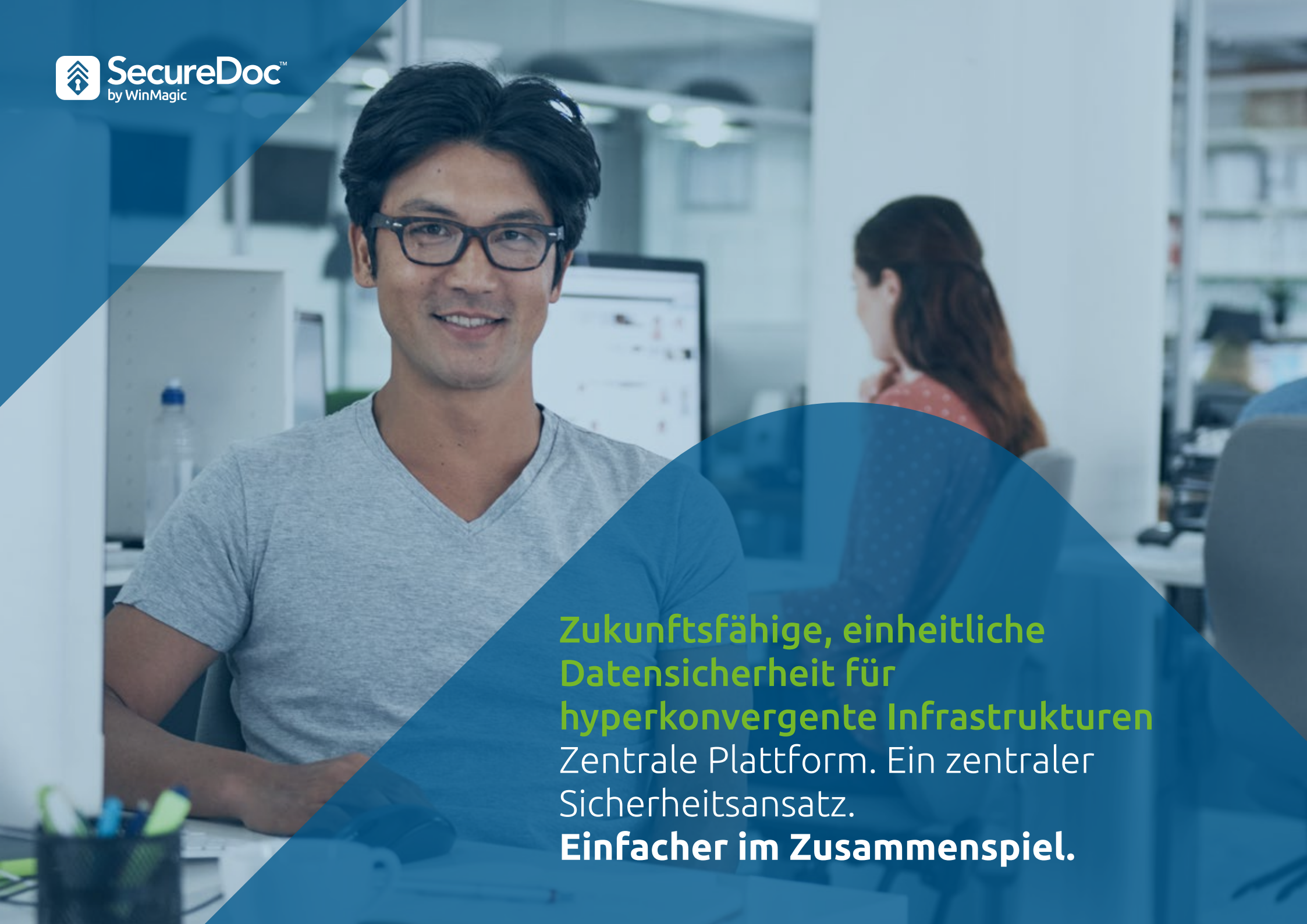


SecureDoc™ by WinMagic

Zukunftsfähige, einheitliche Datensicherheit für hyperkonvergente Infrastrukturen

Zentrale Plattform. Ein zentraler Sicherheitsansatz.

Einfacher im Zusammenspiel.

Die steigende Datenverbreitung ist der große Feind der Datensicherheit und Compliance.

Für IT-Experten bedeutet das mehr Druck und eine nie dagewesene Komplexität. Die Art und Weise, auf die Daten erstellt und bewegt werden, ändert sich heute sehr schnell. In der Folge entstehen neue Sicherheitslücken, die selbst versierte IT-Manager nur schwer schließen können. Die Zahl der Herausforderungen nimmt ebenso zu wie ihre Vielfalt.

