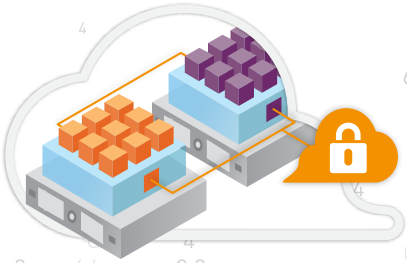
SafeNet | THE DATA PROTECTION COMPANY



ProtectV™

Datensicherheit für die Cloud

PRODUKTÜBERSICHT

Sicherheitsrisiken der Virtualisierung

Die strukturellen Unterschiede zwischen physikalischen und virtuellen Umgebungen können die Datenintegrität gefährden, die Kontrolle über die Benutzerzugriffe einschränken, die Compliance negativ beeinflussen und Haftungsrisiken erhöhen.

Weite Verbreitung der VMs

- Leicht zu replizieren durch einfache Snapshots
- Backups über unterschiedliche Rechenzentren rund um die Welt
- Snapshots und Backups lassen sich leicht verschieben, kopieren oder stehlen, ohne dass dieses erkannt wird

Mehr privilegierte Benutzer

- Admins und Benutzer mit besonderen Rechten arbeiten häufig unabhängig voneinander
- Vermischung der Daten in mandantenfähigen Umgebungen
- Trennung der Aufgaben zwischen Cloud-Dienstleister und IT-Administration des Unternehmens ist schwer sicherzustellen

Die Cloud bietet wichtige Funktionen, um Wettbewerbsvorteile am Markt zu erhalten: Agilität, Elastizität, Kapazität und Redundanz.Mit dem Umzug der Server vom dedizierten, physikalischen Rechenzentrum auf virtuelle Infrastrukturen oder in private, hybride oder mandantenfähige öffentliche Clouds erlangen Unternehmen wesentliche Vorteile hinsichtlich Kosten und Effizienz.

Allerdings führt dieser Schritt zu einer zusätzlichen Schicht an virtualisierungsspezifischen Sicherheitsfragen. Die Unternehmen sind immer gefordert, eine stabile Informationssicherheit zu gewährleisten. Und selbst in privaten Clouds oder auch noch stärker isolierten Umgebungen wie virtuelle Rechenzentren sind die Daten Gefährdungen ausgesetzt.

Vorhang auf für SafeNet ProtectV – die erste umfassende, hochsichere Lösung zur Absicherung virtualisierter Infrastrukturen und Daten. So können Unternehmen auf virtualisierte Umgebungen oder in Clouds migrieren, ohne die Eigentumsrechte, Compliance und Kontrolle über die Daten aufs Spiel zu setzen.

Schützen Sie Ihre Daten in virtualisierten Umgebungen und in der Cloud mit ProtectV

