Paper

Bitdefender®

Delivering Strong Security in a Hyperconverged Data Center Environment

Introduction

A new trend is emerging in data center technology that could dramatically change the way enterprises manage and maintain their IT infrastructures. It's called hyperconvergence, and it's gaining momentum as companies look for ways to run more efficient and agile technology environments.

Indeed, early adopters of hyperconverged data centers are already reporting benefits such as cost savings, improved data protection, greater scalability and easier management of their IT environment.

The idea of hyperconvergence is to simplify operation and management of data centers by converging the computing, storage and networking components into a single, software-driven appliance.

It's defined as an IT infrastructure framework in which storage, virtualized computing and networking are tightly integrated within a data center. The software-based architecture that is the centerpiece of hyperconvergence is what makes the integration possible.

In a hyperconverged environment, all of the servers, storage systems and networking equipment are intended to work together through the appliance. The simplification comes from the fact that the technology providing the hyperconverged capability comes from a single vendor.

The idea of hyperconvergence emerged from the concept of converged infrastructures, in which a pre-configured package of software and hardware delivers simplified management of data center components. In a converged infrastructure, the components are discrete and can be separated. But in a hyperconverged data center, the components are integrated so closely that they cannot be separated.

As with so many technological developments of recent years, the emergence of hyperconvergence introduces cyber security issues, challenges and opportunities for organizations. IT, security and business leaders at enterprises need to get up to speed on security in the age of hyperconvergence before launching any major initiatives in this area.

This white paper examines the growing move toward the hyperconverged data center, explores issues related to cyber security and hyperconvergence, and presents solutions and best practices for ensuring data protection in this new environment.

The Growing Hyperconvergence Movement

The emergence of the hyperconverged data center could reshape business—in a favorable way. So it should come as no surprise that the market for hyperconvergence technology is growing.

According to data from research firm Gartner Inc., the market for hyperconverged integrated systems (HCIS) will jump 79% to nearly $2 billion in 2016, bringing the technology into mainstream use within five years. Gartner said HCIS will be the fastest-growing part of the overall market for integrated systems, totaling nearly $5 billion by 2019 and accounting for about a quarter of the market.

A report released by International Data Corp. (IDC) in 2016 offers different numbers but also predicts growth for the market. It says the worldwide converged systems market, including hyperconvergence, increased revenue 11% year over year to $2.5 billion during the first quarter of 2016. The market generated 1,367 petabytes of new storage capacity shipments during the quarter, up 36% from the same period a year earlier.

"End users within the mid-market and even in the outer edge of the enterprise data center continue to prioritize simplicity in all aspects of the user experience," IDC said. "This is at the heart of the rapid growth rate within hyperconverged systems."

In a September 2016 report, 451 Research noted that adoption of converged infrastructure is changing IT environments and the personnel who manage it, and that 40% of enterprises use a hyperconverged infrastructure. The firm based its findings on a survey of more than 750 IT professionals worldwide in July and August 2016.

"Hyperconverged infrastructure represents the next evolutionary step of standard converged infrastructure," the firm stated in its quarterly Voice of the Enterprise survey of IT buyers. Analysts at 451 Research expect the percentage of organizations using hyperconvergence to rise substantially over the next two years.

Nearly a quarter of the organizations 451 surveyed indicated they have hyperconverged infrastructure either in a pilot phase, or in plans for future adoption. Hyperconverged infrastructure is evolving from a supportive, edge infrastructure to a primary component of today's IT organizations, the report said. The survey showed that 74% of organizations currently using hyperconverged infrastructure are using the solutions in their central data centers.

Loyalties to traditional, standalone servers are diminishing in today's IT environments as companies adopt innovative technologies that eliminate multiple pain points, the report noted. Innovation inherent in converged systems and particularly in hyperconverged infrastructure is driving process efficiencies and a level of agility that are increasingly measurable, it said.

The dramatic spread of this new type of IT infrastructure is not merely changing the technological identity of IT environments, the 451 report said. It is also changing the personnel who manage the technology. And the larger the organization, the more prevalent the shift. More than 40% of very large enterprises (those with 10,000 or more employees) plan to change their IT team layouts.

