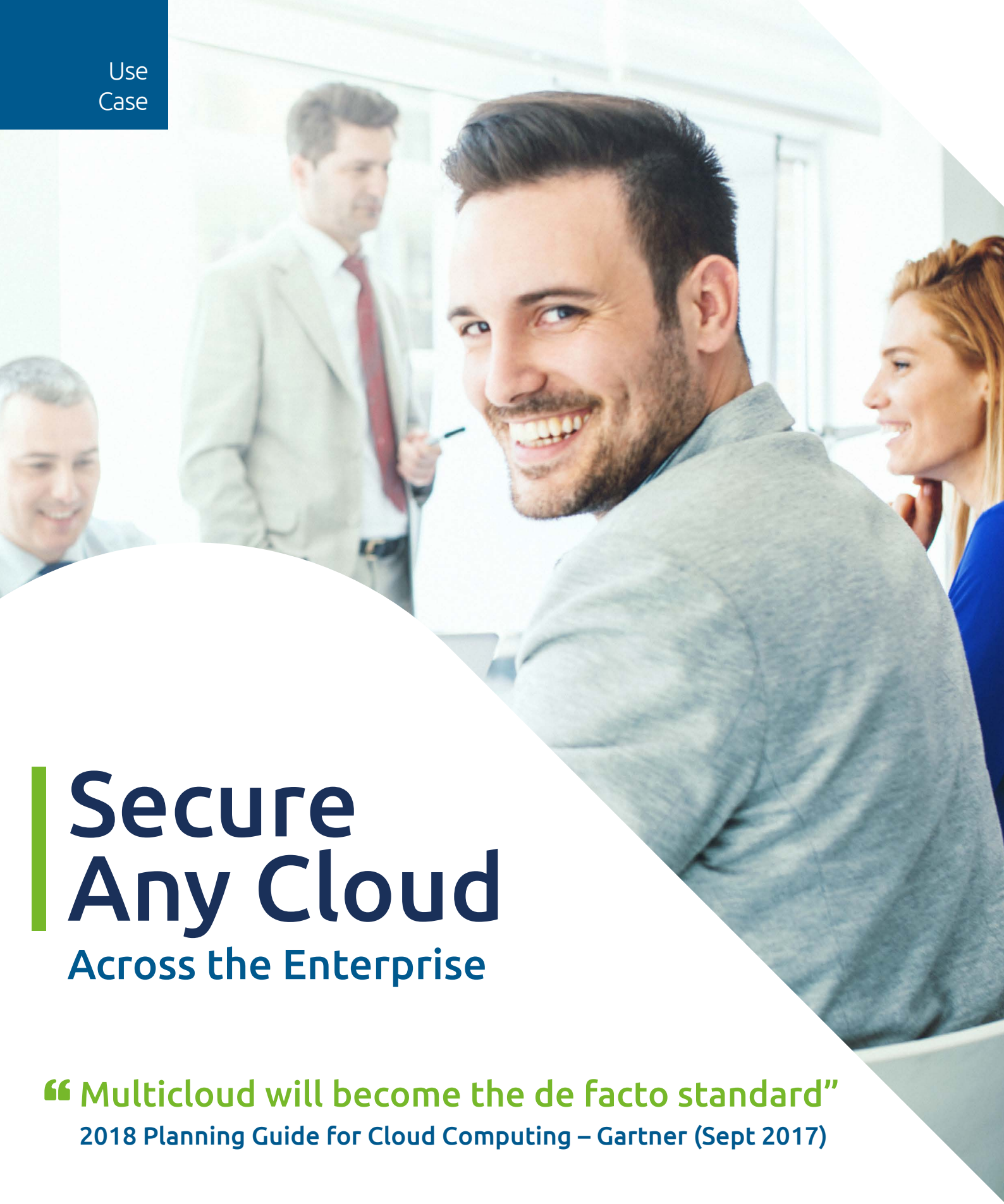
Use Case



Secure Any Cloud

Across the Enterprise

> “Multicloud will become the de facto standard”
>
> 2018 Planning Guide for Cloud Computing – Gartner (Sept 2017)