Das weltweite Datenvolumen wird EMC-Experten* zufolge bis 2020 um das Zehnfache auf 44 Zettabyte steigen. Gleichzeitig gibt es auch immer mehr Clouds und Geräte, sodass Unternehmensdaten heute mehr verbreitet sind als jemals zuvor und nur schwer kontrolliert werden können. Hinzu kommen sich ständig ändernde Anforderungen an den Datenschutz und die Compliance. Veraltete Sicherheitslösungen stoßen hier an die Grenzen ihrer Leistungsfähigkeit.

Vorausdenkende IT-Experten setzen daher zunehmend auf moderne, hyperkonvergente Infrastrukturlösungen, um der komplexen Verwaltung und IT-Silos ein Ende zu setzen. Damit einher geht jedoch eine weitere Herausforderung für IT-Manager: Wie lassen sich diese neuen Lösungen am besten schützen?

*EMC Digital Universe und Untersuchungsergebnisse von IDC, „The Digital Universe of Opportunities: Rich Data and the Increasing Value of the IoT“, April 2014, VMware „Balancing Freedom and Control: Evolution of Cloud – 2006–2030“, Oktober 2016

Einheitliche Datensicherheit ist ein Muss.

Eine einfache, konvergente IT benötigt eine einfache, einheitliche Sicherheit.

Alle physischen, cloud-basierten und virtuellen Workloads mit einer unternehmensweiten Strategie für die Verschlüsselung und die Schlüsselverwaltung zu schützen, klingt kompliziert, muss es aber nicht sein. Sie benötigen lediglich SecureDoc CloudVM von WinMagic, um den Wunsch eines jeden IT-Managers nach einer richtliniengesteuerten, portablen Datensicherheit mit einfacher Schlüsselkontrolle wahr werden zu lassen.

Alle Workloads werden zuverlässig geschützt – und zwar unabhängig von deren Speicherort, der Art der Übertragung in der hyperkonvergenten Infrastruktur oder des Geräts, über das auf die Daten zugegriffen wird.

- **Konsistent:** Die Schlüsselkontrolle für alle Plattformen, Konten und internationalen Jurisdiktionen erfolgt über eine zentrale Management-Konsole.
- **Kontinuierlich:** Alle Workloads bleiben stets verschlüsselt und die Verschlüsselungs-Keys bleiben sogar während der Übertragung gesperrt.
- **Konform:** Compliance-Anforderungen durch die neue EU-DSGVO bis hin zu HIPAA, PCI-DSS und anderen (künftigen) Standards werden durch den Schutz der Workloads einfach eingehalten. Zudem wird die Nutzung von Daten durch unberechtigte Personen verhindert, und Audit und Berichterstellung werden zum Kinderspiel.

Volle, ständige Kontrolle

FROM ENDPOINT TO CLOUD AND EVERYTHING IN BETWEEN

NUTANIX vmware SCALE COMPUTING CITRIX Microsoft Hyper-v amazon web services Microsoft Azure IBM Cloud Google Cloud Platform

Moderne Cloud-Sicherheit für hyperkonvergente Systeme

Hyperkonvergente Infrastrukturen überzeugen durch eine unkomplizierte Verwaltung und hohe Agilität. Diese Vorteile spiegeln sich in der einfachen, einheitlichen Cloud-Sicherheit von SecureDoc CloudVM wider.

Schutz von Workloads vor externen und internen Bedrohungen

- Eine Verschlüsselung auf der Ebene virtueller Maschinen senkt die Kosten und die Komplexität im Vergleich zur Verschlüsselung auf Hardware-Ebene.
- PBConnex, die WinMagic-Lösung für die Authentifizierung vor dem Systemstart, sorgt für die Authentifizierung von VMs über einen Remote-Management-Server. Dies geschieht, noch bevor vertrauliche Daten in der VM geladen werden, damit weder Schlüssel noch Daten offengelegt werden.
- Die Schlüsselverwaltung erfolgt getrennt vom Hypervisor, damit das Unternehmen jederzeit die volle und alleinige Kontrolle über die Schlüssel behält. So sinkt das Risiko einer Offenlegung gegenüber Unbefugten um ein Vielfaches.
- Die Schlüsselverwaltung lässt sich über eine virtuelle Appliance für Cloud-Service-Anbieter realisieren, die ganz einfach bereitzustellen ist.