One factor driving the rise of hyperconvergence is the massive shift underway toward cloud-based services. Today's enterprises expect the same level of flexibility from their internal IT infrastructure that a public cloud service can provide, the report said. And a hyperconverged infrastructure can transform the technology that supports today's business needs.

While hyperconvergence for many organizations represents the data center of the future, some are already well into implementations and seeing benefits.

For example, a healthcare company developed a hyperconverged infrastructure two years ago to cut costs, simplify IT management, and eliminate information silos within the organization.

With a hyperconvergence solution, the company

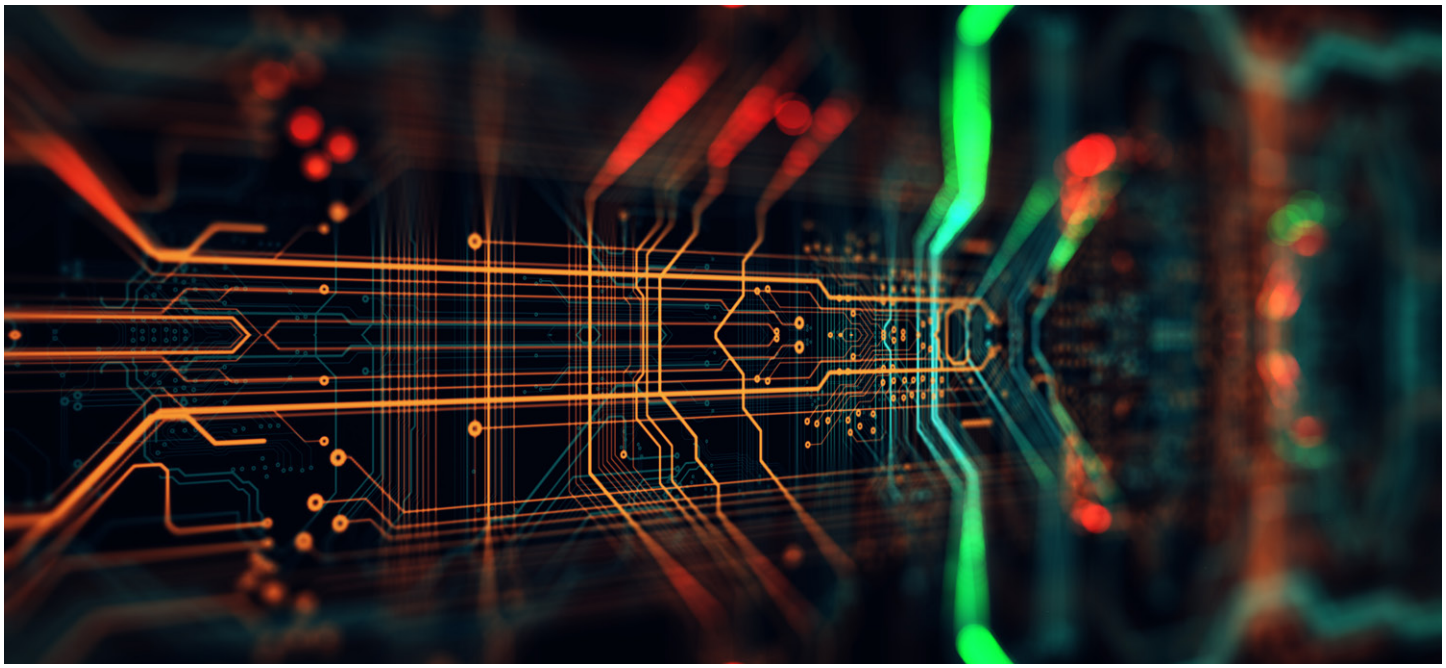
consolidated workloads that had been on blade servers and storage-area networks to a single platform. It moved most of its physical infrastructure to a virtualized environment on the platform. By leveraging hyperconvergence, the healthcare provider expects to decrease costs by millions of dollars over a five-year period.