Geschäftsnutzen	Merkmale
Erstes vertrauenswürdiges „Schließfach" zum Schutz virtueller Umgebungen Die vollständige Verschlüsselung sowohl virtueller Maschinen als auch von Speicher-Volumes in Verbindung mit der manipulationssicheren Authentisierung vor dem Start des Betriebssystems gewährleistet eine komplette Isolierung der Daten und die Trennung der Verantwortlickkeiten. ProtectV gewährleistet, dass die virtuellen Server und Massenspeicher so sicher sind wie physikalische Server und Storage in einem robusten, sicheren Rechenzentrum vor Ort. ProtectV ermöglicht es Unternehmen, den Zugriff und die Vernichtung der Daten zu kontrollieren. Unerlaubte oder versteckte Snapshots und Kopien werden so nutzlos.	**Vollständige Verschlüsselung virtueller Maschinen und Speicher:** • Ermöglicht die Verschlüsselung von kompletten virtuellen Maschinen und der zugehörigen Speicher-Volumes. • Es werden keine Daten auf Systempartitionen oder Speicher-Volumes geschrieben, ohne diese zuerst zu verschlüsseln. • Selbst Daten, die auf der OS-Partition gespeichert werden, sind geschützt. • Das Schlüssel-Material wird in einem hochsicheren, Hardware-basierenden Key-Manager gespeichert.
Die einzige hochsichere Lösung zur Daten-Compliance Hardware-basierendes Key-Management vor Ort zusammen mit Authentisierung vor dem Systemstart und granulare Zugriffssteuerung – das bedeutet unangefochtene Kontrolle über Daten und Schlüssel sowie sichere Eigentumsrechte. ProtectV schützt virtualisierte Daten, verhindert unerlaubte Verwendung von Daten und Missbrauch von Superuser-Rechten. So hilft die Lösung bei der Einhaltung verschiedener Vorschriften wie PCI oder HIPPA.	**Authentisierung vor dem Systemstart:** • Der Zugriff auf Daten, die in einer geschützten VM gespeichert oder verarbeitet werden, erfordert die explizite Authentisierung und Autorisierung des Benutzers durch ProtectV. **Trennung der Aufgaben:** • Die Trennung der Aufgaben zwischen den Systemadministratoren des Cloud-Dienstleisters und den IT-Administratoren des Unternehmen wird durch rollenbasierende Verschlüsselungsrichtlinien und einem isolierten Key-Management sicher gestellt.
Übersicht und Nachweis der Data Governance Erhöhte Kontrolle und robuste Sicherheit – SafeNet bietet einen einzigen, zentralen Punkt zur Durchsetzung der Richtlinien und für Audits. So wird Data Governance auf Basis von expliziter Authorisierung und Logging aller Zugriffs-Events auf geschützte VMs ermöglicht.	**Sicherheits-Management über Cloud-Umgebungen hinweg** • Eine einheitliche Management-Plattform dient als zentraler Auditpunkt. Dieser bietet ein Dashboard, das auf einen Blick alle verschlüsselten und unverschlüsselten virtuellen Maschinen und Speicher-Volumes des Unternehmens zeigt. **Key-Lifecycle-Management auf höchstem Niveau** • Die einzige Lösung, die über ein Key-Management-System vor Ort in Form einer hochsicheren KeySecure-Appliance verfügt. Diese ist nach FIPS 104-2 Level 3 zertifiziert.

1. Installieren Sie den ProtectV Client auf Ihren VMs. Wählen Sie die Server und Speicher-Volumen aus, die Sie verschlüsseln wollen, und erstellen Sie Ihre Richtlinien.

2. Der ProtectV Manager ist eine virtuelle Maschine, die als AWS AMI oder als VM in einer VMware-Umgebung läuft. Sie konfigurieren den ProtectV Manager durch das Anlegen von Benutzern und Rechten.

3. KeySecure ist eine notwendige Komponente, um das Schlüsselmaterial der VMs in Hardware zu sichern. Installieren Sie KeySecure vor Ort als „Root of Trust" zum Management der Lebenszyklen aller Arten von Keys über Ihre Rechenzentren, privaten und öffentlichen Clouds hinweg.

Technische Spezifikationen

Unterstützte Plattformen

- Amazon Web Services EC2
- Amazon VPC
- VMware vCenter

Unterstütze Betriebssysteme

- Microsoft Windows Server 2003 R2 32 Bit
- Microsoft Windows Server 2003 R2 64 Bit
- Microsoft Windows Server 2008 32 Bit
- Microsoft Windows Server 2008 64 Bit
- Microsoft Windows Server 2008 R2 64 Bit
- Linux CentOS 5.6 32 Bit
- Linux CentOS 5.6 64 Bit
- Linux SUSE Server 10 SP4, 64 Bit
- Linux SUSE Server 11 SP1, 64 Bit
- Red Hat Enterprise Linux (RHEL) 5.5 64 Bit
- Red Hat Enterprise Linux (RHEL) 5.6 32 Bit
- Red Hat Enterprise Linux (RHEL) 5.6 64 Bit
- Red Hat

ProtectV Client: Unterstütze Browser

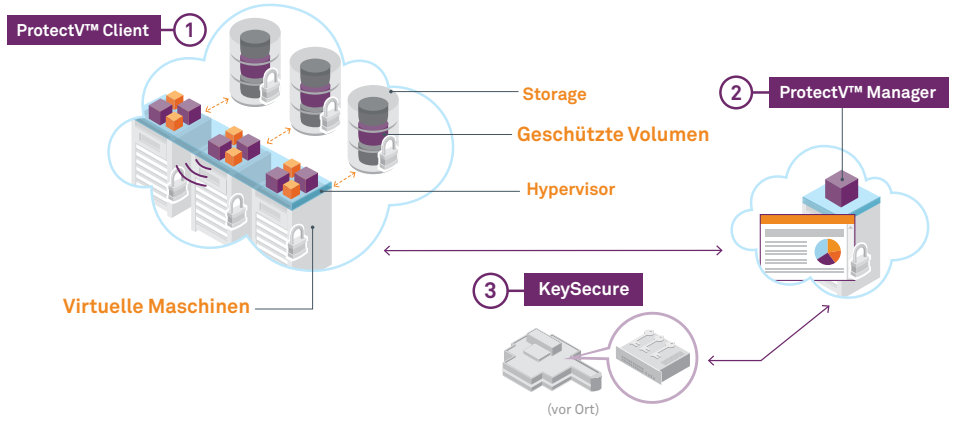
- Internet Explorer
- Firefox
- Google Chrome