• Automatisierung von DevSecOps

- VM-Vorlagen können bei laufender Verschlüsselung erstellt und verschlüsselte VMs bereitgestellt werden.
- Sicherheitsteams sind für die Verwaltung aller Sicherheitsaspekte zuständig, damit Entwickler keine Einstellungen verändern oder unverschlüsselte Workloads hochladen können.

Größtmögliche Flexibilität bei der Bereitstellung

- Verschlüsselte VMs können für Hochverfügbarkeitslösungen ohne Kompatibilitätsprobleme bereitgestellt werden.
- Es werden mehrere Abonnement-IDs von Azure und AWS unterstützt.
- Die Verschlüsselung mehrerer Festplatten (Volumes) ist möglich.

Durchsetzung von Vorschriften zur Datenhoheit und Data Governance

- Die betrieblichen Grenzen von VMs und andere Parameter wie Klon-Kontrolle, IP-Sperren sowie geografische und zeitzonenbasierte Zugriffsbeschränkungen lassen sich detailliert festlegen.

Übertragbarkeit und cloud- und cluster-unabhängige Umgebung

- Workloads können ohne Entschlüsselung und erneute Verschlüsselung beim Klonen, Verschieben oder Replizieren von VMs/Laufwerken frei bewegt werden.
- Daten auf nicht mehr benötigten virtuellen Instanzen werden dank SecureDelete (Löschen verschlüsselter Daten) geschützt, indem die Verschlüsselungs-Keys entfernt werden, um künftige Zugriffe zu verhindern.

Transparenz für die Cloud

- Hochverfügbarkeit, Migration, Klonen und Schnappschüsse werden unterstützt und VMs bleiben in allen Clouds verschlüsselt.

Unterstützung mehrerer Plattformen (Windows und Linux)

- Windows Server 2008 R2, 2012, 2016, Windows 7, 8, 8.1 und 10, Red Hat 7.2 und 7.3, CentOS 7.2 und 7.3, Ubuntu 14.04 und 16

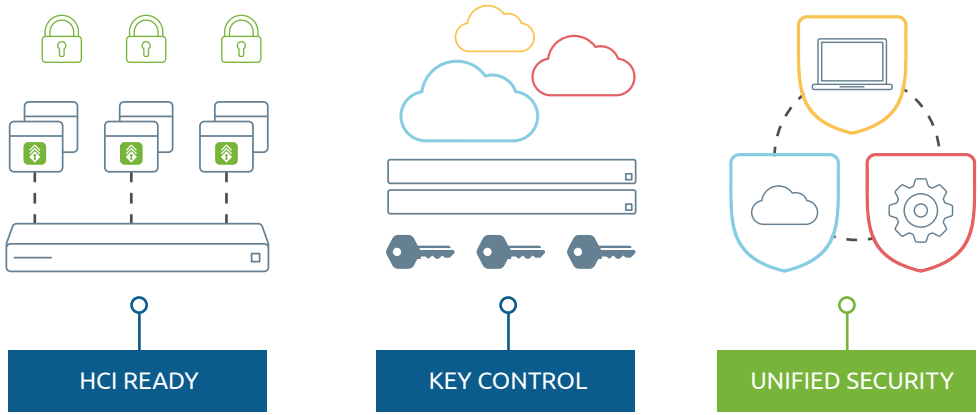
Compliance, Skalierbarkeit und Kosten

Unkomplizierte Verwaltung mehrerer VMs

In virtualisierten Umgebungen ist der Zugriff auf VMs deutlich leichter. Das bedeutet aber auch, dass IT-Mitarbeiter weniger Kontrolle haben, was wiederum allerlei Gefahren mit sich bringt. SecureDoc CloudVM von WinMagic läuft auf der Enterprise-Cloud-Plattform von Nutanix und auf der HC3-Plattform von Scale Computing und bietet somit umfassenden VM-Schutz:

- **Schutz** von Workloads vor Datenmissbrauch und unbefugtem Zugriff mithilfe durchgehender Verschlüsselung auf VM-Ebene für alle virtuellen Maschinen in virtualisierten Umgebungen. So bleibt Ihr Unternehmen geschützt, ganz gleich, wo sich die VMs befinden und ob sie aktiv genutzt, inaktiv und offline sind oder als Backup fungieren.
- **Dauerhafte Workload-Verschlüsselung** beim Verschieben von Cluster zu Cluster und von Cloud zu Cloud.
- **Support** von hybriden und Multi-Cloud-Umgebungen.
- **Authentifizierung vor dem Systemstart** mit SecureDoc zur Kontrolle des Datenzugriffs und zur Authentifizierung neuer Workloads.

