IDC VENDOR SPOTLIGHT

Sponsored by: Check Point Software Technologies Ltd.

Hybrid datacenter solutions address many of the security pain points enterprises have with visibility, portability, and scalability for on-premises private and hybrid cloud solutions.

Guide to Securing the Hybrid Cloud Datacenter in the Age of Digital Transformation

January 2022

Written by: Philip Bues, Research Manager, Cloud Security

Introduction

Today, many organizations are not only shifting more workloads to the cloud but also modernizing their datacenters. They are creating hybrid cloud environments with distributed workloads that must be secured. The modern datacenter and network require the flexibility of a hybrid cloud security architecture that uses automation and artificial intelligence to scale threat prevention performance on demand both on premises and in the cloud, with a simplified and unified management system. The hybrid datacenter security challenge is one of the untold stories of the enterprise digital transformation (DX) journey.

The DX journey for many organizations began pre-pandemic. During that era, enterprises were using broadband to connect the datacenter with public clouds. It was also the beginning of the "lift and shift" of workloads from the datacenter to the cloud. The shift to the cloud was the easy part. What's not easy is managing the cloud environment. DX was still in its infancy, the confidence and trust in cloud had yet to take hold, and many were still tunneling or backhauling remote offices and users to the datacenter.

Once COVID-19 hit, transformation plans accelerated, but so did the complexities. When work from home began globally, enterprises secured the cloud using services such as infrastructure as a service (IaaS) and software as a service (SaaS). At the same time, cybercriminals increased the frequency and sophistication of their cyberattacks. Cloud services were not immune to attack. As security risks increased, both the benefits and the complexities of leveraging cloud services became apparent.

AT A GLANCE

KEY STATS

Over the next five years, 59% of organizations will shift more workloads to the cloud while 65% will modernize their datacenters.