Supported SafeNet Enterprise Key Management Products

- SafeNet KeySecure k460
- SafeNet KeySecure k150
- SafeNet DataSecure i450
- SafeNet DataSecure i150

So funktioniert ProtectV

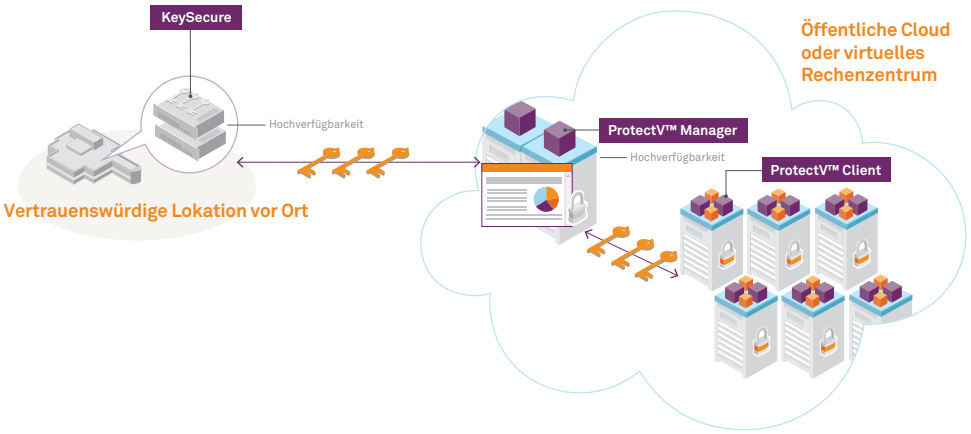
ProtectV sichert Daten, die gesetzlichen Regelungen unterliegen, auf VMs und Speicher-Volumen in virtuellen Rechenzentren sowie öffentlichen und privaten Clouds.



Einführungsszenarien

Egal, ob die Daten in einer virtuellen Umgebung wie VMware vCenter gespeichert sind oder ob sie in öffentlichen oder in privaten Clouds wie Amazon Web Service EC2/EBS und Amazon VPC liegen: Der ProtectV Manager kann einfach mit Hilfe von vorgefertigten Images eingeführt werden. ProtectV verfügt über eine benutzerfreundliche Web-Oberfläche, über die Richtlinien, Benutzer und Rollen bearbeitet werden. Auch das System-Monitoring und Event-Management erfolgt über diese GUI. Zudem bietet die Lösung APIs zur Automation und zur Integration in Provisionierungssysteme für virtuelle Server sowie CLIs für Scripting. Das sorgt für bessere Agilität und schnelles Provisionieren.

Einführungsszenarien für ProtectV in virtuellen Rechenzentren sowie öffentlichen und privaten Clouds



Öffentliche Cloud oder virtuelles Rechenzentrum

Lösungen zur Virtualisierungs- und Cloud-Sicherheit müssen, wie alles im Bereich der Unternehmenssicherheit, in einem mehrstufigen Ansatz entsprechend dem Lebenszyklus des Informationsschutzes verwaltet werden. Dieses verbindet Verschlüsselung, Zugriffsrichtlinien, Key-Management, Content-Security und Authentisierung. Die Schichten müssen in ein flexibles Framework eingebettet sein, mit dem das Unternehmen sich seinen Risiken anpassen kann. Egal, wo sich die Daten befinden: SafeNet bietet ganzheitliche Verschlüsselung für strukturierte und unstrukturierte Daten. SafeNet verfügt über ein praxisorientiertes Framework, das Unternehmen beim Umzug von Daten, Anwendungen und Systemen in virtuelle Umgebungen oder Clouds das bietet, was sie brauchen: Vertrauenswürdigkeit, Sicherheit und Compliance.

Kontakt: Alle Niederlassungen und Kontaktinformationen finden Sie im Internet unter **www.safenet-inc.com**
Folgen Sie uns: www.safenet-inc.com/connected