White Paper

Build a Secure Enterprise Cloud

With Nutanix and Bitdefender

By Mike Leone, ESG Senior Analyst; and Leah Matuson, Research Analyst

July 2019

This ESG White Paper was commissioned by Nutanix and Bitdefender and is distributed under license from ESG.

Contents

Introduction

While many organizations are undergoing a digital transformation to improve agility, efficiency, and productivity with a modern infrastructure, they also realize that a secure infrastructure is crucial. In fact, the need to improve cloud security across the organization is the most often cited justification for short-term cybersecurity investment priorities.[1] Additionally, according to ESG research, improved cybersecurity continues to be the top business driver for technology spending with 40% of IT professionals stating strengthening cybersecurity will be one of the initiatives that drives the most technology spending over the next 12 months.

But it's not that simple. With an increased focus on cybersecurity, organizations are seeing more involvement from business personas within the organization, including C-level executives, and this is creating a challenge for IT and security administrators to continue to meet top-level security mandates.

Protection in Dynamic Business Environments

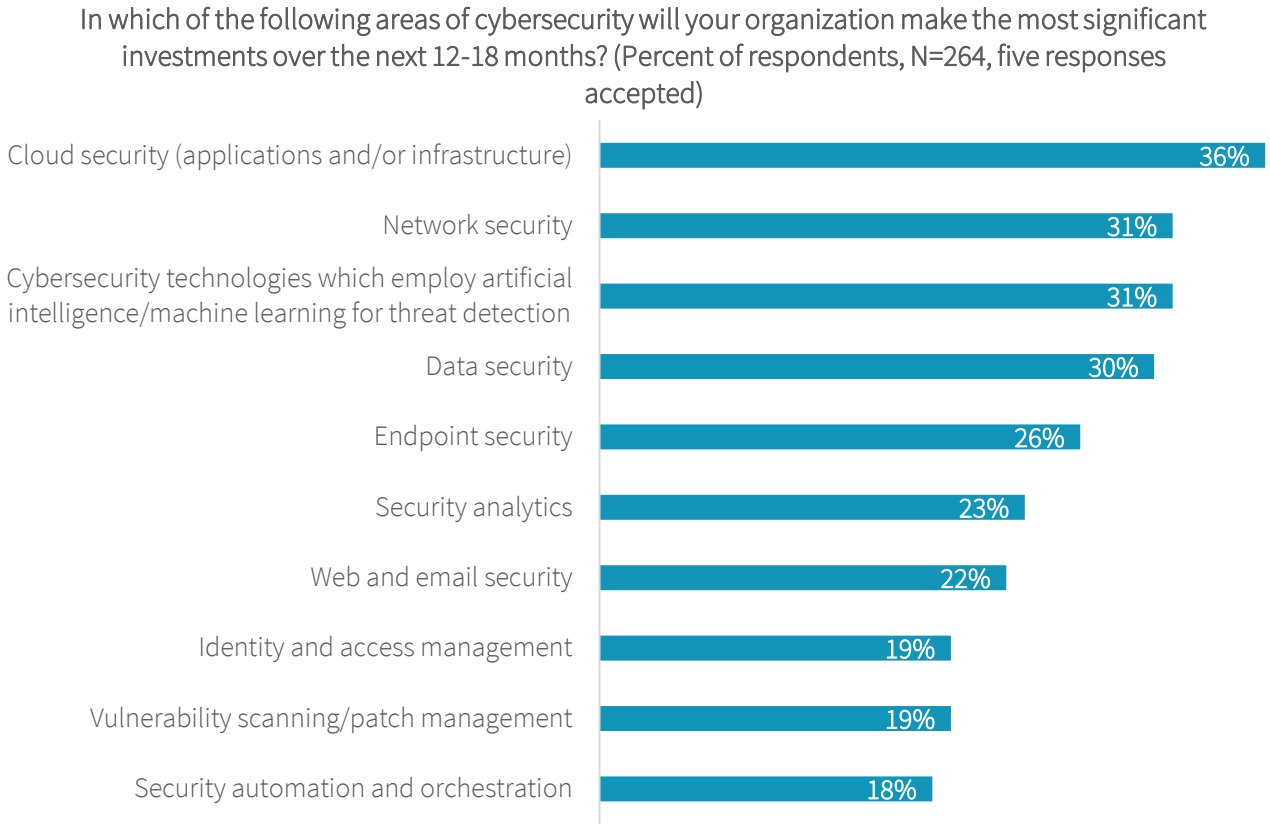
Today, it's essential to protect corporate data (think business-critical data, customer information, financial records, personal health care records, etc.) while also prioritizing initiatives that foster a modern infrastructure that can support the continuing health and agility of the business.

