

safend

Data Protection Suite

Einhaltung der regulatorischen
Datensicherheits- und
Datenschutzstandards



Pflege einer optimalen Balance
zwischen Produktivität und
Datensicherheit

Schutz von Firmen-IP,
Betriebsgeheimnissen, sensiblen
Kunden- und Mitarbeiterdaten

Wirksamer Datenschutz beginnt am Endpunkt

Die Safend Data Protection Suite schützt Organisationen gegen Datendurchsickern und -diebstahl mit einem einzelnen Softwareprodukt, das detaillierte Port- und Gerätekontrolle, transparente Festplattenverschlüsselung, umfassende Wechselmedienverschlüsselung und genaue Inhaltskontrolle bietet. Es liefert vollständigen Schutz der sensiblen ruhenden, beweglichen und Nutzungsdaten ohne Produktivitätseinbußen.

Die Gefährdung – Datenverlust am Endpunkt

Das Überleben und der Erfolg des Geschäfts basieren auf der Datensicherheit. Organisationen sind von der Sicherheit ihrer Daten abhängig – vom geistigen Eigentum wie Geschäftspläne und Firmengeheimnisse bis hin zu sensiblen Kundendaten wie Gesundheitsdaten, Finanzdaten und Personalausweisnummern.

Gesetzliche Sicherheitsinitiativen wie z.B. Sarbanes Oxley (SOX), HIPAA, PCI, FISMA und der UK Data Protection Act (DPA) fordern, dass Organisationen eine laufende Sicht in die Endpunkt-Aktivitäten haben. Bei dem heutigen empfindlichen Gesetzesklima wird von Organisationen erwartet, eine umfassende Datenschutzstrategie und Verständnis aller Datenübertragungsaktivitäten darzulegen.

Branchenstatistiken zeigen ständig, dass die bedeutendsten Sicherheitsbedrohungen für das Unternehmen aus dem Inneren kommen. Bei über 60% von Unternehmensdaten, die auf Endpunkten angesiedelt sind, können Gateway-Lösungen und geschriebene Sicherheitsrichtlinien alleine das Risiko nicht mindern.

Die wachsende Anzahl an Wechselspeichergeräten, Schnittstellen (physikalischen und drahtlosen) sowie Benutzern mit Zugang zu sensiblen Daten haben das Durchsickern von Daten über Endpunkte, sei es versehentlich oder böswillig, zu einer echten Bedrohung gemacht. Es ist eine unvermeidliche Tatsache, dass Laptops verloren gehen oder gestohlen werden. Genauso ist es auch zu leicht möglich, dass sensible Daten auf einem iPod das Haus verlassen oder in das Internet hochgeladen werden. Laut Forrester ist der Datenverlust über Endpunkte jetzt ein führendes Endpunkt-Sicherheitsproblem – vor Malware, Spyware und anderen Bedrohungen.

Die Herausforderung – Wirksamer Endpunkt-Datenschutz

Trotz der deutlich offensichtlichen Gefahr des Durchsickerns und des Verlustes von Daten bleibt der wirksame Endpunkt-Datenschutz für die meisten Organisationen ein mühsamer Kampf. Die Sicherung von Endpunkten, ohne die Produktivität der Mitarbeiter und die Systemperformance zu beeinträchtigen, erfordert eine höchst flexible Lösung, die die Dynamik des realen Umfelds berücksichtigt.

Viele Endbenutzer betrachten externe Geräte und ausgehende Kommunikation als persönlich und erachten die Verschlüsselung jeder Art als eine lästige, oft gescheute und hemmende, aufgezwungene Sicherheitsmaßnahme. Daher müssen die Datenschutzlösungen von heute transparent sein, ohne die Datensicherheit einer Organisation zu gefährden. Alle möglichen Wege des Durchsickerns von Daten an Endpunkten müssen mit leistungsstarker, durchsetzbarer, manipulationssicherer Sicherheit verwaltet werden.