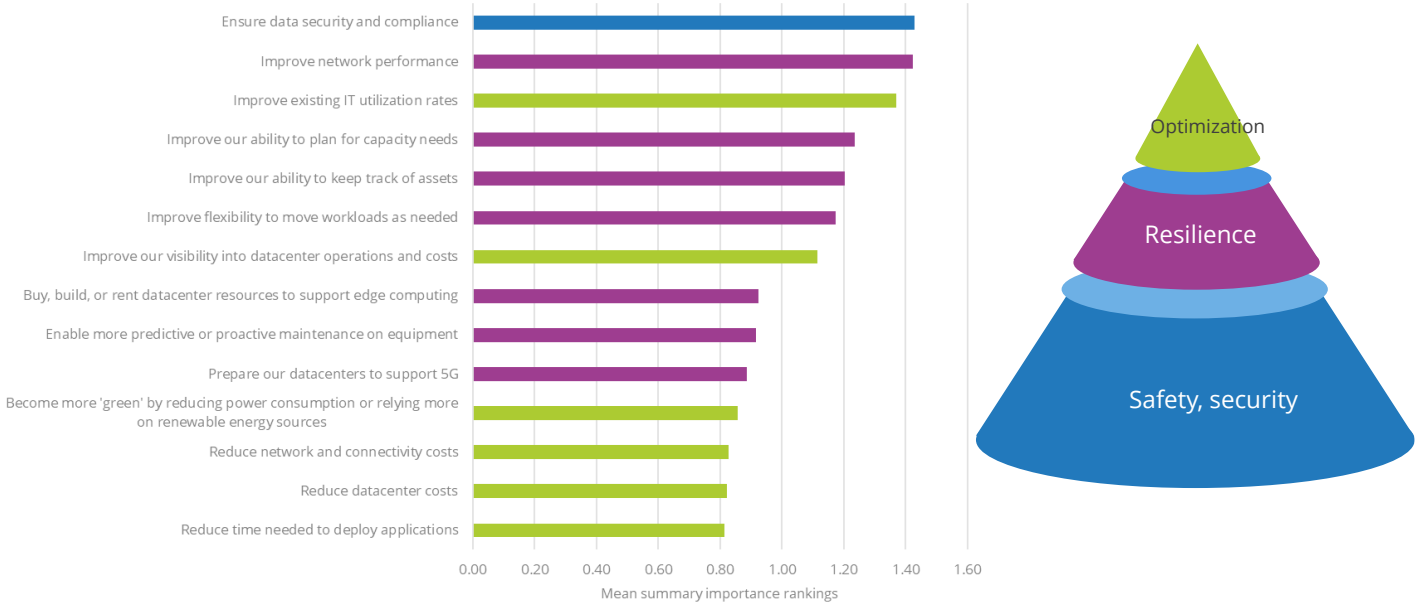
KEY TAKEAWAYS

- A modern hybrid datacenter solution can extend shared architecture, rules, and policies from an on-premises private cloud to the public cloud. This allows organizations to maximize their institutional investments and reduces retraining or upskilling.
- Modern hybrid datacenters utilize cloud-based platforms to provide artificial intelligence and machine learning automated threat management and response. These security policies not only streamline and add efficiency for Ops teams but also reduce the need for manual change controls, lowering the risk of human error and breaches as a result.

All organizations need to ensure control over their data and business operations. However, those in highly regulated industries such as financial services, healthcare, and retail must take additional measures, including keeping specific data and workloads on premises to be compliant. An on-premises private cloud is the most efficient solution.

Modernizing the datacenter is no longer tied to only avoiding downtime; it's also about safety, security, resilience, and optimization to meet the demands of the new digital economy. Make no mistake: These initiatives have a domino effect. The aged "piecemeal" solutions that lead to complexities have run their course. In IDC's 2021 *Datacenter Operational Survey,* enterprises identified the importance of modern datacenter initiatives, including making data security and compliance the top priority (see Figure 1). Next is recognition that integrating a hybrid cloud solution into the modern datacenter brings us closer to ensuring data security and compliance, improving network performance, improving existing IT utilization rates, and many other benefits revealed in the survey. Organizations looking to optimize compute and storage while taking advantage of managing changes via APIs should consider the benefits of "cloudifying" their on-premises datacenters.

FIGURE 1: ***Datacenter Initiatives***



n = 400

Source: IDC's Datacenter Operational Survey, 2021

Key Challenges for On-Premises Private and Public Clouds

Datacenter private clouds and hybrid clouds are now inextricably linked yet likely serve different functions. An on-premises private cloud might be used for running large customer relationship management (CRM)/enterprise resource planning (ERP) workloads requiring low latency, while commodity services such as email and file storage are hosted in the cloud. First, we need to put some context around public and private cloud security challenges: Complexities still exist, and organizations continue to experience breaches both on premises and in the cloud.

In the past, many customers of security services may have waited until an emergency, such as a breach, occurred before implementing a cloud posture or hygiene strategy. The reasons for waiting could be traced back to insufficient staffing, skills/training, and complex tools. However, the rate of breaches has intensified. According to IDC's 2020 *EDR and XDR Survey,* over the past two years, most organizations have had from one to six or more major security breaches on premises, which involved spending significantly extra resources to rectify. As a result, these organizations then began a shift to the cloud. IDC's 2020 *Cloud Security Survey* found that most organizations' IaaS cloud environments have also been breached with the same outcome that involved the spending of significant extra resources to rectify. It should be noted that less are reporting "no breaches" in the cloud compared with on premises. This is largely due to the shared infrastructure model found in public clouds where the cloud service provider becomes a security custodian for varying levels of responsibility beginning in IaaS with the physical, infrastructure, network, and virtualization. Additional services are provided by third-party vendors.

