Paper

Bitdefender

# Virtualization's hidden traps: security has become a battlefield for CISOs

Author: Razvan Muresan

# Executive summary

The increasing adoption of hybrid cloud -- a mix of public cloud services and privately owned data centers, already in place for 70 percent of companies on a global level – is giving rise to new security challenges and prompting CISOs to adopt different technologies to fight zero-day exploits, advanced persistent threats, and other devastating types of cybercrime.

Six in seven IT decision makers are concerned with the security of the public cloud, and 17% do not deploy security for sensitive data stored outside the company's infrastructure. Half of those surveyed admit cloud migration has significantly expanded the size of the border they have to defend, while only one in six encrypts already migrated data.

Respondents from France, the US, and Germany fear public cloud issues most (nine in ten), while most Danish, Italian, and Swedish CISOs say they are somewhat concerned.

This study explores the pressures cloud migration place on 1,051 IT security professionals from large enterprises with 1,000+ PCs and data centers, based in the US, the UK, France, Italy, Sweden, Denmark, and Germany.

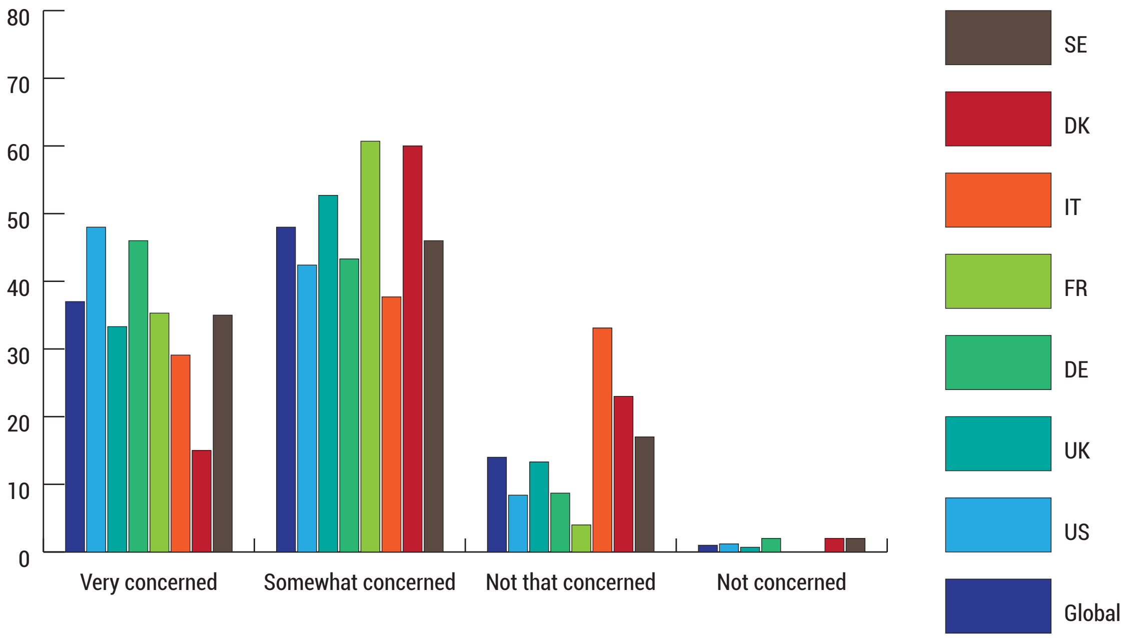
As EU's General Data Protection Regulation (GDPR) goes into effect on May 2018 — roughly eight months away — many organizations still find themselves struggling to comply. The new requirements include that data be protected adequately, and when breaches do occur organizations had better have notification capabilities in place that align with GDPR standards.

Research firm Gartner Inc. predicts that by the end of 2018 more than half of companies impacted by GDPR will not be in full compliance with the requirements.

To become GDPR compliant, companies need to identify data that falls under the regulations' control – *"any information relating to an identified or identifiable natural personal"* –, document how this data is secured, and create incident response plans.