Endpunktdaten können die Unternehmensbarrieren auf zahlreichen Wegen verlassen: Sie können auf einem unverschlüsselten Speichergerät abgespeichert und entwendet werden, versehentlich an unbefugte E-Mail-Empfänger gesendet oder mit dem Laptop, auf dem sie gespeichert sind, gestohlen werden. Ein wirkungsvolles Endpunkt-Sicherheitsprogramm muss den gesamten Risikobereich angehen, um die Daten der Organisation ordnungsgemäß zu schützen.

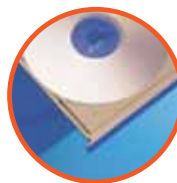
* Forrester Research Inc, eine Marktforschungsfirma

Die Endpunkt-Gefährdung in Zahlen

- *Mehr als ein Drittel (36%) der befragten US-Unternehmen stellten fest, dass ihr Geschäft durch die Veröffentlichung von sensiblen oder peinlichen Informationen in den letzten 12 Monaten betroffen war.*
– Osterman Research 2010
- *Mehr als 70% der Sicherheitsverletzungen und des Datendiebstahls kommen von Innen*
– Vista Research

Die Kosten des Datenverlusts

- *Durchsickerns*
Die Durchschnittskosten für jede Datenverletzung betragen 6.75 Mio US Dollar, und die Kosten pro Datensatz lagen 2009 bei 204 US Dollar
– Ponemon Institute
- *Informationsverletzungen verursachten einen durchschnittlichen 5%-igen Rückgang des Aktienpreises des Unternehmens. Eine Erholung auf das Niveau vor dem Vorfall dauert fast ein Jahr*
– EMA Research



Die Lösung – Safend Data Protection Suite

Die preisgekrönte Safend Data Protection Suite liefert vollständigen Endpunkt-Datenschutz ohne die Produktivität zu beeinträchtigen. Jede Komponente der Safend Data Protection Suite kann einzeln oder in Kombination implementiert werden und ergänzt Ihre bestehende Sicherheitsinfrastruktur.

Die Safend Data Protection Suite beinhaltet:

Safend Discoverer – Lokalisieren und Abbilden sensibler Daten, die auf den Endpunkten Ihrer Organisation gespeichert sind.

Safend Inspector – Prüfen, Klassifizieren, Filtern und Blockieren des Durchsickerns von sensiblem Inhalt durch E-Mail, IM, Internet, externe Speicher, Drucker usw.

Safend Encryptor – Transparenter Schutz und Verschlüsselung von Laptops und PCs.

Safend Protector – Sperren oder Verschlüsseln von Daten, die auf externe Medien und Geräte (CD/DVD, USB, FireWire, usw.) übertragen werden, und Sperren von Verbindungen zu unsicheren drahtlosen Netzen.

Safend Auditor – Direkte Erkennung Ihrer Sicherheitsrisiken durch ein clientloses Tool, das die aktuell oder zuvor an Endpunkten über USB, Firewire, PCMCIA oder WiFi-Ports angeschlossenen Geräte identifiziert.

Safend Reporter – Einfache Generierung grafischer Compliance-Reports und Sicherheitslog-Übersichten mit Hilfe eines intuitiven Tools.

Kundenempfehlungen

“Einfach mehr als 500 Leuten zu sagen, sie sollten ihre USB-Ports nicht benutzen, war keine realistische Lösung...Safend gibt uns, was wir brauchen, um den Datenschutz und die Integrität unserer Kundendaten zu erhalten.”

- Bill Liston, IT Solutions Technician, ConnectiCare

“Die Produkte von Safend sind gut durchdacht und erreichen tatsächlich mehr, als wir erwartet haben. Das Produkt ist robust und hilft uns bei unserem proaktiven Streben, mögliche Probleme zu identifizieren.”

- Alan Pomerantz, Chief Security Officer, Philadelphia Stock Exchange

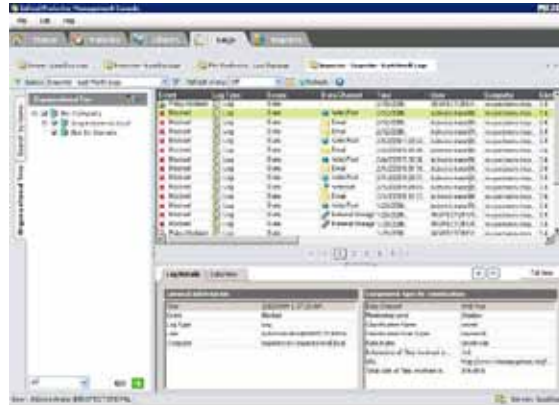
“Seitdem wir Safend installiert haben, können wir leicht alle Geräteaktivitäten in unserer Organisation überwachen und kontrollieren...das Deployment lief reibungslos – keine Fehler, keine Umstände...das hat uns Zeit und unnötigen Aufwand erspart.”