In the cloud, complexity for the organization is reduced. However, the reality is that enterprises are adopting a hybrid datacenter solution with a presence in both an on-premises private cloud and an off-premises public cloud:

- The digital transformation journey leads many organizations to migrate to several IaaS cloud environments. Each cloud has different configurations, code vulnerabilities, and maintenance issues. Clouds are different.
- Managing multiple disparate private and public clouds means learning how to use multiple tools to orchestrate and secure those environments without a unified visibility, management, and compliance platform.
- The cloud shared infrastructure model means user controls decline as the deployment model migrates to services. In an on-premises private cloud, the organization retains full control. In a public cloud, the provider takes on more responsibility and risk as the organization moves to higher levels of virtualization. In a typical SaaS offering, the user retains control over only identity and data. The complexity increases as more SaaS instances are added.
- A private cloud and a public cloud are optimized for different workloads and applications.

Infrastructures change. Data residency changes. Threats change. Some of the key benefits that a hybrid datacenter solution can deliver are based on resiliency — no matter what change brings.

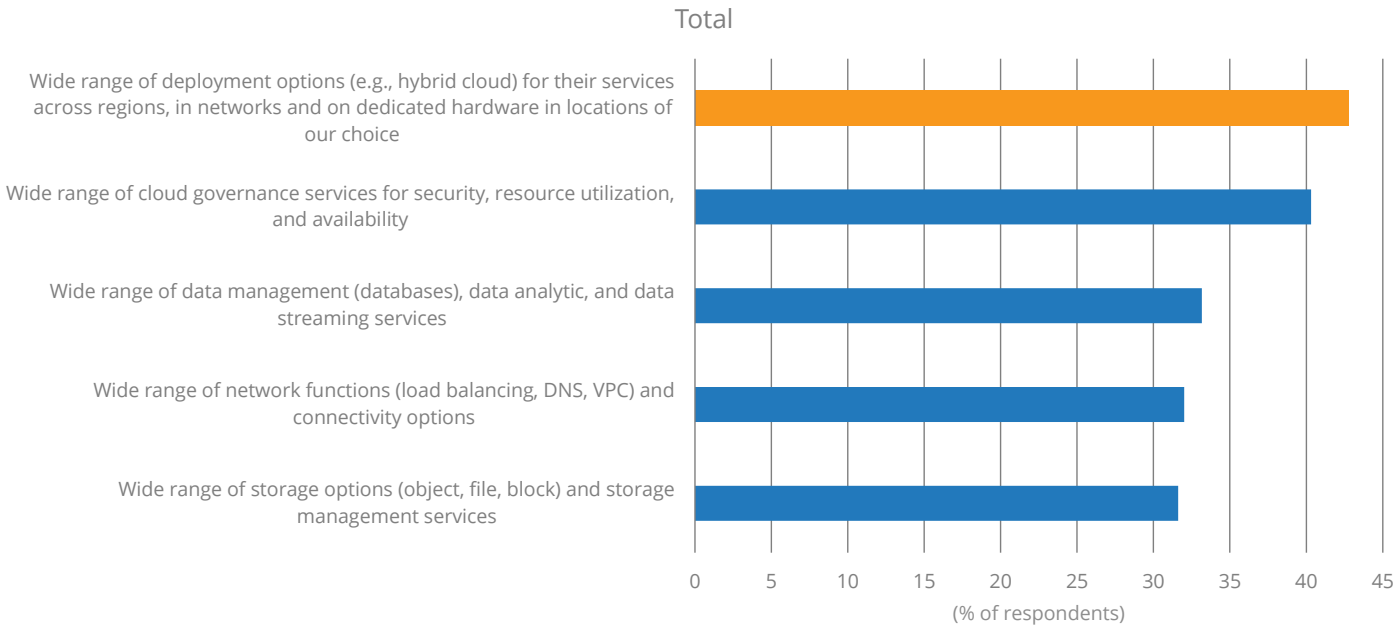
Benefits of a Hybrid Datacenter Solution

A hybrid datacenter solution provides a unique opportunity for organizations to operationally optimize and secure their environments. It starts by reducing management complexity of multiple cloud environments by transforming an organization's business and development processes. In this scenario, a hybrid datacenter solution can extend shared architecture, rules, and policies from the private cloud to the public cloud.