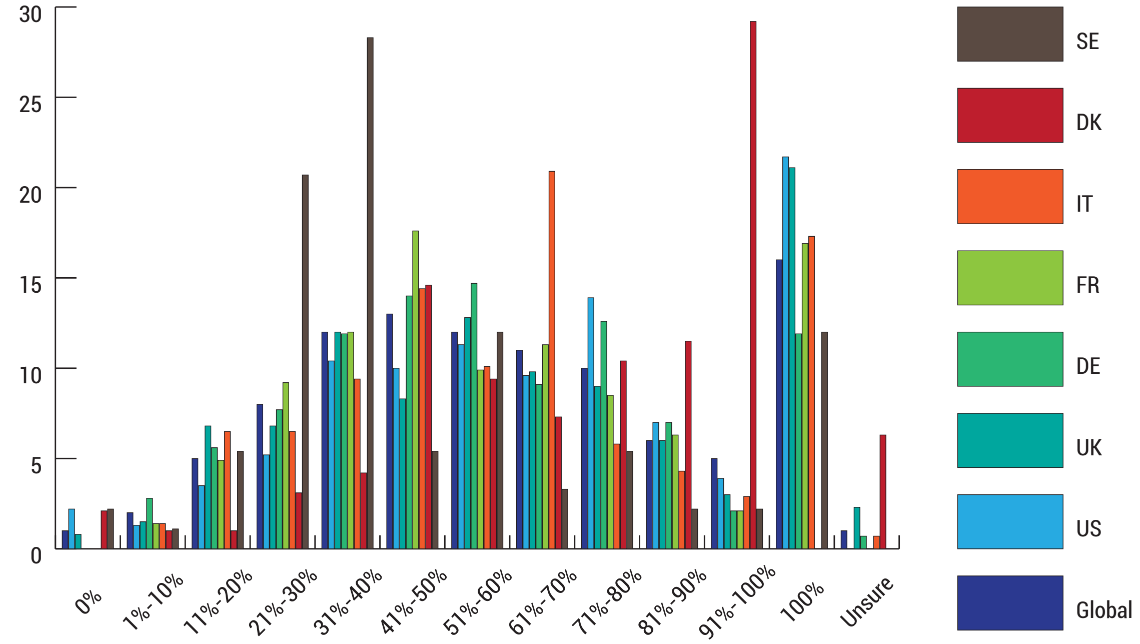
**Concerned? Yes, indeed**

| Answer | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| Very concerned | 37 | 48 | 33.3 | 46 | 35.3 | 29.1 | 15 | 35 |
| Somewhat concerned | 48 | 42.4 | 52.7 | 43.3 | 60.7 | 37.7 | 60 | 46 |
| Not that concerned | 14 | 8.4 | 13.3 | 8.7 | 4 | 33.1 | 23 | 17 |
| Not concerned | 1 | 1.2 | 0.7 | 2 | 0 | 0 | 2 | 2 |



On average, companies secure 31 to 60 percent of their data stored in the public cloud, while only one in six encrypts all data stored outside its infrastructure. Most companies that choose to encrypt all data stored off-premises are from the US and the UK, with more than a fifth of respondents, while Germany and Sweden are the low ranking countries regarding encryption of all their data from the public cloud. However, most Danish companies – more than half - secure 71 to 99 percent of data stored in the public cloud, the country with the highest results from those surveyed.