According to ESG research, 21% of IT professionals say that strengthening cybersecurity tools and processes will be the most important focus areas over the course of 2019.[2] Due to an ever-expanding perimeter, protecting only the perimeter is not an option. The attack surface is no longer everything beyond the firewall. This means cybersecurity strategies need to continually evolve to deal with rising numbers of ever-changing cyber threats.

Additionally, cybersecurity strategies must deal with the constantly changing needs of the business. ESG research shows that IT professionals have a wide range of cybersecurity concerns, citing network security, technologies that use AI/ ML for threat detection, data security, endpoint security, cloud application security, and cloud infrastructure security investments as significant cybersecurity priorities for 2019 (see Figure 1).

[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019. All ESG research references and charts in this white paper have been taken from this report unless otherwise noted.
[2] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.

Figure 1. Top Ten Short-term Cybersecurity Investment Priorities



Source: Enterprise Strategy Group

The challenges seem daunting—from dealing with multiple clouds and bring-your-own-device initiatives to rising numbers of interconnected supply chains and an escalation of cyberattacks across organizations. Organizations are experiencing increasing numbers of malicious threats and cyberattacks, progressively increasing in complexity, from phishing, denial-of-service, password, and drive-by attacks to man-in-the-middle, SQL injection, eavesdropping, and malware attacks (ransomware attacks are among the swiftest growing cybercrimes today). And what about serverless applications and data processing tools, and their vulnerability to attack?

A Modern Infrastructure for an Evolving Threat Landscape

Given an ever-evolving threat landscape, organizations must be fully prepared. But while security is clearly top of mind across industries, organizations are also focused on agility and productivity, and simplifying infrastructure administration and management.

Organizations want the flexibility of deploying applications in minutes (and cost effectively), reducing capital investments on infrastructure, and decreasing time expended on routine maintenance and management. As such, organizations are turning to HCI as a means of meeting these requirements, while helping bridge the gap to the cloud. In fact, deploying consolidated infrastructures, such as HCI, is a top investment priority to satisfy short-term data center modernization initiatives.[3] But the million-dollar question is this: How can organizations effectively keep the business safe while improving IT agility and productivity—all while reducing costs?

[3] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.

Operational Efficiency and Agility with Management Simplicity

Dealing with an organization's infrastructure has traditionally fallen upon the shoulders of IT operations and infrastructure teams. They have long been charged with managing the infrastructure—often across a globally distributed organization—while deploying security, troubleshooting, reporting, etc. And a traditional, three-tier architecture consisting of siloed components creates numerous hurdles, especially when it comes to incorporating a comprehensive security plan.

If that isn't enough, with many organizations embarking on digital transformation journeys to modernize their infrastructures with HCI, IT must look to an infrastructure that benefits from a cloud-operating model—one that enables them to achieve the agility needed to quickly respond to constantly changing needs of business. ESG research shows that operational efficiency remains the most common objective for digital transformation with more than half of organizations (55%).

Figure 2. Organization's Most Important Objectives for Digital Transformation Initiatives

Source: Enterprise Strategy Group

And all of this is before thinking about next-generation technology and the positive impact it could have on organizations across the board. IT teams are starting to acknowledge they must invest in technology that will enable them to easily view and analyze all data in real time, including operational data spread across a globally-distributed organization, as well as integrate data generated from next-generation applications at edge locations. How can they expect to succeed on next-generation initiatives without an agile infrastructure foundation that incorporates security as a core tenet across the infrastructure stack?