Infrastructures change. Data residency changes. Threats change. Some of the key benefits that a hybrid datacenter solution can deliver are based on resiliency — no matter what change brings. To prepare for novel business disruptions, organizations need plans, tools, and the right partners to enable them to rapidly adapt as opposed to respond (see Figure 2).

FIGURE 2: ***Top Cloud Services***

Q ***Which of the following portfolio of services/options are the most important in your choice of a primary cloud platform to support your digital transformation plans? They offer a...***



n = 198

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 7, July 2021

- Portability and being resilient to changing global business conditions are fundamental in business today. Organizations need to look at cloud in a holistic way to meet these elasticity demands. Hybrid datacenter solutions meet this need by utilizing virtualization and being focused on security that is flexible and scalable.
- Unified visibility, policies, and centralized controls are necessary to ensure the system health and safety of customer data from the datacenter private cloud to public cloud IaaS, platform as a service (PaaS) (containers), function as a service (FaaS) (serverless), or SaaS. This need has increased given the distributed nature of SaaS environments and the work-from-anywhere environment.
- Modern hybrid datacenters utilize cloud-based platforms to provide artificial intelligence and machine learning automated threat management and response. These security policies not only streamline and add efficiency for Ops teams but also reduce the need for manual change controls, lowering the risk of human error and breaches as a result.
- Redundancy and disaster control are part of the hybrid datacenter fabric.

The cybersecurity talent shortage has been made even worse by the pandemic. IT teams have been stretched, and IDC has observed that traditional roles — for example, help desk administrators — are now spending time on nontraditional IT tasks such as cybersecurity. Taking advantage of the cloud means there will be time for security practitioners to triage alerts and breaches while leaving other tier 1 functions to the cloud service provider. Anytime organizations can reduce risk and complexity, it's a win.

To maintain the pace of innovation in order to protect workloads against threats and vulnerabilities, ease of use, compatibility with existing cyber-risk management tools, and ease of implementing security as new workloads are instantiated in development and production are essential.

Key Trends

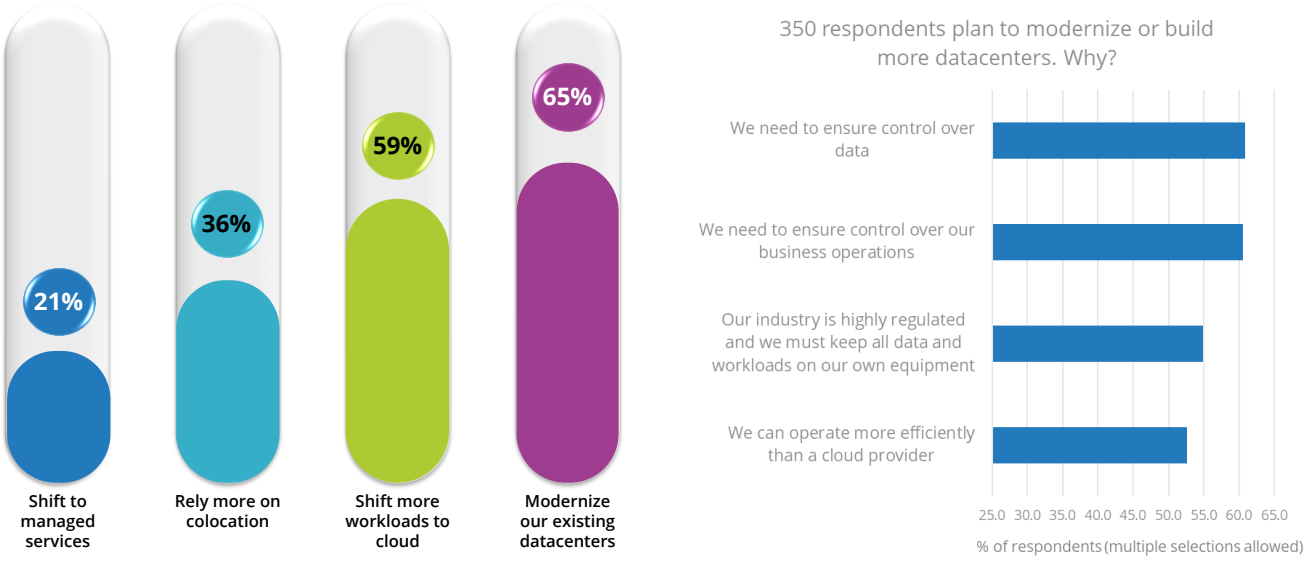
Digital transformation investment is on pace with — and, in some cases, ahead of — pre-pandemic spend. But who are the decision makers, and what are the investment and cost optimization activities?