Unkomplizierte Sicherheit für Clouds und Rechenzentren



Sorgenfreies Verschieben von Daten

Verwaltung von Umgebungen mit Hard- und Software-Verschlüsselung

Die Hardware-Verschlüsselung kommt üblicherweise für gespeicherte Daten zum Einsatz. Allerdings bietet dieses Verfahren nur einen eingeschränkten Schutz und ist kostspielig in der Verwaltung. Die software-basierte Verschlüsselung auf VM-Ebene zusätzlich zur hardware-basierten Sicherheit bietet noch mehr Schutz für transiente Workloads.

- **Schutz** verloren gegangener und gestohlener Laufwerke, vor der Nutzung von Daten durch Unberechtigte, Ausuferung von Daten usw. durch Schutz auf VM-Ebene
- **Verschieben** von Workloads auf Hardware und in der Cloud bei durchgehender Verschlüsselung und mit einer zentralen Verschlüsselungslösung für unternehmensweite und öffentliche Cloud-Plattformen
- **Keine Anbieterabhängigkeit** für Hardware, Hypervisoren oder Clouds sowie Übertragbarkeit: Daten werden überall zuverlässig geschützt.
- **Geschlossene** Sicherheit für lokale, cloud-basierte und Remote-Backups
- **Kosteneinsparungen** durch Vermeidung von Hardware-Ersatz und Upgrade auf selbstverschlüsselnde Laufwerke (SEDs). Stattdessen Verschlüsselung auf VM-Ebene und intelligente Schlüsselverwaltung mit einer zentralen Lösung.
- **Sicherheit** beim Stilllegen von Workloads und Laufwerken – agiler Betrieb und Beibehaltung anderer Datensätze

Das Beste aus zwei Welten

Der einfache Weg zur besseren Compliance

Eine cloud-unabhängige, kontinuierliche Verschlüsselung für alle VMs verschafft Ihnen viele Vorteile in Bezug auf die Compliance. Aber sind Ihre Daten wirklich geschützt, wenn auch andere Personen im Besitz der Verschlüsselungs-Keys sind? Bei SecureDoc CloudVM erfolgt die Schlüsselverwaltung getrennt vom Hypervisor, damit das Unternehmen jederzeit die volle und alleinige Kontrolle über die Schlüssel behält.

Außerdem bietet SecureDoc CloudVM benutzerfreundliche Audit-Tools, anhand derer ersichtlich wird, wo sich die Schlüssel befinden und welche Daten geschützt sind. Durch zentrale Dashboards und aussagekräftige Sicherheitsdaten werden Compliance-Verstöße verhindert. Möglich ist dies durch die Nachverfolgung und Berichterstellung der allzeit geschützten VMs und Daten in Ihrer konvergenten Umgebung. So werden die Einhaltung der Compliance und der Nachweis dieser Einhaltung im Falle eines Datenverlusts deutlich vereinfacht.

SecureDoc CloudVM beinhaltet zudem eine Überwachung und detaillierte Berichterstellung für Endpunkte – vom Verschlüsselungsstatus bis hin zur fehlgeschlagenen Authentifizierung. So lässt sich die Compliance für die gesamte Unternehmensinfrastruktur ganz einfach durchsetzen.

- **Verbesserte, detaillierte Kontrollmöglichkeiten**, um den Zugriff, die gemeinsame Nutzung, das Klonen und das Replizieren von VMs festzulegen
- **Verwendungskontrolle** für mehrere Standorte (Zeit, Standort, Duplizierung)
- **Vermeidung** des Risikos einer Offenlegung von Schlüsseln gegenüber Unbefugten
- **Unterstützung** der Hochverfügbarkeit von SecureDoc Enterprise Server (Schlüsselverwaltung), damit Schlüssel zum Entsperren von VMs immer verfügbar sind
- **Umfassende Remote-Verwaltung** für IT-Administratoren und Bereitstellungsmöglichkeiten über die Konsole von SecureDoc Enterprise Server (SES)
- **Zeitgleiches Anzeigen aller VMs**, Workloads und Cloud-Instanzen, um geschützte VMs zuverlässig zu erkennen

Unkomplizierte Data Governance

Agilität und Skalierbarkeit leicht gemacht

Der moderne Markt ist hart umkämpft. Probleme mit veralteter IT dürfen sich nicht auf wichtige Geschäftstätigkeiten auswirken. Die cloud-unabhängige, kontinuierliche Verschlüsselung von SecureDoc CloudVM erlaubt es, Workloads jederzeit überall hin zu verschieben, ohne dabei den Geschäftsbetrieb zu beeinträchtigen.