Improved ROI

HCI enables organizations to become more agile and operationally efficient by integrating the management plane for virtualization, compute, storage, and networking, and automating IT operations. And while 13% of organizations view

improving TCO as the primary reason for deploying HCI, 28% of those that have deployed it view improved TCO as the most significant benefit they've realized.[4]

For security specifically, HCI-optimized workload security promotes agility and operational efficiency by integrating security operations with infrastructure operations. For example, when a virtual machine is created, the appropriate security policies can be automatically provisioned and configured. By leveraging a workload-security solution that is optimized for HCI, organizations can drive additional savings and even faster ROI, compared to legacy security approaches.

Traditional Security Challenges

It's no secret that traditional solutions can negatively affect infrastructure utilization and latency (speed of application response) as security agents run resource-intensive tasks, such as anti-malware scanning and downloading signature databases. While rising numbers of organizations are deploying new solutions to specifically support the security aspects of their modern infrastructures, they must also focus on resource utilization to improve ROI. In fact, ESG research shows that organizations' top considerations when purchasing a cybersecurity product/service are effectiveness, ease of operation, and cost.[5]

For example, an organization deploying thousands of virtual machines using traditional security solutions could have thousands of copies of the same signature database per session, per day. If each of the virtual machines began scanning simultaneously (think AV storm), a massive amount of network resources would be consumed at the same time, resulting in dramatic latency and greatly decreased performance.

The Value of a Holistic Approach to Security

For security professionals, managing enterprise security can be like trying to solve an ever-morphing Rubik's Cube. When even a small number of pieces don't match up, the entire system doesn't correctly perform—and that's not an option. Organizations that don't perform due diligence when adding new solutions can open the door to security risks through unsecured third parties, email hacks, etc. Likewise, the public cloud is a huge point of entry for cybercriminals, and without a holistic multitiered security approach, organizations can leave themselves vulnerable to breaches.

A holistic approach to security involves integrating the pieces of a security framework necessary to the continuous protection of an organization across prospective attack surfaces. In essence, IT must protect the business and mitigate risk by taking a holistic approach across the full stack, encompassing physical/virtual hosts, the network, underlying data, and endpoints.

When it comes to host security on HCI, organizations should look to prioritize platforms with security designed into the system (as opposed to bolted on)—enabling higher efficiency for updates and patching, and significantly reducing risk exposure. On the networking side, the enablement of micro segmentation as it relates to every application in the data center is ideal. Organizations should be able to customize application protection for each unique application and workload while ensuring control and transparency across environments (both on-premises and in the public cloud) to ensure there are no network security gaps.

Growing numbers of data breaches have compelled enterprises to be more proactive by encrypting data at rest and in flight, protecting sensitive and business-critical data. Organizations can further protect their data, maintain compliance, and ensure tracking control by encrypting it at the file system level, while providing access controls to the encrypted data (including enterprise key and policy management).

[4] Source: ESG Master Survey Results, *Converged and Hyperconverged Infrastructure Trends*, October 2017.
[5] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018.

Endpoint Security

An integral part of an organization's security strategy is endpoint security. Bad actors, becoming stealthier in their tactics, are continually innovating new and more complex methods to gain access to corporate data. In response, organizations have continued to intensify their efforts to protect their valued data, adding prevention, detection, and response controls to traditional endpoint control solutions. Piling on additional controls and solutions (requiring additional resources and costs) is not as effective as employing a unified platform that uses layers of detection and protection technology to secure endpoints in all environments. But with organizations shifting from virtualized environments and private clouds to hybrid clouds and multi-clouds across public cloud service providers, the diversity of use cases and requirements are raising security and compliance concerns.

Nutanix and Bitdefender: Secure Cloud, Secure Workloads

Global hyperconverged infrastructure leader, Nutanix, and global security technology company, Bitdefender, combine to provide organizations with a viable means to cost-effectively increase IT efficiency, agility, and productivity, and mitigate risk through a comprehensive automated cloud workload security solution.

