

safend inspector

Inhaltsprüfung und Filterung



- Verhinderung des Durchsickerns sensibler Daten durch E-Mail, Internet, Wechselspeicher und andere Datentransferkanäle
- Verhindern von Benutzerfehlern und erhöhtes Sicherheitsbewusstsein
- Ermöglichung der Einhaltung von gesetzlichen, Datensicherheits- und Datenschutzstandards.
- Nutzen und Verwalten eines einzelnen Agenten für alle Datenschutzbedürfnisse

Safend Data Protection Suite

schützt Ihre Organisation gegen Datenverlust am Endpunkt, Missbrauch oder Diebstahl durch seine Ein-Server-, Eine-Konsole-, Ein-Agent-Architektur. Die preisgekrönte Suite besteht aus:

Safend Discoverer – Lokalisieren und Abbilden sensibler ruhender Daten.

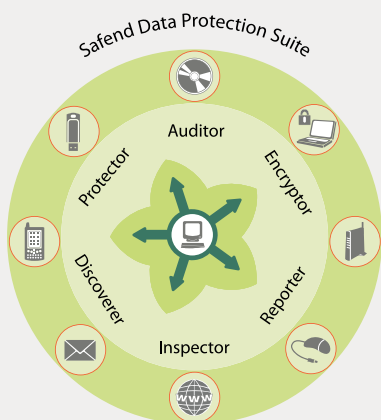
Safend Inspector – Prüfen, Klassifizieren und Blockieren des Durchsickerns von sensiblem Inhalt durch E-Mail, IM, Internet, externe Speicher, Drucker usw.

Safend Encryptor – Transparente 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 von Sicherheitsrisiken durch Identifizieren der WiFi-Ports oder Geräte, die aktuell oder zuvor an Endpunkten angeschlossen sind bzw. waren.

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



Der Bedarf an Endpunkt-Inhaltskontrolle

Branchenstatistiken zeigen ständig, dass die bedeutendsten Sicherheitsbedrohungen für die Organisation 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.

Sensible Daten können die Organisationsgrenzen über mehrere Kanäle verlassen. Sie können auf einem USB-Flash-Drive weggetragen, auf CD gebrannt, per E-Mail gesendet oder im Internet eingestellt werden. Während einige Datenübertragungskanäle teilweise deaktiviert werden können, um das Risiko zu minimieren, können doch nur wenige Organisationen den abgehenden Datenverkehr komplett deaktivieren, ohne die Produktivität drastisch zu beeinträchtigen. Für die richtige Ausgewogenheit von Sicherheit und Compliance-Bedürfnissen mit den Geschäftszielen müssen Durchsetzungsmaßnahmen sorgfältig so abgestimmt werden, dass nur die spezifischen, durch die Firmenrichtlinien eingeschränkten Daten kontrolliert werden, ohne legitime Benutzeraktivitäten zu unterbrechen.

“Beispielloser Datenschutzskandal bei der Telekom: 17 Millionen Handy-Nummern und Personendaten sind gestohlen worden - auch jene von Prominenten, deren Sicherheit gefährdet ist. Jetzt bietet der Konzern besorgten Kunden neue Telefonnummern an.” Der Spiegel

“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 eine durchschnittlich 5%-igen Rückgang des Aktienpreises des Unternehmens. Eine Erholung auf das Niveau vor dem Vorfall dauert fast ein Jahr” EMA Research

Safend Inspector - Verhindern des Durchsickerns sensibler Daten

Safend Inspector setzt eine datenzentrische Sicherheitsrichtlinie über mehrere Kanäle durch, darunter E-Mail, Internet (HTTP, HTTPS), FTP, externe Speichergeräte, CD/DVD-Brenner, iPad, iPhone und andere smart phones, Dateispeicher, Bildschirmdruck, lokale Drucker, und Netzwerkdrucker, ohne legitime Geschäftsprozesse zu unterbrechen oder die Produktivität der Endbenutzer zu beeinträchtigen.

