White Paper

Bitdefender®

Virtualization brings new security challenges for large companies

A survey on US IT decision makers

electronic version only

Executive summary

An October 2016 Bitdefender survey of 250 IT decision makers in the United States in companies with more than 1,000 PCs shows that virtualization is a strategic priority, yet they are still not fully ready for the security challenges this environment brings. Hybrid infrastructures have become the major common architecture in the enterprise environment and CIOs have to adapt to the new world. This survey, carried out by iSense Solutions, shows the main security concerns and issues they face. What cyber threats are companies not ready to handle? What are the main concerns regarding the security management of hybrid infrastructures? Why do IT decision makers fear for their jobs?

Key findings

- Some 73% of IT decision makers fear the financial compensation the company might have to pay in the event of a security breach, while 66% even fear about losing their job.
- Seven out of 10 IT decision makers replied they are “concerned” or “completely concerned” regarding managing security of hybrid infrastructures.
- The main security concerns when migrating data to a hybrid model are: security of data in transit (66%), security of data at rest (60%), security of backups and snapshots (54%), increased attack surface (53%).
- Main security issues after migrating to a hybrid infrastructure are: lack of visibility (51%), lack of policies (41%), and access from unauthorized devices (34%). IT professionals are unable to monitor workloads across clouds (47%), 44% agree or strongly agree there is insufficient network control and monitoring in the cloud.
- The main cyber threats companies are not prepared for are: outsider attack (43%), data vulnerability (38%), insider sabotage (35%), user errors (35%), and phishing (35%)

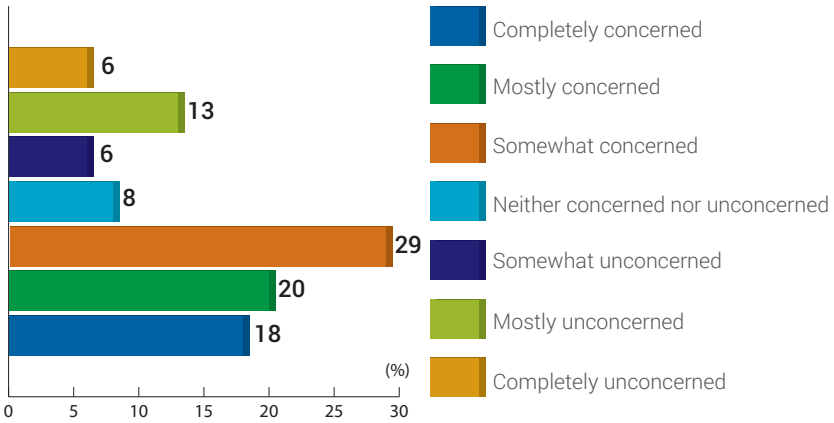
Gartner recently predicted in a report that the cloud will most commonly be used in a hybrid manner by 2020, and emphasized that operating entirely off the cloud will largely disappear by the end of the decade. The advisory company estimates that, by 2019, more than 30 of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only.

"Aside from the fact that many organizations with a no-cloud policy actually have some under-the-radar or unavoidable cloud usage, we believe that this position will become increasingly untenable," said Jeffrey Mann, research vice president at Gartner. "Cloud will increasingly be the default option for software deployment. The same is true for custom software, which increasingly is designed for some variation of public or private cloud." By 2020, a corporate "no-cloud" policy will be as rare as a "no-internet" policy is today, Gartner also says. "Technology providers will increasingly be able to assume that their customers will be able to consume cloud capabilities."[1]

Cloud adoption and the widespread usage of hybrid infrastructures will bring unknown security challenges that CIOs have to prevent by adopting breakthrough technologies able to fight zero-day exploits, Advanced Persistent Threats, and other devastating types of cybercrime.

A Bitdefender study on large US companies revealed that 73% of IT decision makers fear having to pay financial compensation in case of a security breach, while 66% even fear their own job safety. Moreover, seven out of 10 IT decision makers are concerned or completely concerned regarding the security management of hybrid infrastructures.