- Michael Apt, IT and Security Manager, SCD



Die ultimative Kombination von Sichtbarkeit, Kontrolle und Schutz

Die Safend Data Protection Suite schützt Ihre Organisation gegen die Kompromittierung oder den Verlust von Daten durch seine **Ein-Server-, Eine-Konsole-, Ein-Agent-Architektur**. Manipulationssicher und mit transparentem Betrieb auf jedem Endpunkt entdeckt, klassifiziert, schützt, alarmiert, protokolliert, sperrt und verschlüsselt die Safend Data Protection Suite die wichtigsten Daten Ihrer Organisation, ganz gleich, ob die Geräte online oder offline sind.



Warum Safend?

- Ergänzt Ihre bestehende Sicherheitsstruktur auf flexible Weise
- Verwaltung aller Ihre Datenschutzmaßnahmen mit einem **einzelnen** Server, einer **einzelnen** Konsole und einem **einzelnen** leichten Agenten
- Echtzeitüberwachung und inhaltspezifisch abgestimmte Zuweisung von Sicherheitsregeln auf alle physischen, drahtlosen und Wechselspeicher-Schnittstellen
- Zugangskontrolle von Anwendungen auf Inhalte (alle Protokolle) – erlauben Sie iPads, iPhones und andere Smartphones selektiv zu synchronisieren
- Port- und Gerätekontrolle der Spitzenklasse
- Die Festplattenverschlüsselung ist absolut transparent und verändert weder die Endbenutzererfahrung noch die üblichen IT-Prozeduren
- Umfassende und durchsetzbare Wechselmedien-Verschlüsselung
- Vollständige Kontrolle über sensible Daten, sowohl innerhalb als auch außerhalb des Netzwerks der Organisation
- Verfolgung der Dateiübertragung von verschlüsselten Geräten sogar auf unternehmensfremden Computern
- Jeder Computer ist die ganze Zeit über geschützt, auch wenn er nicht mit dem Netz verbunden ist
- Von Grund auf so aufgebaut, umfassende Sicherheitsrichtlinien durchzusetzen, die Ihren speziellen organisatorischen Bedürfnissen entsprechen
- Common Criteria EAL2-Zertifizierung und FIPS 140-2 bestätigt

Über Safend

Safend ist ein führender Lieferant von Endpunkt-Datenschutz-Software. Unsere Produkte schützen gegen den Verlust von Unternehmensdaten, indem sie umfassende Datenverschlüsselung, Portkontrolle, Gerätekontrolle und Inhaltsprüfung bieten und dabei die Einhaltung der regulierten Datensicherheits- und Datenschutzstandards sicherstellen. Die Produkte von Safend verschlüsseln interne und externe Festplattenlaufwerke, Wechselspeichergeräte und CD/DVDs. Sie bieten eine detaillierte Port- und Gerätekontrolle über alle physikalischen, drahtlosen und Wechselmedien-Geräte und kontrollieren die sensiblen Daten, die über Endpunkte und Netzwerkkanäle transferiert werden. Mit über 2,200 Kunden weltweit und 2.6 Millionen verkauften Lizenzen wird die Software von Safend von multinationalen Unternehmen, Regierungsstellen, Gesundheitsorganisationen und kleinen bis mittelgroßen Firmen auf der ganzen Welt eingesetzt.



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: +1.215.496.0251

Gebührenfrei in den USA (nach US und Israel): 1.888.225.9193 info@safend.com

Copyright © 2011 Safend Ltd. Die hierin gemachten Angaben gelten zum Zeitpunkt der Veröffentlichung und können ohne Vorankündigung geändert werden. 01/11