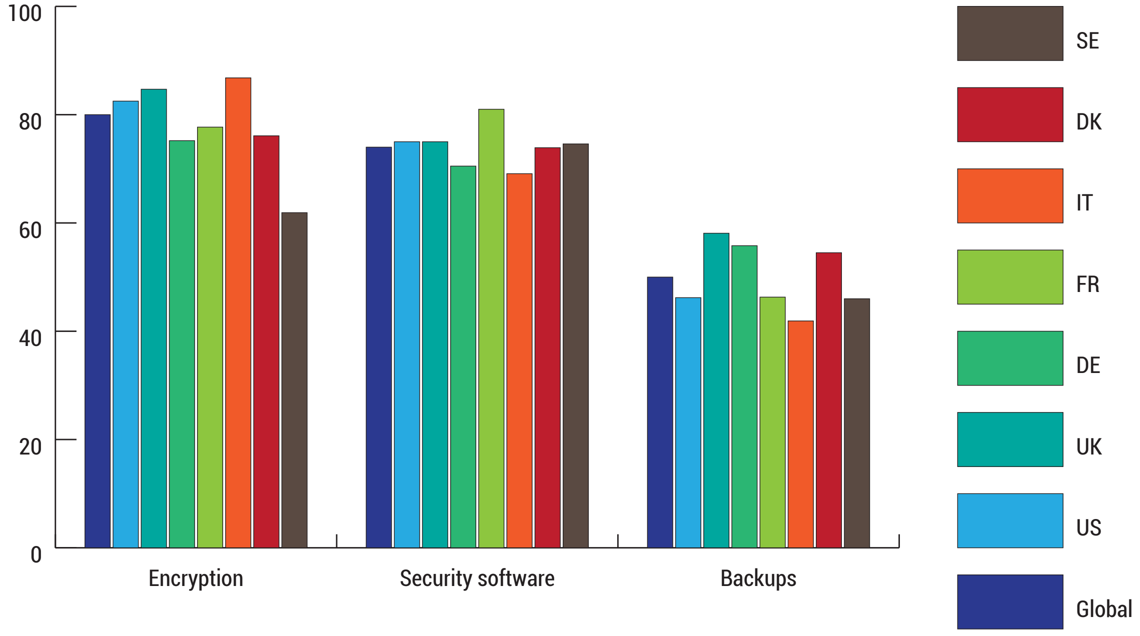
**How much of the data stored on public clouds do companies encrypt? (%)**



| *Results* | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| 0% | 1 | 2.2 | 0.8 | 0 | 0 | 0 | 2.1 | 2.2 |
| 1%-10% | 2 | 1.3 | 1.5 | 2.8 | 1.4 | 1.4 | 1 | 1.1 |
| 11%-20% | 5 | 3.5 | 6.8 | 5.6 | 4.9 | 6.5 | 1 | 5.4 |
| 21%-30% | 8 | 5.2 | 6.8 | 7.7 | 9.2 | 6.5 | 3.1 | 20.7 |
| 31%-40% | 12 | 10.4 | 12 | 11.9 | 12 | 9.4 | 4.2 | 28.3 |
| 41%-50% | 13 | 10 | 8.3 | 14 | 17.6 | 14.4 | 14.6 | 5.4 |
| 51%-60% | 12 | 11.3 | 12.8 | 14.7 | 9.9 | 10.1 | 9.4 | 12 |
| 61%-70% | 11 | 9.6 | 9.8 | 9.1 | 11.3 | 20.9 | 7.3 | 3.3 |
| 71%-80% | 10 | 13.9 | 9 | 12.6 | 8.5 | 5.8 | 10.4 | 5.4 |
| 81%-90% | 6 | 7 | 6 | 7 | 6.3 | 4.3 | 11.5 | 2.2 |
| 91%-100% | 5 | 3.9 | 3 | 2.1 | 2.1 | 2.9 | 29.2 | 2.2 |
| 100% | 16 | 21.7 | 21.1 | 11.9 | 16.9 | 17.3 | 0 | 12 |
| Unsure | 1 | 0 | 2.3 | 0.7 | 0 | 0.7 | 6.3 | 0 |

Some 80 percent of the CISOs say encryption is the most effective security mechanism to secure public-cloud-stored data, followed by security software (mentioned by 74 percent of respondents) and backups (trusted by half of those surveyed). By country, encryption is mostly trusted in Italy, the UK and the US.