Concerns regarding the security management of hybrid infrastructures (%)

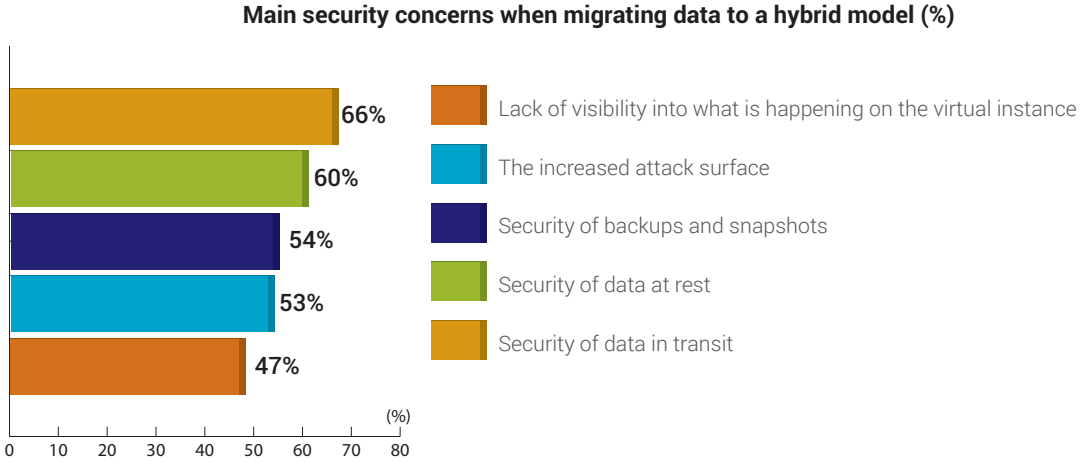


In the past two years, companies witnessed a rise in security incidents and breaches, with a significant increase in documented APT (Advance Persistent Threat) type of attacks targeting top corporations or government entities (such as APT-28). This type of attack is intended to exfiltrate sensitive data over a long period or silently cripple industrial processes. In this context, concerns for security are rising to the top levels, with decisions taken at the board level in most companies. Both IT decision makers and CEOs are concerned about security, not only because of the cost of a breach (unavailable resources and/or money lost), but also because the reputation of their companies is at risk when customer data is lost or exposed to criminals. As real cases have shown, the bigger the media coverage a security breach receives, the greater the complexity of the malware causing it. On top of this, migrating corporate information from traditional data centers to a cloud infrastructure has significantly increased companies' attackable surface, bringing new threats and more worries to CIO offices regarding the safety of their data.

Bitdefender's survey points out that IT decision makers say that the main security concern when migrating data to a hybrid model is the security of data in transit (66%). Security of data at rest (60%), security of backups and snapshots (54%), and the increased attack surface (53%) also top their list of security concerns.

Security specialists advise that, when opting for a hybrid cloud solution, an organization must first perform an analysis of the type of data it is handling and evaluate it based on its level of sensitivity – both for the company and its clients. Critical, personal and private data related to intellectual property must be stored on premise, with access to it available only to authorized personnel.

1 "Gartner Says By 2020, a Corporate No-Cloud Policy Will Be as Rare as a No-Internet Policy Is Today", June 22, 2016, http://www.gartner.com/newsroom/id/3354117



Security of data in transit or at rest is CIOs' main concern when shifting companies' IT architectures towards that mix the latest in public cloud services with their own private data centers. Bitdefender security specialists recommend that any data transfer between the client and the cloud service provider needs to be encrypted to avoid man-in-the-middle attacks that could intercept and decipher all broadcasted data. More than that, any data stored locally or in the cloud should be encrypted to make sure cybercriminals cannot read it, in case of data breaches or unauthorized access.

Previous surveys have shown that:

1. With cloud adoption becoming a reality for an increasing number of companies, most companies admit having experienced cloud security incidents – almost half of the reported incidents are related to unwanted external sharing and involve access from unauthorized devices.[2]

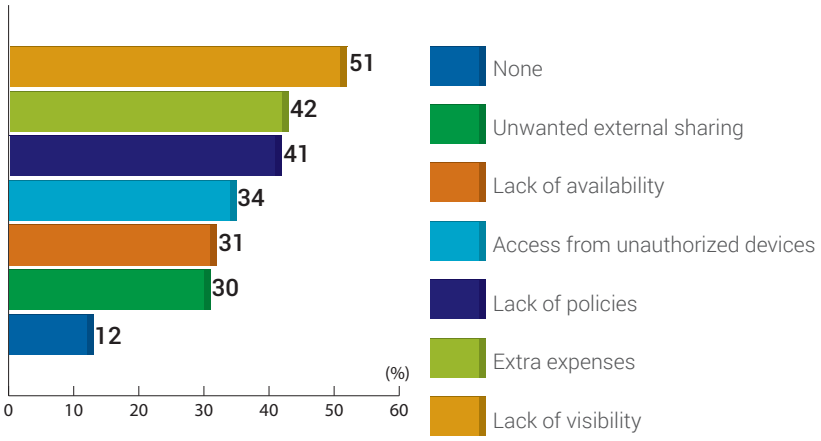
2. For many companies the primary reasons for selecting a particular cloud provider are efficiency (41 percent of respondents) and cost (37 percent), followed by reputation and customer service. Security comes only fifth.[3]

