
- Licensing flexibility: customers can separately license data protection and encryption enabling them to only pay when needed.
- Extensive interface coverage: supports all latest Windows operating systems.
- Optimum balance between security, productivity and performance.
- Due to its seamless and unique technology the Encryptor has almost no impact on a user's day to day activities.
- Directory services integration: Safend server automatically synchronizes with Active Directory and enables applying policies to specific organizational units, machines or users.
- Automatic key management: Encryptor incorporates a fully automated key management solution. All encryption keys are centrally generated and securely stored on the management server before encryption is initialized. Encryption keys are generated using a FIPS approved PRNG.
- Comprehensive data recovery: data recovery is intuitive, comprehensive and always possible. Data recovery is performed using a lightweight executable which is installed on endpoint machines or supplied on a bootable Windows PE CD.
- Full visibility and audit trail: enables receiving and viewing detailed logs regarding endpoint security incidents and time-stamped encryption status. Saves detailed forensic information on encryption status and administrative actions.
- Real-time alerts on all events received by the server by email, SNMP and additional methods.
- Tamper resistant: the Safend agent includes redundant, multi-tiered anti-tampering features that guarantee permanent control over enterprise endpoints.

COMPETITIVE ANALYSIS

Requirement	Safend Encryptor	Full Disk Solution
Start-up does not require pre-boot authentication	Yes	No
Need to decrypt OS files after system failure	No	Yes
Fast system start-up	Yes	No
Technician mode enabling IT personnel to log in to a computer without accessing encrypted data	Yes	No
Centrally managed encryption of computers outside a domain	Yes	No

CUSTOMER BENEFITS

- Minimizes loss: protects an organization's intellectual property from unintended loss and intentional theft.
- Security: encrypts all data on laptops and desktops.
- Compliance: AES256 compliance, Common Criteria EAL2 certified, FIPS 140-2, helps customers comply with privacy regulations.
- Cost: minimizes IT overheads and help desk costs associated with the setup, deployment and maintenance of encrypting machines.
- Flexible and intuitive management: IT-familiar interface. Automatically synchronizes with Microsoft Active Directory.