The Why, the What and the How of the Software-Defined Data Center

An Osterman Research Executive Summary

Published May 2017

McAfee™   vmware®

EXECUTIVE SUMMARY

The Software-Defined Data Center (SDDC) is an overarching philosophy for implementing better data centers. The most basic way to think about an SDDC is as a combination of virtualized computing resources, plus software-defined storage and networking. In addition, SDDC often includes overarching security aspects: in other words, SDDC abstracts and automates all the compute, storage and networking aspects that are traditionally physical, and it can put that automation and abstraction to use in enhancing security.

Building on virtualization, SDDC combines software-defined networking (SDN) and software-defined storage (SDS). In practice, SDDC is a useful way to think about building a virtualized data center – e.g., a private cloud or a hybrid cloud. Indeed, most large-scale public cloud providers use some flavor of SDDC philosophy, helping them to keep costs down.

Our research found that the vast majority of servers are already running virtualized today, while roughly one-half of organizations are either planning to transform their data center(s) into SDDCs or they have already done so. Among those planning to transition their data center(s) to SDDC, most are planning to do so within the next two years.

WHY SDDC?

Our research found that most organizations are interested in moving to SDDC in order to improve the performance of their operations, but security is also a primary consideration for most organizations. Other common drivers include reducing expenditures, reducing complexity, and enabling improved control. The top three drivers for moving to SDDC are shown below:

Reasons That Organizations Want to Move to an SDDC

Improve performance	**57%**
Improve security	**53%**
Reduce capital expenditures	**47%**

Source: Osterman Research, Inc.

THE BUSINESS BENEFITS OF SDDC

SDDC offers a number of important business benefits:

*   **Improved speed and productivity of IT staff**
    By its very "software-defined" nature, an SDDC is easier to configure, reconfigure, and keep secure (given the proper tools), resulting in IT operations that are more responsive to change and more efficient. Moreover, SDDC also permits frequent service updates and rapid standup/teardown of test environments.

*   **Improved security**
    SDDC allows centralization of the control and management of virtualized data-center components and makes them more visible to IT operations. Centralization and visibility are inherent in SDDC's software-defined nature, and this is key to consistent and rigorous security. SDDC contrasts with traditional data-center operations, where rules are distributed across a range of devices and are dependent upon fragile physical topologies. By contrast, in an SDDC world consistently-enforced policies act on logical, abstracted characteristics of the

workload and its data, not on frangible, physical characteristics that will inevitably become out of date.

- **Improved reliability**
  Traditional IT operations are inherently error-prone, even when using a centralized management console. SDDC's ability to automate operations reduces repetitive tedium and error, which in turn maximizes security and minimizes *unplanned* downtime.

- **Improved utilization of hardware**
  Virtualization increases the utilization of hardware, allowing organizations to make more efficient use of their capital expenditures. For example, it allows several workloads to share software-defined computing and software-defined storage resources. Moreover, SDDC unifies networking functions that traditionally are segregated into separate boxes and it unifies storage array roles.

- **It enables an interoperable cloud**
  SDDC helps organizations realize the inherent benefits of hybrid clouds and without vendor or technology lock-in. The combination of automation, abstraction, visibility and control tends to bring consistency, which will ease the placing of workloads into public or private clouds to an even greater extent than virtualization alone will permit.

SDDC ENABLES BETTER SECURITY

There are some important things to keep in mind about security in SDDC environments:

- Moving to an SDDC doesn't suddenly change the nature of security threats, nor the human expertise required to assess those threats and their risks. However, SDDC no longer locks security into a physical point on the network, since the virtual machine platform abstracts the networking and security capabilities away from the underlying hardware platform.

- A key security advantage of SDDC is that the virtual machine platform can oversee all the behaviors of the workloads they manage – not just within a virtual machine, but *between* them, allowing the virtual machine platform and the security software to watch behavior *in context*.

- Moving intelligence up the stack brings benefits to security software from being closer to the workloads, and results in key advantages to improve the security software's view of data at rest and data in transit.

- Being closer to the workloads allows security software to better protect against denial-of-service attacks, malicious attempts to break out of the virtual machine, geographic access-control violations, and other problems.

- SDDC allows inspection of potential threats based on behavioral information that is rarely available in a conventional data center, it makes it easier to connect to external threat-intelligence networks, and to run real-time forensic examination of potential threats inside a "throw-away" virtual environment.

THE BOTTOM LINE

SDDC can significantly improve an organization's security posture; reduce its IT, capital expenditure and operating costs; increase its overall network and application reliability; and enable greater flexibility as organizations migrate to public, private or hybrid clouds.