Another company, a transportation and logistics business, created a hyperconverged environment as part of a multi-year effort to revamp its data center. Its infrastructure had consisted of computing, networking and storage systems from different vendors, and these systems were costly and difficult to manage.

Hyperconvergence let the company replace existing servers and storage platforms, cutting out some licensing expenses. The company also expects benefits such as greater scalability, increased efficiency and easier management of its data center.

Addressing the Security Implications

Just as hyperconvergence in the data center will have a huge impact on how systems and data are managed, it will have significant repercussions for information security. Any organization that thinks security does not need to change in a hyperconverged environment puts data and systems reliability at risk.



As Gartner has stated, there is a need for security controls for hyperconverged integrated systems in software-defined data centers.

HCISs need to be protected from attacks against the control plane, data plane and management infrastructure, the firm said.

Some security challenges the hyperconverged infrastructure raises stem from from the very reasons hyperconvergence will be so popular: performance and agility. To be effective in this type of setting, security solutions must understand the hosting environment so that performance can be maximized without the loss of security functionality.

Agility is a critical feature that must be embedded in the security layer to cope with the rapid changes of the software-defined environments. New security models need to be as flexible as the underlying infrastructure, and security must be able to support IT infrastructures that are automated and quickly spun up and spun down as required.

Hyperconvergence simplifies the data center and makes it more automated. Traditional security architectures, with full-scale agents running on each endpoint, cause major performance drops in hyperconverged infrastructure environments. The modern data center requires new security architectures with a light agent, or no agent at all, running on virtualized endpoints.

Centralized security controls must have built-in reliability, be easily scaled and accommodate fast virtual machine deployments. Security solutions must also enable centralized policy management, deployment, monitoring and response to security incidents, in order to enforce security compliance across the entire data center infrastructure.

Traditional security tools were designed for legacy data centers, with hardware-centric architectures, so they do not provide the level of performance and automation needed for the hyperconverged infrastructure and software-defined data center.

According to the Market Guide for Cloud Workload Protection Platforms published by Gartner in 2016, security executives should deploy products designed to protect hybrid cloud workloads. The security architecture must be an integral part of the migration toward hyperconverged infrastructure and software-defined data center environments.

They need to deploy security solutions that are enablers rather than detractors of the major shifts underway in the data center space: hyperconvergence, software-defined data centers and the hybrid cloud. Such products are available today, and enterprises need to look for certain key capabilities when evaluating these offerings.

For one thing, the solution needs to be built from the ground up for virtualization and cloud environments. That includes offering anti-malware protection for virtual machines, optimizing not only consolidation ratios but also operational costs.

It should also be designed as an enterprise solution capable of supporting the largest data centers. At the same time, integration into a production environment should be simple, and the technology benefits should apply to a virtual environment of any size.

Some solutions, such as GravityZone from Bitdefender, rely on an adaptive, layered protection powered by machine learning technology to provide efficacy. It works to predict, prevent, detect and remediate known and unknown threats, and protects organizations from advanced attacks. Although optimized for virtualization, GravityZone makes no compromises in protecting the entire data center, including physical servers, desktops, laptops or mobile devices that are part of the environment.

A key consideration when looking at any security solution for a hyperconverged data center is whether the solution has been tested to see what kind of impact it has on applications running in virtualized environments. The impact on performance should be minimal. Otherwise, the benefit of strong security will be offset by the lower level of performance in the data center, something that business users will not be happy with.

