US companies' experience and attitudes towards security threats

Quantitative survey within Large and Medium companies in the USA

MillwardBrown

Bitdefender

Objectives

- **Determine the existing experience and attitudes towards security attacks of large and medium companies in the USA**
  - *Security features used most;*
  - *Endpoint security capabilities used most;*
  - *Level of custom security software equipment;*
  - *Experience with determined set of attacks;*
  - *Impact of determined set of attacks on business areas;*
  - *Level of virtualization;*
  - *Information process;*

Key findings

- **Firewall and anti-virus/malware** are the features used mostly by the companies that were interviewed. Performance in **prevention is the benefit valued the most**, but also the power of limiting the impact while security solutions are in use.

- **All investigated types of attacks** are perceived as **relatively equally hard** to detect and mitigate. Still, **APT types** are **having the edge**, almost 1 in 5 large and medium companies mentioning it.

- **Password cracking** is, out of the tested types of threats, the one **experienced very recent** (last 3 months) **by the most** (25%) of the interviewed companies.

- Overall, the areas with the **highest impact** after attacks occur, are related to **time spent** (either with Help Desk or in-house IT support) and that of **employee productivity**.

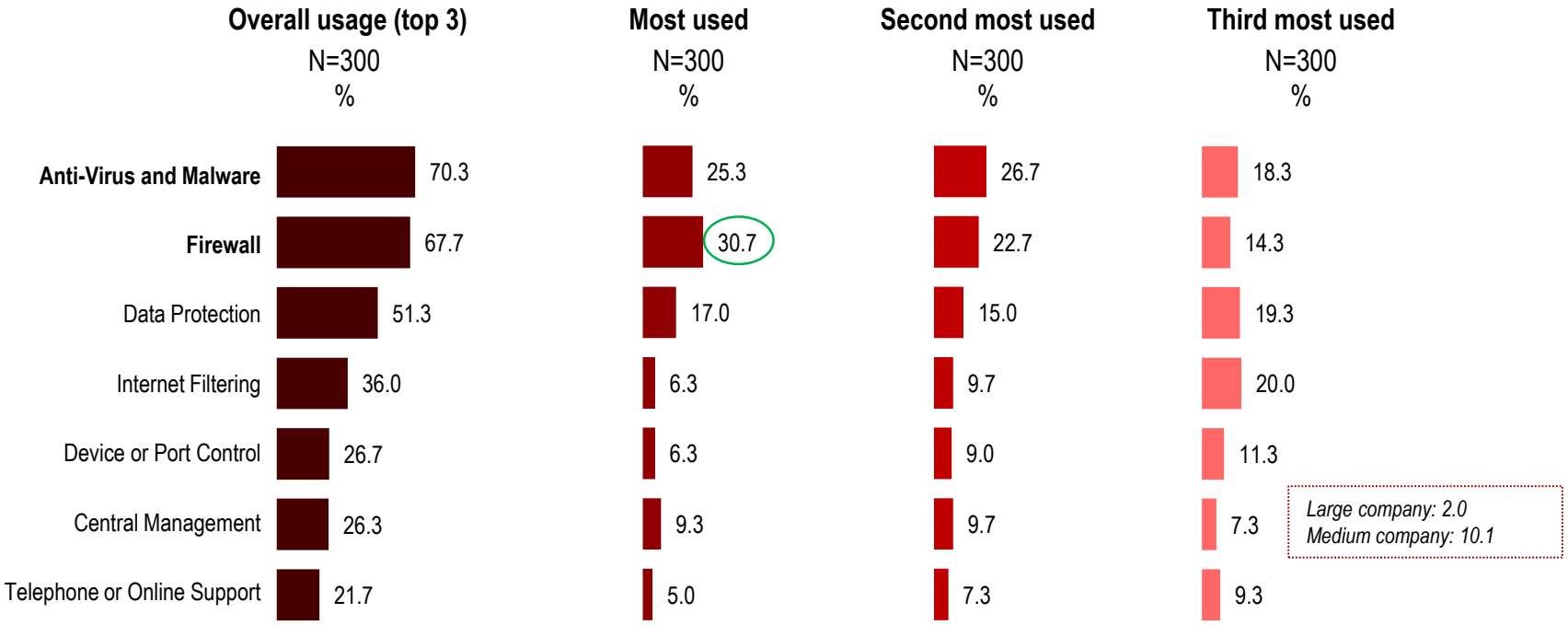
- Only **15% of the companies are currently fully virtualized**, but about 47% of them are only partially virtualized but are seeking to become more in the future.

- On the whole, slightly more than the average (**55%) of the companies are managing IT functions fully in-house**, while only 15% of them outsource them entirely.

- Dual model of information process: either targeted, on providers website or exploring using search engines.

