McAfee
Together is power.

How secure is your private cloud?

Most workloads are already implemented in private clouds.[1]

Where Workloads Are Implemented

Cloud Service Provider (Off-Premises)

Private Cloud (On-Premises)

100%

0%

64% of enterprise apps are virtualized

68% are kept in an enterprise-managed data center

Where the Majority of Workloads Are Implemented

Traditional Apps

Virtualized Apps

100%

How Workloads Are Implemented
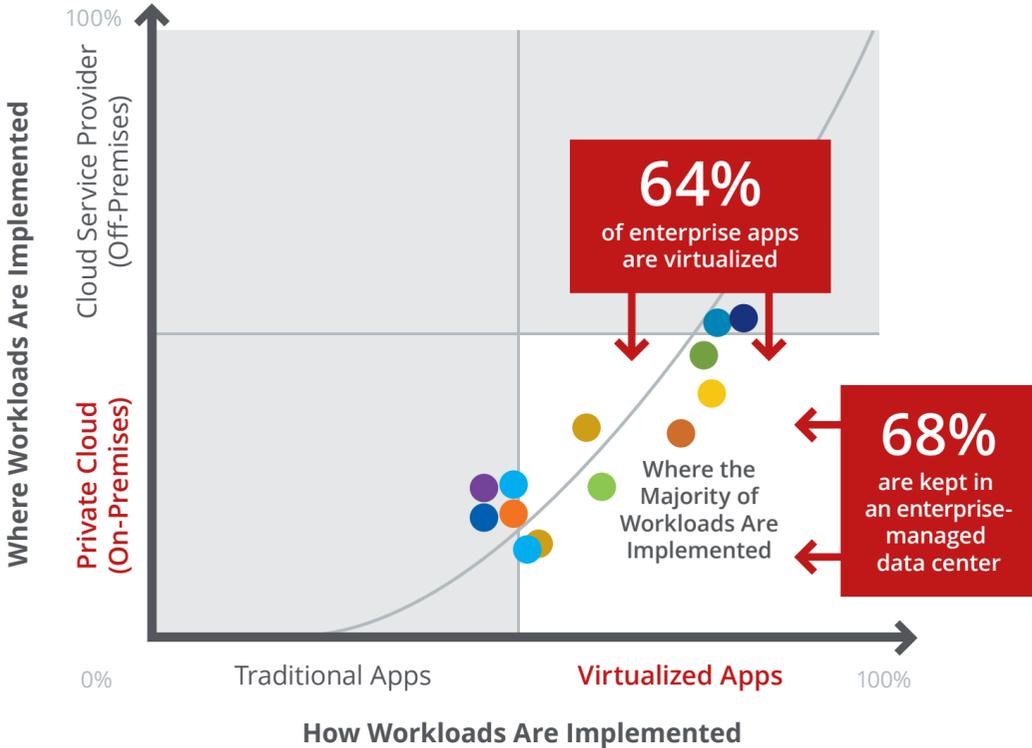
Private cloud security remains a major concern.

50%
of enterprise IT decision makers are concerned about sensitive data breaches in their private clouds.[2]
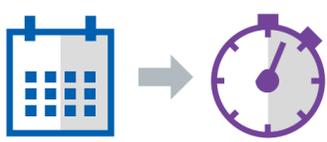
63%
of CISOs don't completely trust private clouds to keep their data secure.[2]

Software-Defined Data Center (SDDC) is the best option for architecting a private cloud.
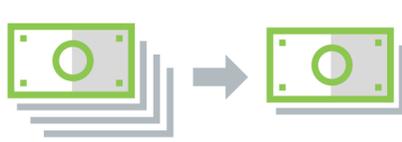
Increase Agility

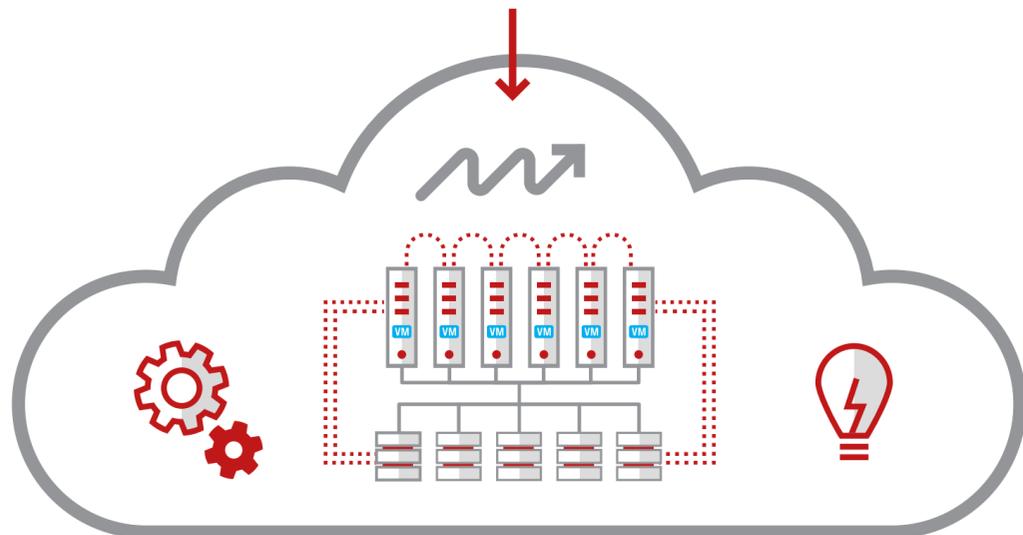Deploy new revenue-generating apps in minutes, not weeks.

Reduce CapEx and OpEx

Reduce costs up to 75% vs. traditional infrastructure.[3]

End-to-End Visibility & Policy-Based Orchestration Across Private Clouds

How do you secure the SDDC?

Ensure security is built into the SDDC architecture.

A core security strategy is an integral aspect of the entire SDDC architecture solution.
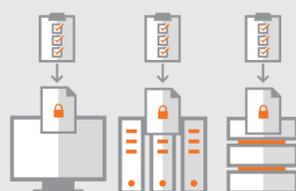
Utilize integrated security solutions.

Extend visibility, control, and threat protection from the SDDC to the cloud.

Deploy a software-defined security model.

Leverage automation, orchestration, and dynamic scalability to manage security across the entire infrastructure.

To learn more, visit:
www.mcafee.com/privatecloudsecurity

McAfee
Together is power.

1. Flash Forward: Moving Critical Workloads to Engineered Systems, The Aberdeen Group 2015, http://goo.gl/DLzHX5

2. Vanson Bourne, on behalf of Intel Security, conducted a survey of 1200 IT decision makers responsible for cloud security, across 8 countries (June 2015).

3. VMWare, Global Financial Institution Selects Software-Defined Data Center http://goo.gl/3DyZ9T. Circumstances will vary. McAfee does not guarantee any costs or cost reduction.