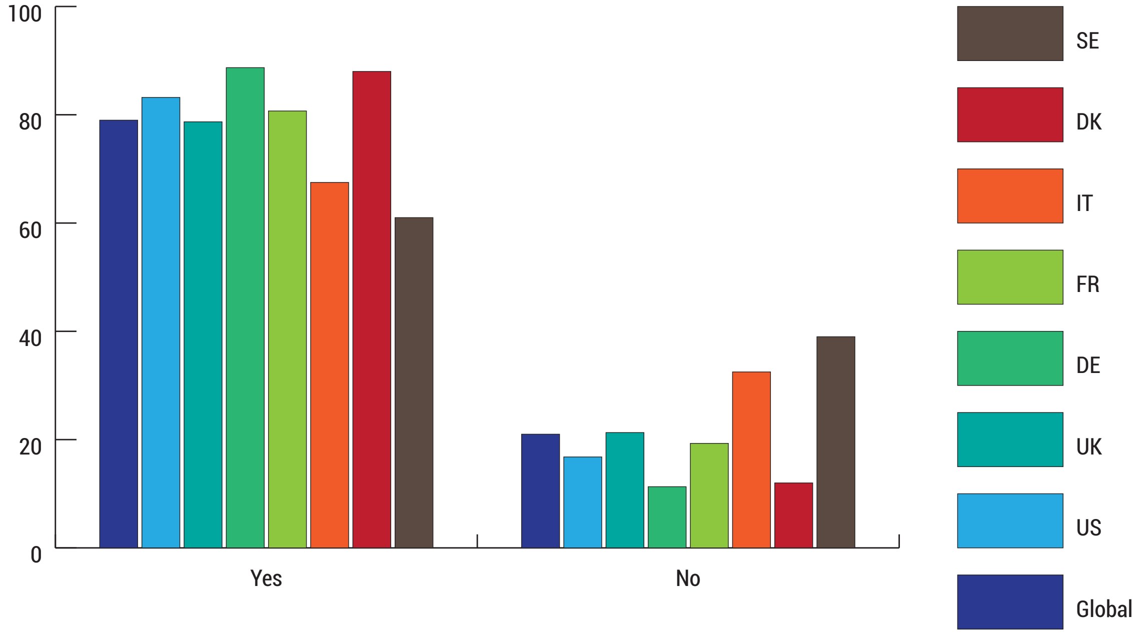
### What security mechanism do you consider effective in securing the public cloud data? (multiple answers possible - %)



| *Results* | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| Encryption | 80 | 82.5 | 84.7 | 75.2 | 77.7 | 86.8 | 76.1 | 61.9 |
| Security software | 74 | 75 | 75 | 70.5 | 81 | 69.1 | 73.9 | 74.6 |
| Backups | 50 | 46.2 | 58.1 | 55.8 | 46.3 | 41.9 | 54.5 | 46 |

Another area of concern is that 17 percent of CISOs do not deploy security in the public cloud, while 21 percent do not encrypt data in transit from their own data center toan external one.

### Do you encrypt in-transit data? (%)



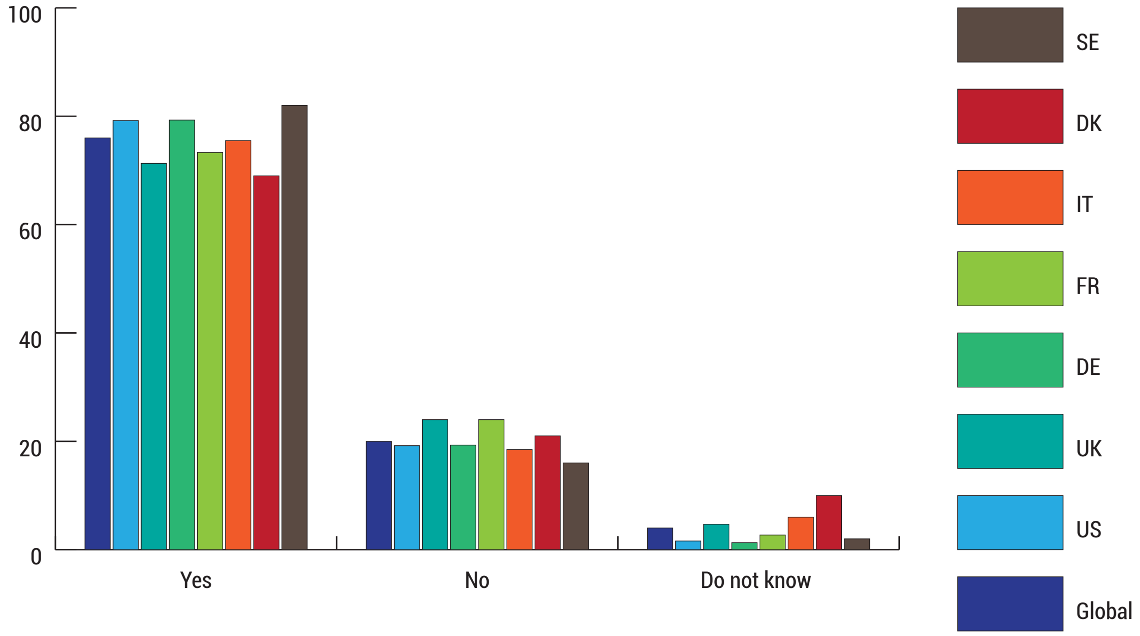
| *Results* | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| Yes | 79 | 83.2 | 78.7 | 88.7 | 80.7 | 67.5 | 88 | 61 |
| No | 21 | 16.8 | 21.3 | 11.3 | 19.3 | 32.5 | 12 | 39 |