Digital transformation has ushered in a new set of technology buyers. According to IDC's Worldwide IT Spending Guide, 50% of technology spending comes from *outside* the IT department and is driven by the line-of-business (LOB) buyers. In general, they prioritize creating revenue, good customer experiences, and cost savings. In IDC's August 2021 *Future Enterprise Resiliency and Spending Survey, Wave 8,* 774 respondents were asked the following question: In the wake of developments during the COVID-19 pandemic, how would you assess where your organization is with respect to its digital transformation compared to peers? The majority of respondents (29.5%) indicated that their DX initiatives are initiated at the function or LOB level, with some connection to enterprise strategy. IDC also found that chief information security officers (CISOs) are rarely included in DX discussions. This seems like a trend organizations should explore.

Cloud and datacenter activities are linked. As shown in Figure 3, resources are being allocated based on a five-year plan for most organizations plotting out their cloud platform and datacenter strategies. In IDC's 2021 *Datacenter Operational Survey* of 400 respondents, 59% of enterprises will shift more workloads to the cloud while 65% will modernize their existing datacenters. Organizations know that they are only as strong as their weakest link. These actions demonstrate the value and trust put into the hybrid datacenter model.

FIGURE 3: ***The Five-Year Plan Is About Cloud and the Datacenter***

Q Over the next five years, will your organization do any of the following?



n = 400

Source: IDC's Datacenter Operational Survey, 2021

The last trend, the one we are focused on the most, is the increase in breaches where organizations have multiple IaaS cloud environments and how those security breaches positively correlate with the elapsed time in investigated triaged alerts. The fewer breaches, response time goes up within an hour and vice versa. This stands to reason given the talent shortage and increase in breaches due to advanced malware, which includes ransomware as a service.

Considering Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. is a major provider of cybersecurity solutions to over 100,000 governments and corporate enterprises globally. Its solutions protect enterprise customers from sophisticated multivector fifth-generation cyberattacks with a substantial catch rate on malware, ransomware, and other types of attacks.

The Check Point Hybrid Datacenter portfolio enables customers to realize the benefits of consolidation by securing their cloud and datacenter environments under a single vendor using a DevSecOps approach from step one, orchestrated from the Infinity-Vision Unified Security Management platform. This platform provides a more user-friendly approach and centrally manages the hybrid datacenter architecture from a single pane of glass. This unified system is also extensible using RESTful APIs, which provide a framework for automating security and responses to threats.

The key innovation to cloudify the datacenter is the Quantum Maestro hyperscale network security architecture. Check Point Maestro brings scale, agility, and elasticity of the cloud on premises by maximizing the security capacity of security gateways with efficient N+1 clustering based on patented HyperSync technology. This enables enterprises to create their own virtualized private-cloud on premises by connecting multiple Check Point security gateways. The security gateways can be grouped by security feature set, policy, or the assets they protect and further virtualize them with virtual systems technology.