Bitdefender's survey shows that the main security challenges after migrating to a hybrid infrastructures are the lack of visibility (51%), the lack of policies (41%), and the potential access from unauthorized devices (34%). CIOs are also unable to monitor workloads across clouds (47%), and 44% agree or strongly agree there is insufficient network control and monitoring in the cloud.

2 "Report on mitigating risks for cloud applications". Cloud Security Alliance and Bitglass conducted a survey of 176 IT security leaders, https://pages.bitglass.com/Mitigating-Risk-For-Cloud-Applications.html

3 "The 2016 global cloud data security study", Gemalto and Ponemon Institute, 2016. Ponemon Institute surveyed 3,476 IT and IT security practitioners in the United States, United Kingdom, Australia, Germany, France, Japan, Russian Federation, India and Brazil.

Main (security) issues encountered after migrating to hybrid infrastructures* (%)



*- multiple answers possible

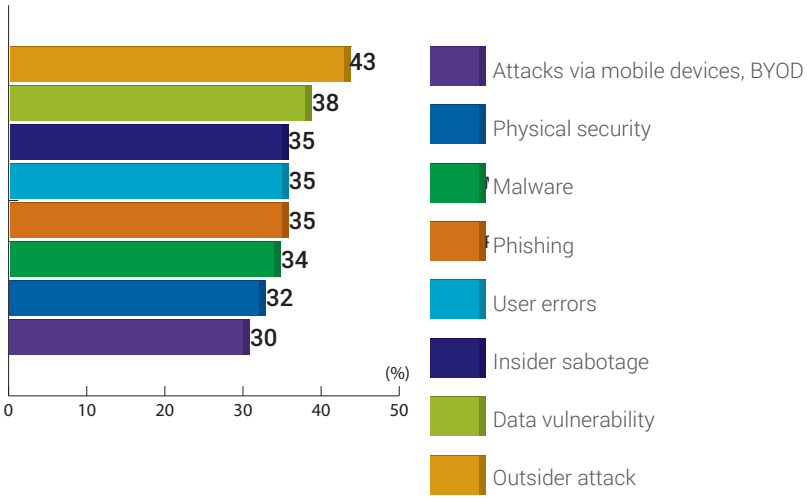
Accessing any type of data, whether stored in the private or public cloud, needs to be done via multiple authentication mechanisms, Bitdefender's security specialists recommend. These should involve a lot more than just usernames and passwords. For access to critical data, two-factor or even biometric data could offer additional control and authorization of qualified and accepted personnel.

Only authorized personnel needs access to critical and sensitive data, and only by adhering to strict security protocols and advanced authentication mechanisms. Besides two-factor authentication, even two-person authentication could be set in place for critical systems, similar to financial institutions where large transactions must be authorized by two or more individuals.

Surprisingly, extra expenses are also perceived as a security issue, despite a lack of direct connection between the two, but many IT decision makers fear their budget is insufficient to fight, detect, or prevent all cyber threats or that it could not accommodate future expansion, while some even admit they are understaffed. This way, extra expenses may soon turn into future security issues.

Bitdefender's survey shows companies are not prepared to handle: outsider attack (43%), data vulnerability (38%), insider sabotage (35%), user errors (35%), and phishing (35%).

Cyber threats that companies are not ready to handle (%)



*- multiple answers possible

Outsider attacks and data vulnerability pose a significant risk for all companies and represent the main threats that companies are unprepared to handle, and CIOs are aware that cybercriminals can spend large amounts of time inside organizations without being detected - APTs are often defined as designed to evade detection.

Cyber criminals also use tactics to draw attention away from what they are doing and where they have succeeded, while these cyberattacks impact business decisions, mergers/acquisitions and competitive positions.[4]

"To limit the risks of insider sabotage and user errors, companies must establish strong policies and protocols and restrict the ways employees use equipment and infrastructure or privileges inside the company network," Bitdefender's Bogdan Botezatu, Senior e-Threat Specialist recommends. "The IT department must create policies for proper usage of the equipment, and ensure they are implemented."