An Agile and Modern Infrastructure with Nutanix

For more than a decade, Nutanix has been an innovator in the hyperconverged infrastructure (HCI) space, helping organizations span the gap between traditional infrastructure and public cloud services. Nutanix Enterprise Cloud helps eliminate complexity across the software stack, offering organizations a way to easily secure and manage the infrastructure. By seamlessly uniting an organization's private and public clouds with a single software fabric, Nutanix Enterprise Cloud is a turnkey infrastructure stack (e.g., integrated server, storage, networking, and virtualization), which can enable organizations to streamline multi-cloud adoption through intelligent management and operations.

Simplicity is key. With Nutanix Enterprise Cloud, purchase, deployment, system management, scale, and upgrades are designed to be straightforward, allowing IT staff to focus more on end-user enablement, with an application- and services-centric approach that leverages a single layer of software to "re-platform" IT.

With Nutanix Prism, organizations can easily manage all aspects of the HCI environment, including the underlying hardware, simplifying common workloads and VM management, and offering deep analytics based on an organization's unique needs—while saving time and resources via self-service provisioning for developers.

Security is vital. While security continues to be the top priority of organizations across industries, it's also one of the areas with which organizations struggle. Protecting data and mitigating breaches is essential, especially in regulated industries (e.g., financial, healthcare, and government). With security a focal point for Nutanix, organizations gain confidence with an application development lifecycle that has built-in auto remediation; built-in encryption with data at rest at the hardware and software layers; and self-encrypting drives.

Data protection at rest. Nutanix's data-at-rest encryption leverages FIPS 140-2 validated encryption libraries to protect your most valuable and sensitive data. Nutanix provides a native software-based encryption with local key management to satisfy most common use cases and can also support hardware-based encryption with SED drives.

The Nutanix Acropolis Operating System (AOS) offers a factory-hardened software platform with a self-healing security baseline configuration based on stringent government and industry standards. The platform is managed using role-based access control (RBAC) industry standards, while SAML supports enterprise authentication models.

Application and network security. Integrated with the Nutanix AHV virtualization platform, Nutanix Flow provides the visibility and granular policy-based application security necessary to help mitigate data breaches and the internal spread of malware via hypervisor-level network microsegmentation.

Additionally, Nutanix Calm Marketplace is a blueprint and orchestration framework offering administrators capabilities that include defining an application in multiple layers, publishing to a marketplace, and allowing users (via self-service) to automatically deploy a blueprint across the software layer using Prism as a single interface.

Integrated Enterprise Security for the Modern Data Center with Bitdefender

An international cybersecurity company since 2001, Bitdefender offers layered, next-generation security to customers in more than 150 countries, protecting more than 500 million machines with an efficient, cost-effective way to secure virtual premise-based and cloud endpoints and files. As a recipient of the 2018 Nutanix Elevate Partner AHV Innovator Award, Bitdefender has the distinction of being the only Nutanix scale-level partner in the workload security category and the only workload security vendor on the Nutanix Calm Marketplace, as well as the only workload security solution integrated with the Nutanix management platform, Nutanix Prism, and the Nutanix enterprise file services and storage software, Nutanix Files.

Bitdefender GravityZone, the vendor's integrated enterprise security platform, is a single agent, single console solution that runs in any environment on all workloads and integrates across the Nutanix software stack. GravityZone Security for Storage (an add-on module) uses machine learning, cloud lookup, heuristics, and other antimalware technologies to offer real-time protection for Nutanix Acropolis File Services (AFS) as well as other leading network storage and file sharing systems, and ICAP-compliant network attached storage (NAS) systems. GravityZone Security for Virtualized Environments is a certified Nutanix AHV-ready cloud workload protection platform. Designed for the modern data center, it leverages layered, next-generation defenses (tunable machine learning, application control, anti-exploit, and network sandboxing) to protect enterprise cloud workloads.