# Encryption, encryption, encryption

Bitdefender security specialists recommend that any data transfer between the client and the cloud service provider be encrypted to avoid man-in-the-middle attacks that could intercept and decipher all broadcasted data. Beyond 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.

The survey also shows that 76 percent of IT decision makers use the same endpoint security solution to protect physical and virtual infrastructures, but 20 percent have implemented separate tools. Out of those, 76 percent do it to protect sensitive customer and consumer data, 70 percent cite compliance with internal and regulatory requirements, and 51 percent want to prevent service interruptions resulting from attacks.

**Do you use the same endpoint security solution to protect physical, virtual on-premises, and cloud-based machines? (%)**



| *Results* | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| Yes | 76 | 79.2 | 71.3 | 79.3 | 73.3 | 75.5 | 69 | 82 |
| No | 20 | 19.2 | 24 | 19.3 | 24 | 18.5 | 21 | 16 |
| Do not know | 4 | 1.6 | 4.7 | 1.3 | 2.7 | 6 | 10 | 2 |

# Tailor-made security against crafted cyber weapons

Bitdefender security specialists strongly advise CISOs to use a security solution specifically designed for the infrastructure it will run on (physical or virtual) instead of a single tool for three main reasons:

- It generates overhead: installing an endpoint solution on different virtual machines hosted on the same servers impacts resources by continuously running redundant apps, like security agents.