Information security teams and infrastructure must adapt to support emerging digital business requirements, and simultaneously deal with the increasingly advanced threat environment, Gartner recommends. As a result, security and risk leaders need to fully engage with the latest technology trends if they are to define, achieve and maintain effective security and risk management programs that simultaneously enable digital business opportunities and manage risk.[5]

Companies are slowly joining the bandwagon with hybrid cloud adoption, but Gartner estimates that it's still three to five years from going mainstream. By the end of 2015, only 15 percent of enterprises have adopted it so far, although the demand for hybrid cloud is estimated to be growing at a compound rate of 27% a year, outpacing overall IT market growth, according to researcher MarketsandMarkets. The company said it expects the hybrid cloud market to reach $85 billion in 2019, up from $25 billion in 2014.[6]

As a result, the hybrid infrastructure has become the major common architecture in the enterprise environment, with the hypervisor now sitting as an intermediary between virtualized endpoints and physical hardware. But endpoint security has not, until now, experienced the same paradigm shift. Traditional network-level security may run as a virtual appliance, but still essentially performs inspection of network traffic just as it did before. Traditional security agents running in protected systems may offload scanning to a virtual appliance for performance, but are still constrained by technical limitations of running within the endpoint operating system.

"As applications became mission-critical, and desktop servers moved into formal data centers, the number of physical servers in a data center grew exponentially, making the job of managing this environment increasingly complex and expensive, says Bitdefender's Head of Antimalware and Antispam Labs, Viorel Canja. Today, data centers are moving from isolated systems to interconnected pools of virtualized resources shared between multiple locations. Once an aspiration, the prospect of a fully virtualized data center is becoming a reality. Yet, while the benefits of virtualizing applications, desktops, hardware or networks are self-evident, security failed, until now, to align to this new paradigm."

Until now, the very concept of endpoint security was constrained to security agents running within a host OS on endpoints – the Windows and Linux servers and desktop operating systems upon which every modern organization depends – or as network devices, and attackers have been taking advantage of this.

Bitdefender has solved the technical challenges of creating a solution to the root problem, giving datacenter owners unprecedented insight, and allowing them to act on information from below the operating system. It is the only security company that provides security at the ring-1 level.

"Hypervisor introspection is a giant leap towards revolutionizing security as we know it, says Bitdefender's Viorel Canja adds. Virtualization technology continues to evolve, with increased levels of automation and comprehensive frameworks for managing the virtualized environment more efficiently. In this context, the hypervisor-based introspection technology is a future-proof advancement with numerous applications in other fields and industries."

4 "Creating trust in the digital world", EY's Global Information Security Survey, 2015, http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

5 "Gartner Identifies the Top 10 Technologies for Information Security in 2016", June 15, 2016, http://www.gartner.com/newsroom/id/3347717

6 SPECIAL REPORT: CIOs Say Hybrid Cloud Takes Off, WSJ, http://blogs.wsj.com/cio/2015/10/20/special-report-cios-say-hybrid-cloud-takes-off/

Methodology

This survey was conducted in October 2016 by iSense Solutions for Bitdefender on 250 IT security purchase professionals (CIOs/CEOs/CISOs – 26 percent, IT managers/directors – 56 percent, IT system administrators – 10 percent, IT support specialists – 5 percent, and others), from enterprises with 1,000+ PCs based in the United States of America.

More than half of the organizations surveyed are from the IT hardware and software / electronic and electrical engineering industries, while 24 percent are from manufacturing, 6 percent from transportation, 4 percent are providers of telecommunication services, 4 percent are utility or public services companies, and the rest come from construction, retail, distribution, media or other industries.

Some 62 percent of the organizations surveyed have over 3,000 employees, 14 percent between 2,000 and 2,999, and 24 percent between 1,000 and 1,999.

Regarding IT infrastructure development in the organizations, 39 percent of the companies have 3,000+ computers, 21 percent between 2,000 and 2,999, and 40 percent between 1,000 and 1,999. The average proportion of employees working on computers in the organizations surveyed is 74 percent.

Geographically, a third of the organizations are in the West, 30 percent in the North-East, 28 percent in the South and 11 percent in the Mid-West.

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/.

Author: Răzvan Mureșan

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/

BD-Business-Nov.02.2016-TK#: 70585