The Nutanix and Bitdefender Advantage

GravityZone helps to increase efficiency and agility by offering single-pane-of-glass security management integrated with the administration of the Nutanix infrastructure, lowering operating costs. The solution can simultaneously protect Nutanix virtual machines (VMs) and files and can be easily deployed as a virtual machine via Nutanix Prism or as a Nutanix Calm Marketplace blueprint. By incorporating machine learning and behavior analytics with response automation, GravityZone provides multi-stage endpoint detection and response—enabling organizations to increase threat visibility and keep resource requirements low.

Nutanix customers can confidently leverage GravityZone without impacting other workloads or services running on the cluster, as GravityZone doesn't pull resources from mission-critical applications that run on the cluster. Organizations can support security while still maintaining mixed, mission-critical application performance that meets individual service level agreements (SLAs).

Streamlined Security Workflow Automation with Enterprise Functionality

Integrating GravityZone with Nutanix enables simplified security workflow automation with enterprise functionality for enterprise cloud workloads—providing one-click server and in-guest tools deployment from a central management security console, automatic policy assignment, compliance reporting, and licensing reuse. Working together, the two solutions provide:

- Easy deployment of security servers. GravityZone SVAs are easily deployed. Once created, the new SVA VM automatically appears in GravityZone under its parent node.

- **Automatic policy assignment at scale**. GravityZone's integration with Prism also enables automatic policy assignment at scale based on hierarchical inheritance, so that all VMs in a cluster or node will automatically inherit the policy.
- **Ease of deployment for in-guest security tools**. Deploying in-guest security tools is simple for all virtual, on-premises, and cloud server, VDI, and DaaS workloads.
- **Efficient compliance reporting**. Creating compliance reports that provide protection status on a Nutanix cluster, node, or individual VM is simple.
- **Licensing reuse**. Because licensing is often based on the number of seats, organizations can quickly use up licenses. With security license recovery upon VM deactivation, GravityZone can save organizations time and resources. The solution employs real-time visibility into the moment a VM was provisioned and determines if the VM has security tools—allowing GravityZone to automatically send a license to the VM. Conversely, when VMs are decommissioned, Prism will notify GravityZone, which can clean up the inventory and reuse the license keys for new VMs being provisioned in the environment.

The Nutanix-Bitdefender solution offers the flexibility and simplicity of securely protecting an organization's multi-cloud environment. And though protecting a dynamic enterprise seems like a daunting task, a full stack solution with Nutanix Enterprise Cloud and Bitdefender GravityZone can help organizations improve their security posture, while reducing the time and resources needed to manually administer a patchworked, siloed system.

Nutanix virtualization software allows organizations to centrally manage virtual machines in conjunction with their network. Along with AI and machine learning, systems analysis of a virtualized network helps improve security, management, and operations, and can lower operating expenses while making compliance easier. Nutanix Flow is Integrated with Nutanix Enterprise Cloud OS and AHV, giving organizations visibility into their virtual networks. The solution offers application-centric protection against network threats, helping to mitigate the spread of malware (via application segmentation and micro segmentation). Additionally, Bitdefender GravityZone integrates with Nutanix Files, providing Nutanix customers with security for files and VMs, managed from the same GravityZone console.

Organizations can enjoy the simplicity and flexibility of the public cloud with Nutanix Enterprise Cloud, while gaining the control and security of a private cloud.

The Bigger Truth

Security remains a top priority for organizations. And as organizations continue to advance their digital transformation efforts by adopting a modern infrastructure that better supports the agility demands of IT, ensuring a holistic approach to infrastructure security is more important than ever before. Organizations understand they need to adopt technologies like HCI to satisfy current and future infrastructure requirements, ensure minimal to no risk exposure, and transition to—and eventually fully operate in—a multi-cloud environment.

By combining the core security capabilities of Nutanix with Bitdefender's endpoint and file-security capabilities, organizations gain an end-to-end workload and file security and protection solution that provides peace of mind to IT and end-users alike. With security across the entire stack, from hosts/VMs, networking, and data to the ever-expanding endpoints across clusters and clouds, organizations gain confidence knowing IT can effectively and cost-effectively respond to the business without sacrificing security.

www.esg-global.com contact@esg-global.com P. 508.482.0188