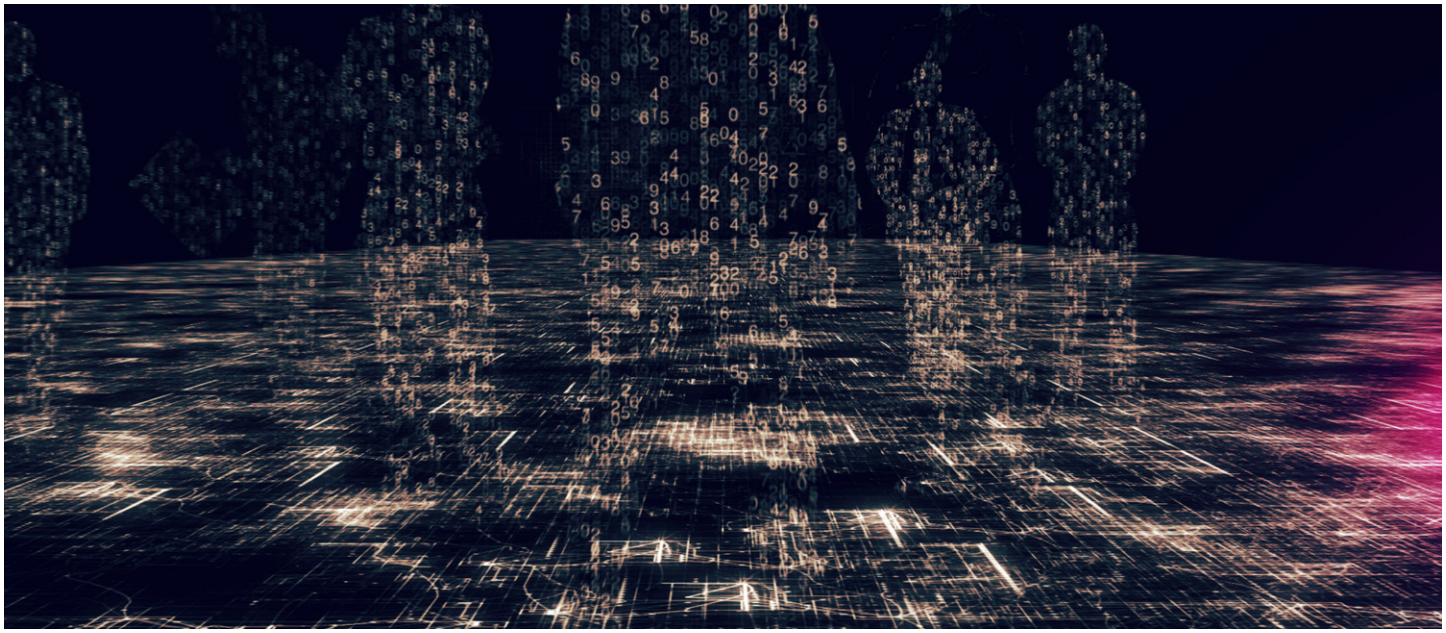
Also important is whether the solution provides optimized security on all major virtualization platforms, including VMware, Citrix, Microsoft Hyper-V, KVM and Oracle, and in any combination of environments such as private clouds, public clouds and hybrid clouds.

The point is security in this new environment needs to provide universal coverage, and to do that it has to be vendor-independent and coexist smoothly in most heterogeneous virtualization environments.

Other key attributes of a security solution for hyperconverged environments should include simplified deployment and management, with all controls consolidated on a single console; agility, so enterprises can easily extend or reduce their computing infrastructure without compromising security.

Summary and Conclusion

Hyperconvergence technologies offer enterprises a unique opportunity to transform their data centers, turning them into more efficient and better performing IT assets that support the move to digital business.



At the same time, a hyperconverged environment presents challenges and opportunities from a cyber security standpoint. Companies naturally need to maintain a high level of data protection in this new environment, but those efforts should not get in the way of what makes hyperconvergence—and the software-defined data center—such valuable resources.

IT organizations should focus on the activities that deliver value for business customers and not on deploying and managing security controls. The security solutions should naturally follow the evolution of the data center infrastructure and accommodate changes in the environment, without compromising the security posture.

Security solutions that consolidate all controls on a single console, and combine simplified deployment and administration of security policies to help streamline IT operations while improving compliance, enable organizations to fully reap the benefits of hyperconverged data centers.

These solutions can provide a blueprint for achieving a secure hyperconverged data center. They allow technology leaders to focus on maintaining an IT architecture that delivers a better return on investment, enables agile service provisioning and easily scales as the business grows.

About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com/.

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-Mar.23.2017-TK#: 70585