The Quantum Maestro Hyperscale Network Security Architecture scales as business and technical requirements change. Whether an enterprise is connected to the public cloud via broadband or just beginning the DX cloud migration process, Quantum Maestro is designed to provide advanced threat protection, enhanced redundancy, automatic provisioning of firewalls, and integrated security all with consolidation in mind, leading to a smaller datacenter footprint.

As users require more SaaS applications in the cloud, such as email, office productivity, and videoconferencing, Check Point Harmony Connect is designed to insert security into that communication. Harmony Connect is the conduit for making on-premises architecture and applications available in the cloud with the same look and feel. Additional protections available by Harmony include endpoint and mobile security solutions that extend to the work-from-anywhere environment. Once an organization moves into the cloud and employs a DevOps approach, Check Point CloudGuard is introduced to offer:

- Private and public network security
- Cloud security posture management
- Workload protection (containers and serverless)
- Web app and API protection
- Cloud intelligence and threat hunting

Organizations can also leverage Check Point Infinity SOC for advanced incident detection and response along with Check Point's ThreatCloud global threat database, which consolidates threats that are local to the network and global. Through ThreatCloud, Check Point leverages anonymized threat data from its own appliances and from external resources such as law enforcement to collect and enhance threat intelligence. The dashboards and security metrics offered in Infinity SOC are also used by the Check Point research team internally. The benefits of these platforms include eliminating false positives and redundant alerts and, importantly, freeing up valuable personnel.

Check Point differentiates itself from the rest of the market by continuing to innovate, adding ecosystem partners, and closing the cybersecurity gaps with strategic acquisitions, most recently Avanan. Integrating Avanan into the Check Point portfolio provides a secure email security offering designed to protect the remote workforce.

Challenges

Check Point has done well in the on premises datacenter and network security marketplace with the Quantum family of security appliances, Maestro Hyperscale Security Orchestrator, and Infinity-Vision Unified Security Management. As more enterprises adopt the hybrid datacenter architecture, Check Point would benefit by continuing to grow its cloud security products and services. Check Point has expanded its CloudGuard security offerings recently with acquisitions such as Dome9 for posture management, Protego for serverless, and Avanan for email security. Check Point recently entered the cloud container security market, but its first version lacked application control. Check Point container security does offer URL filtering, threat prevention, and autonomous access policy. Check Point should continue to expand cloud security features for applications, APIs, and microservices including containers and serverless functions.

Conclusion

IDC believes the hybrid datacenter is a "best of both worlds" scenario, taking advantage of modern datacenter and hybrid cloud services and innovations. As companies begin their modernization and cloud journeys, they would do well to work with a vendor that will help facilitate a multiyear plan and that values a DevSecOps approach and recognizes that performance metrics should include trust as a key element. The hybrid datacenter market will continue to grow along with hybrid cloud. Given the Check Point Hybrid Datacenter security portfolio enables enterprises to confidently secure their cloud and datacenter environments under a single unified security management system, the company has a significant opportunity for continued success.

About the Analyst

Philip Bues, *Research Manager, Cloud Security*

Phil Bues is the Research Manager for IDC's Cloud Security practice. In this role, Phil drives research, provides thought leadership, and advises clients on complex issues, including cybersecurity of the cloud and in the cloud. His commentary addresses the benefits and challenges to what's been called the shared responsibility model and how that line may change going forward.

MESSAGE FROM THE SPONSOR

About Check Point Software

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions that protects over 100,000 organizations of all sizes. Its solutions protect enterprises from 5th generation cyber-attacks with an industry leading catch rate against malware, ransomware, and other types of attacks. Check Point offers its Infinity Total Protection multilevel security architecture with threat prevention against advanced Gen V cyberattacks. Check Point security defends enterprise datacenter s, cloud, networks, mobile, endpoint and IoT devices. Check Point provides the most comprehensive and intuitive one point of control unified security management system.

Determine your datacenter, network, and cloud security risk today through a Free Hybrid Datacenter Security Assessment at https://www.checkpoint.com/solutions/data-center-security/

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com