Benutzeraktionen können mit einer “Sind Sie sicher?”-Meldung gestoppt oder überwacht werden, oder es kann ein Alarm für den Sicherheitsadministrator auf der Basis des aktuellen Inhalts der transferierten Daten sowie des Aktionszusammenhangs und der Metadaten erstellt werden. Dieser Schutz ist voll aktiv, unabhängig davon, ob das Gerät an das Netz der Organisation angeschlossen ist oder offline genutzt wird.

Sicherheitsrichtlinien sind äußerst detailliert und können unterschiedliche Schutzmaßnahmen anwenden, je nach den kanalspezifischen Kontextdaten. Beispielsweise kann eine Sicherheitsrichtlinie Benutzer daran hindern, vertrauliche Daten auf externe Speichergeräte, die keine vom Unternehmen herausgegebenen hardwareverschlüsselten Geräte sind, herunterzuladen.

Safend Inspector – Funktionen und Vorteile

- **Umfassender Schutz**
Setzt eine datenzentrische Sicherheitsrichtlinie über mehrere Kanäle durch, unabhängig davon, ob das Gerät an das Netz der Organisation oder ein Heimnetz angeschlossen ist oder offline genutzt wird. Weitere Kanäle können bei Bedarf mittels Application Data Access Control hinzugefügt werden.
- **Genauere Datenklassifizierung**
Mehrere Datenidentifizierungstechniken können für eine äußerst genaue Datenklassifizierung kombiniert werden.
- **Integrierte Compliance-Richtlinien**
Enthält vorkonfigurierte Sicherheitsrichtlinien, die darauf ausgelegt sind, bestimmte regulatorische Compliance-Standards (wie PCI, HIPAA und Basis-Il) anzugehen.
- **Umfassende Endbenutzer-Interaktion**
Sicherheitsrichtlinien können Benutzer auffordern, Berechtigungen für problematische Aktionen nachzuweisen. Eine solche Policy kann schnell und genau die Durchsetzungsschleife schließen und Benutzern helfen, möglicherweise schädliche Aktionen zu vermeiden, ohne die Geschäftsprozesse zu unterbrechen.
- **Volle Sichtbarkeit und Prüfprotokoll**
Liefert detaillierte Protokolle und Reports zu Sicherheitsvorfällen und administrativen Aktionen.
- **Manipulationssicher**
Der Agent enthält Multi-Tier Manipulationsschutz-Fähigkeiten, um die ständige Kontrolle über die Endpunkte des Unternehmens zu garantieren.
- **Flexible und intuitive Verwaltung**
Automatische Synchronisation mit Microsoft Active Directory und Novell eDirectory.
- **Kontrolle iPad, iPhone und andere Smartphones Synchronisation**

Über Safend

Safend ist ein führender Lieferant von Endpunkt Datenschutz-Software. Unserer 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.

Technische Daten

Kontrollierte Netzwerkkanäle

- ✓ E-Mail
- ✓ Internet (HTTP / HTTPS)
- ✓ Netzwerkdrucker
- ✓ Gemeinsame Dateinutzung
- ✓ FTP

Kontrollierte Endpunktkanäle

- ✓ Wechselspeichergeräte
- ✓ Externe Festplattenlaufwerke
- ✓ CD/DVD
- ✓ Lokale Drucker
- ✓ Bildschirmaufnahmen
- ✓ Anwendungskanäle (eigen)
- ✓ iPad, iPhone, iPod

Zertifizierung

- ✓ Common Criteria EAL2-Zertifizierung
- ✓ FIPS 140-2 Bestätigt

Systemanforderungen – Agent

- ✓ Windows XP Professional SP2+ x32 and x64
- ✓ Windows XP Tablet PC Edition (SP2, SP3)
- ✓ Windows 2003 Server (SP1, SP2)
- ✓ Windows Vista SP1+ (x32 and x64)
- ✓ Windows 7 (x32 and x64)
- ✓ Windows 2008, R1, R2

Systemanforderungen – Server

- ✓ Windows 2003 Server (SP1, SP2)
- ✓ Windows 2008, R1, R2