SecureDoc™ by WinMagic

WINMAGIC®

Use Case

According to the Right Scale 2017 State of Cloud Report

85%

Of Enterprise have a multi-cloud strategy, with 95% running apps or experimenting with Infrastructure as a service.[1]

> Most organizations have a stated intention to standardize on at least two

IaaS

Providers, in addition to private cloud infrastructure, creating the need for solutions that support hybrid and heterogeneous cloud environments.[2]

Sources

1 2017 State of Cloud Report – Right Scale (2017)

2 Market Guide for Cloud Workload Protection Platforms – Gartner (Mar 2017)

The Move to Any Cloud Infrastructure

Servers are at the core of enterprise operations, delivering hundreds of applications – both internal and customer-facing – as well as databases, file sharing, websites and communications. Many choose to run these servers within a private datacenter virtualized with VMware, Hyper-V or Citrix Xen. Nevertheless, the era of cloud is here, and businesses can't afford to ignore the known advantages of infrastructure as a service (IaaS) solutions like Amazon Web Services, Microsoft Azure or Google Compute Engine. Meanwhile, hyper-converged infrastructure (HCI) solutions like Nutanix and Scale Computing are re-defining the private cloud, with hybrid integrations.

Demands to cut costs, automate operations and maximize agility have pushed many enterprises to move up the stack, out of their datacenter into on-demand public cloud IaaS. Hybrid IT has quickly become the standard, but IT leaders must start planning for multi-cloud strategies as a way for their enterprise to move cloud-ward without placing all their eggs in one basket.

Any Cloud Advantages

Optimize ROI
Every IaaS or hyper-converged solution offers distinct functionalities that may be the right fit for one app or business need, but not for another. Having a rich set of options optimizes use of workloads with different needs.

Reduce Risk
100% uptime is never guaranteed, but a multi-cloud strategy offers business continuity (BC) and disaster recovery (DR) models which can significantly reduce the risk of data loss and compliance failures.

Eliminate Lock-in
Smart businesses don't put all their eggs in one basket, even if that basket is their own datacenter or a reliable cloud service provider (CSP).

Use Case

Through 2020

95%

Of cloud security failures will be the customer's fault.[1]

> As a best practice, all data deployed in public clouds should be encrypted to avoid inadvertent access by the CSP or other tenants, and to help meet data residency and compliance requirements. It also ensures deletion of the data at the end of life by simply shredding the encryption keys.[2]

> However, with native IaaS KMaaS solutions, even with a BYOK approach, the root of trust is under the control of the CSP.[2]

Sources

1 How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center – Gartner (Oct 2017)

2 Hype Cycle for Cloud Security – Gartner (Jul 2017)

Business Need: **Unified Data Security, Not Silos**

Every cloud is built differently. Enterprises can leverage a range of different feature sets, functionality, pricing models and policies to optimize ROI and meet specific business unit needs. That said, security of each cloud is also built differently. Security and privacy, both top concerns for CISOs, can be easily disrupted by lack of standardization across cloud IaaS platforms. This especially rings true for encryption and key management, both core components of workload security.

In a multi-cloud environment, enterprises can spin up whatever resources they need without compromising choices, but at the same time, must use separate encryption solutions between IaaS platforms – all with little or no support for cross-cloud portability. Even worse, key management is often handled separately between different clouds, subscriptions and even different regions, creating siloes in policy framework and compliance.

The Problem: **Complex Hybrid IT**

As more and more businesses adopt multiple cloud solutions, it's clear that multi-cloud is the way forward. Traditional boundaries of virtualization continue to fade as the four walls of the datacenter collapse. Unfortunately, organizations adopting multi-cloud models find it increasingly difficult to secure their workloads in this new complex and distributed IT architecture.