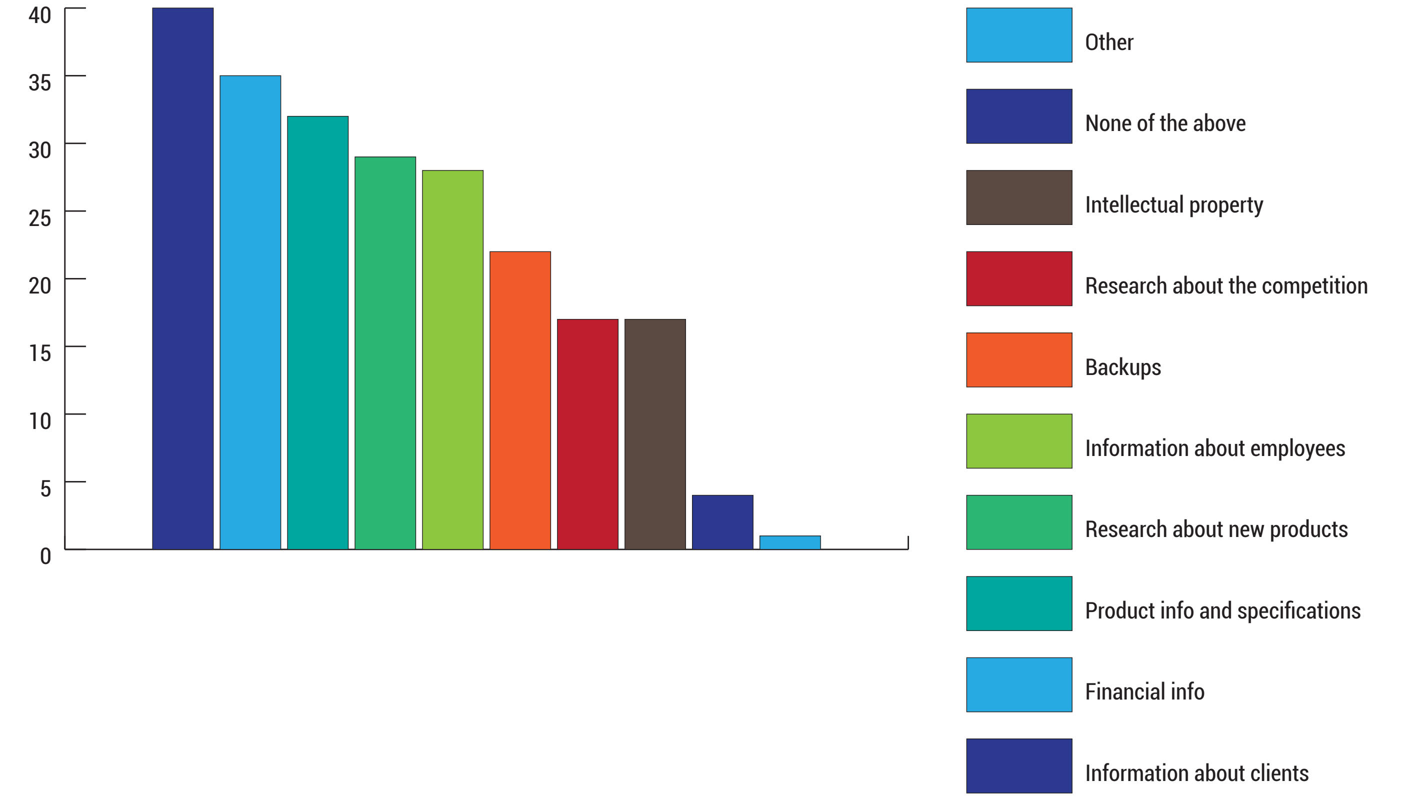
- It significantly reduces performance: security tools tailored for virtual environments use optimized agents that integrate with a security virtual appliance on server/servers, so previously scanned files are not rescanned each time a user needs them.

- The typology of attacks is different: boot time security-coverage gaps leave the system vulnerable to malware attacks. As a result, virtual environments often face more sophisticated cyber weapons, such as advanced persistent threats, and targeted attacks, aiming at both companies and government entities (such as APT-28 and, just recently, Netrepser). In this respect, security for virtualized environments is by far the most effective way to detect and fight these complex tools.

## What's stored in the public cloud must not go public

Companies mostly store in the public cloud information about clients (48 percent), product information (45 percent), and financial data (44 percent), and avoid storing off-premise what they perceive to be more sensitive data (i.e. research into new products and competition – 34 percent and 28 percent, respectively; backups - 27 percent; intellectual property - 24 percent). Thus, companies encrypt more often information about clients (40%), financial info (35%), product info and specs (32%) than backups (22%), research into competitors (17%) and intellectual property (17%).

**What data stored on public clouds do you encrypt? (global results - %)**



| | |
|---|---|
| Information about clients | 40 |
| Financial info | 35 |
| Product info and specifications | 32 |
| Research about new products | 29 |
| Information about employees | 28 |
| Backups | 22 |
| Research about the competition | 17 |
| Intellectual property | 17 |
| None of the above | 4 |
| Other | 1 |