In Bezug auf die Virtualisierung besticht SecureDoc CloudVM durch hohe Skalierbarkeit. So lassen sich Lizenzen einfach bereitstellen. Das Unternehmenswachstum wird unterstützt – ganz unabhängig von Ausmaß und Geschwindigkeit der Veränderungen. Workloads lassen sich sicher und vorschriftsmäßig über mehrere Plattformen und Clouds hinweg verschieben. Darüber hinaus können ältere Anwendungen sicher in eine Cloud migriert werden, wo sie sich flexibel und kostengünstig skalieren lassen.

Die Bereitstellung erfolgt schnell und ohne Ausfallzeiten bei der Online-Verschlüsselung für virtuelle Maschinen unter Windows oder Linux.

CLOUD-AGNOSTIC

ALWAYS-ON

SNAPSHOTS/CLONES

Mehr Agilität für Unternehmen

Einfache Strategie zur Senkung von Betriebskosten

Die IT steht zunehmend unter Druck, die Effizienz von Technologien, Systemen und auch Anwendern zu steigern und IT-Silos durch eine hyperkonvergente Infrastruktur zu ersetzen.

Durch eine solche Infrastruktur sind Unternehmen in der Lage, ihre Betriebskosten zu senken. Mit SecureDoc CloudVM wird sichergestellt, dass die so erzielten Kosteneinsparungen erhalten bleiben. Die WinMagic-Lösung reduziert die Betriebskosten, und eine Verschwendung wichtiger IT-Ressourcen wird vermieden, da der Aufwand deutlich geringer ist als bei anderen Verschlüsselungslösungen. SecureDoc CloudVM besticht durch eine einzigartige Performance. Verschlüsselungsprozesse wirken sich weder auf Ihre Systeme noch auf Ihre IT-Mitarbeiter aus.

- **Schnelle** Bereitstellung von VMs, enorme Zeit- und Kosteneinsparungen
- **Kürzeste** Umwandlungszeiten auf dem Markt
- **Vollständige Umwandlung** für Online- und Offline-VMs

Mehr Budget für die Innovation

Einfacher im Zusammenspiel

Schützen Sie Ihr Unternehmen zuverlässig und setzen Sie auf eine hyperkonvergente Strategie mit kontinuierlicher Verschlüsselung – und zwar jetzt!

Mit SecureDoc CloudVM können Sie die Vorteile hyperkonvergenter Systeme ganz ohne Sicherheitsbedenken nutzen. So behält Ihre IT die ständige Kontrolle über die Datensicherheit in der gesamten konvergenten Infrastruktur und wird zuverlässig vor Datenverlusten durch unberechtigte Kopiervorgänge und Schnappschüsse, Datenumzug, der Nutzung öffentlicher Clouds und der Nachlässigkeit von Mitarbeitern sowie vor anderen Bedrohungen geschützt.

Die preisgekrönten WinMagic-Lösungen werden von führenden Plattformen für hyperkonvergente Systeme wie z. B. Nutanix und Scale unterstützt.

Wussten Sie schon?
Dem unabhängigen Branchenbeobachter BreachLevelIndex.com zufolge waren nur vier Prozent aller weltweiten, seit 2013 gemeldeten Datenschutzverletzungen Sicherheitsverstöße, bei denen die entwendeten Daten verschlüsselt und somit unbrauchbar waren. Seit 2013 wurden über 9 Mrd. Datensätze weltweit gestohlen oder sind verloren gegangen.

NUTANIX READY • AHV •

SCALE COMPUTING

Sprechen Sie uns an, wenn Sie die hyperkonvergente Infrastruktur in Ihrem Unternehmen fit für die Zukunft machen möchten. **Zentrale Plattform. Ein zentraler Sicherheitsansatz. Einfacher im Zusammenspiel.**

USA und Kanada +1 888 879 5879 | **Vereinigtes Königreich** +44 (0)148 334 3020 | **Deutschland** +49 (0)69 175 370 530 | **Japan** +81 (0)3 5403 6950 | **Indien** +91 124 4696800 | **APAC-Singapur** +65 9634 5197

WINMAGIC®