Encrypting dedicated servers, virtual servers and cloud workloads is critical to mitigate risk and manage compliance. But the challenge of securing data and in today's complex IT stack can seem near impossible, considering:

Disparate Solutions
Just as each cloud is built differently, so is each data security solution – with different types of encryption, keys and policies to be managed. Problem is, too many solutions tied to different hardware, hypervisors and cloud providers creates gaps in security and a lack of overall visibility and control.

Lack of Control
Even in bring your own key (BYOK) models, the root of trust is still with the cloud service provider (CSP), leaving concerns about access, availability or compromise of keys. Furthermore, disparate key managers for each platform require different expertise, deployment and pricing models.

Vendor Lock-In
Encryption tied to any one vendor, hypervisor, or underlying hardware can undermine the benefits of cloud agility. Migration or failover of encrypted workloads between private or public clouds also becomes problematic.

Performance & Security Issues
Many available encryption solutions can't operate at the speed of the cloud, limited by the necessity to take data and applications offline during encryption, de-crypt and re-encrypt workloads as they traverse the network, or they are simply unable to encrypt all the data – including new and existing workloads.

The Solution: **Any Cloud Security with SecureDoc CloudVM**

Migrating data and applications to the cloud poses significant challenges for enterprises concerned about compliance, security, and control of data. Naturally, these concerns are magnified as workloads are deployed across complex hybrid and multi-cloud environments, all tied into a shared responsibility model where the enterprise is ultimately held responsible for protecting their data.

Whether you're virtualizing or converging your private infrastructure, moving up the stack into the cloud, or building out a multi-cloud strategy, WinMagic can help. SecureDoc CloudVM encrypts and locks down workloads, regardless of the infrastructure they run on, maintaining encryption from cloud to cloud, all under one platform. Keys are held by the enterprise, not the cloud providers – giving full control to protect data and monitor compliance.

Transition to Multi-Cloud

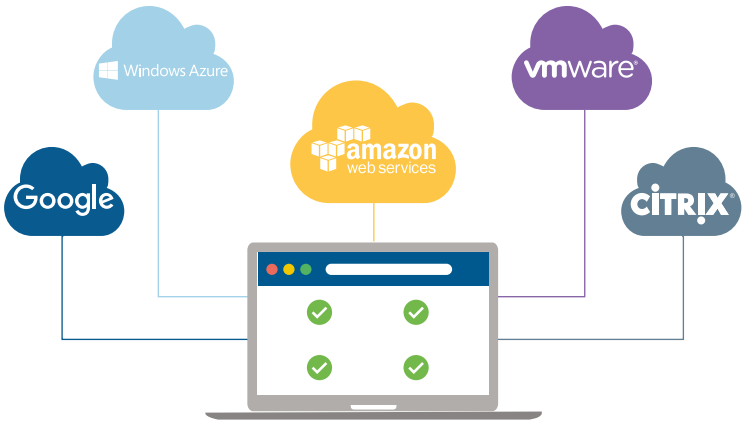
Discover and secure workloads wherever they run with persistent, always-on encryption that travels with your VMs from cloud to cloud and protects all data-at-rest – including the OS, data volumes, images and even snapshots.

Break Down Siloes

Reduce the need for multiple, disparate encryption solutions. Store, distribute and revoke encryption keys for workloads across multiple clouds, accounts and regions – all from a single console controlled within your enterprise.

Simplify Compliance

Reduce compliance burdens with a single dashboard to monitor, report and respond to workload security status across private, public and hyper-converged platforms – radically simplifying audits and ongoing risk management.



Take Back Control

Ensure that workloads only run when and where you want with policy-driven security including time-based access restrictions, clone controls, geo-location and IP-blocking policies to reduce data sprawl and unauthorized access.

Automate & Enforce Security

Security admins can automate and script encryption to facilitate a data protection by default strategy with the ability to remotely enforce policy control on-premise.

Secure with Speed

Deploy and protect workloads with encryption optimized for the speed of the cloud – all without the need to take data and applications offline or decrypt and re-encrypt workloads when they move.