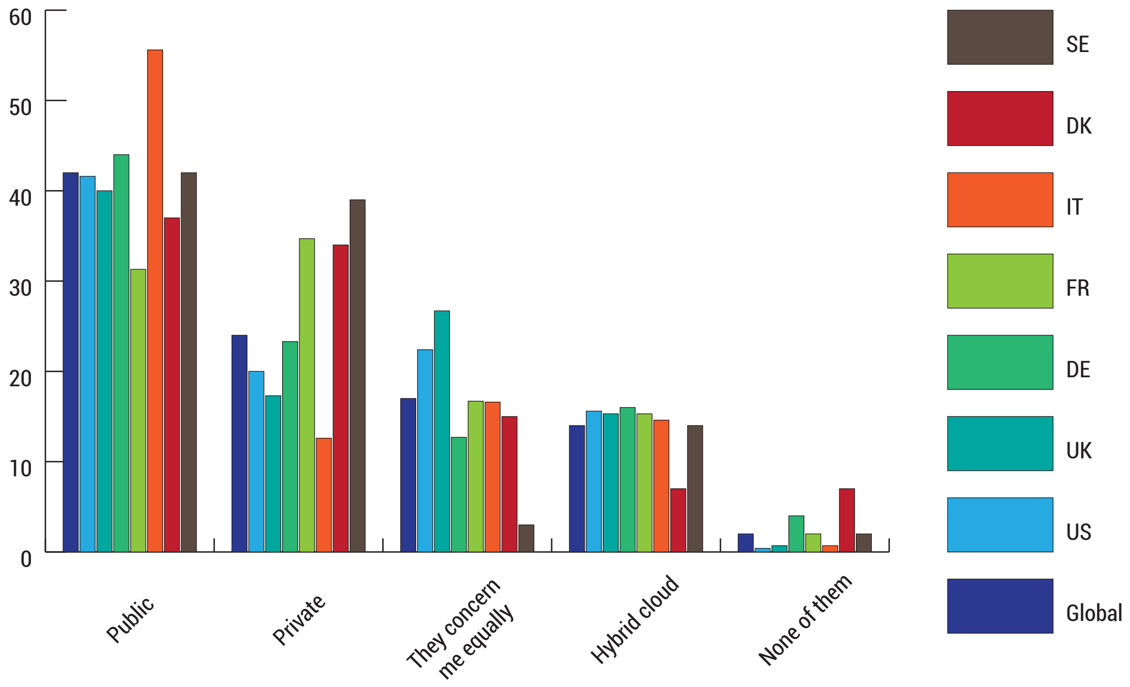
## Hybrid cloud brings hybrid issues

Bitdefender security specialists recommend that, when opting for a hybrid cloud solution, an organization must analyze the type of data it handles and evaluate it based on its sensitivity – both for the company and its clients. Critical, personal and private data related to intellectual property must be stored on premise, with access only to authorized personnel. Organizations that handle sensitive or confidential data, or data related to intellectual property, need to ensure their private cloud infrastructure remains private. No one outside the local network should be able to access that data and only authorized personnel should be vetted for handling it. The private cloud needs to be completely isolated from public internet access to prevent attackers from remotely accessing the data through security vulnerabilities.

In terms of security challenges, 42 percent of CISOs say that public cloud is their major concern and private cloud comes second (24 percent). Another 17 percent say they are equally concerned about both. CISOs in Italy are concerned with public cloud security challenges most, followed by Germans and Swedes.

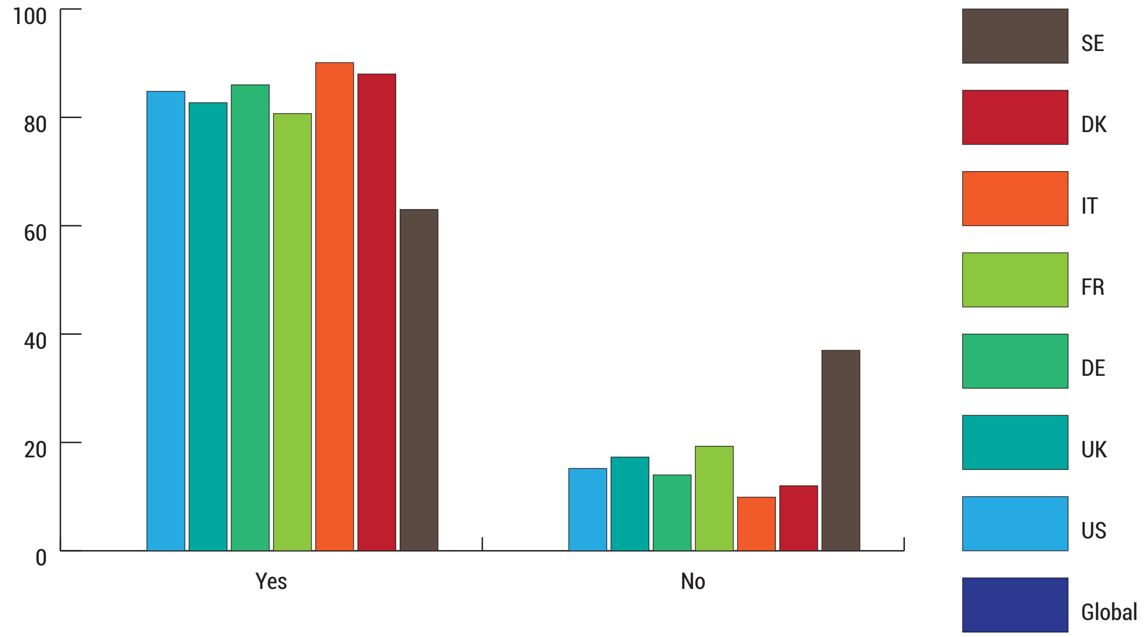
“The risk of being GDPR non-compliant means not only negative publicity and damage to the companies’ reputation as it has been until now, but also penalties that can total up to 4% of a company’s global annual revenue,” Bitdefender’s Senior eThreat Analyst Bogdan Botezatu says. “With 2017 having already set new records in terms of magnitude of cyberattacks, boards should be aware that it’s only a matter of time until their organization will be breached since most still lack efficient security shields.”

**Which of the following are you more concerned with in terms of security challenges? (%)**



| *Answer* | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| Public | 42 | 41.6 | 40 | 44 | 31.3 | 55.6 | 37 | 42 |
| Private | 24 | 20 | 17.3 | 23.3 | 34.7 | 12.6 | 34 | 39 |
| They concern me equally | 17 | 22.4 | 26.7 | 12.7 | 16.7 | 16.6 | 15 | 3 |
| Hybrid cloud | 14 | 15.6 | 15.3 | 16 | 15.3 | 14.6 | 7 | 14 |
| None of them | 2 | 0.4 | 0.7 | 4 | 2 | 0.7 | 7 | 2 |

**Do you deploy security in the public cloud? (%)**



| *Answer* | *Global* | *US* | *UK* | *DE* | *FR* | *IT* | *DK* | *SE* |
|---|---|---|---|---|---|---|---|---|
| Yes | 83% | *84.8* | *82.7* | *86* | *80.7* | *90.1* | *88* | *63* |
| No | 17% | *15.2* | *17.3* | *14* | *19.3* | *9.9* | *12* | *37* |

Lack of infrastructure-agnostic security, lack of predictability, and lack of visibility are perceived as top security challenges of cloud adoption by half of the companies surveyed.

Gartner recommends that companies focus on five high-priority areas in order to be ready to meet GDPR requirements.

First, they should determine their role under the GDPR. As mentioned, the regulation applies not only to businesses in the EU but to organizations outside the region that process personal data for the offering of goods and services to the EU.

Second, appoint a data protection officer. In fact, many organizations are required to appoint such an officer, a step that's especially important if the organization is a public body, processes operations that require regular monitoring, or has large-scale processing activities, Gartner said.

Third, demonstrate accountability in all processing activities. Data quality and relevance should be decided upon when starting a new processing activity, Gartner said. This will help companies to maintain compliance in future personal data processing activities.

Fourth, check cross-border data flows. Data transfers to any of the 28 EU member states are still allowed, as are transfers to other countries the European Commission (EC) has deemed to have an "adequate" level of protection, Gartner noted. Outside of these areas, appropriate safeguards should be used.

Finally, prepare or data subjects exercising their rights. Data subjects have extended rights under the regulation, Gartner said, including the right to be forgotten, to data portability and to be informed of data breaches. If a company is not prepared for subjects exercising their rights, this is the time to begin implementing needed controls.

# Methodology

The survey, conducted in April-May 2017 by Censuswide for Bitdefender, included 1,051 IT security purchase professionals from large enterprises with 1,000+ PCs and data centers, based in the US, the UK, France, Italy, Sweden, Denmark, and Germany.

# 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/

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/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com