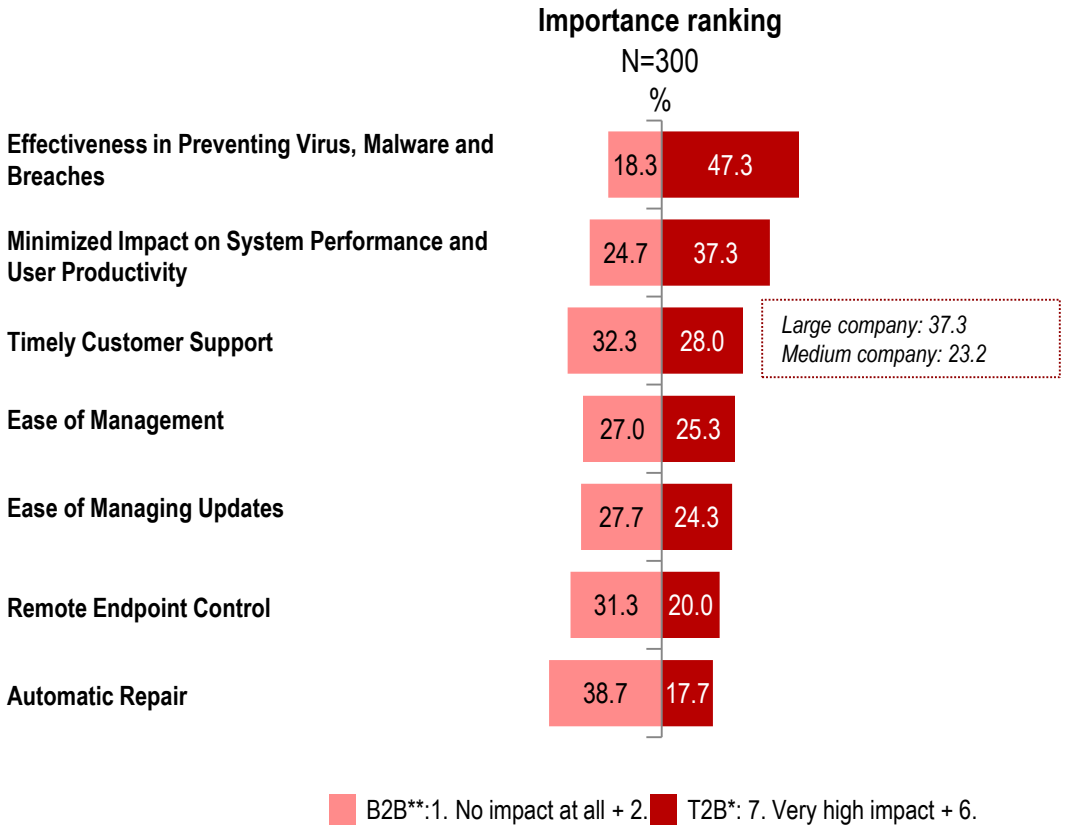
Results

Firewalls are the feature used the most - almost a third of the companies using them the most. Anti-virus/malware are used second most often.



Q13. Please select out of the following endpoint security features the top 3 ones that you leverage most in your organization.

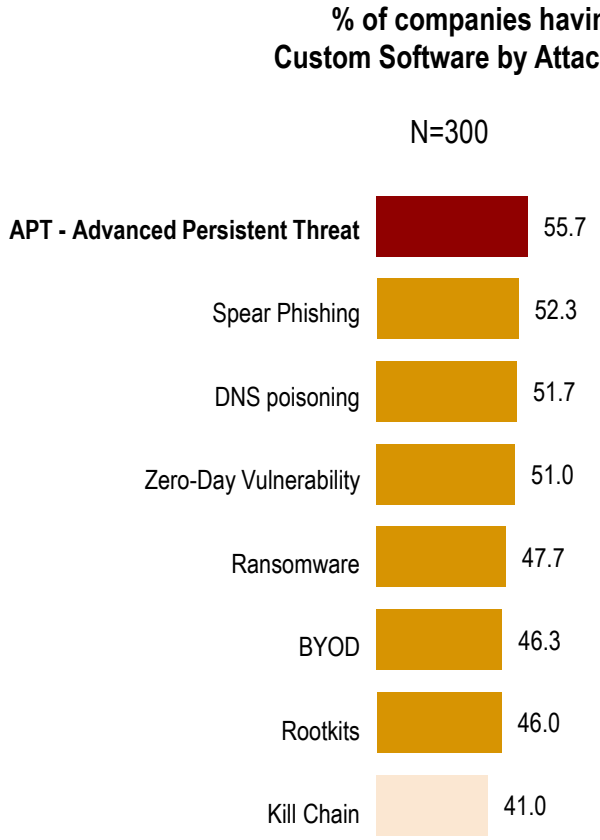
Technical performance of the solution as well as low impact on productivity are key. Large companies are looking more for timely customer support than medium ones.



Scale: 1. No impact at all … 7. Very high impact

Q14. Considering the endpoint capabilities below, please rank them by order of importance to you.

On average, the target audience companies use custom software for 4 types of threats. Most common are those against APTs, while for Kill Chain are least used.

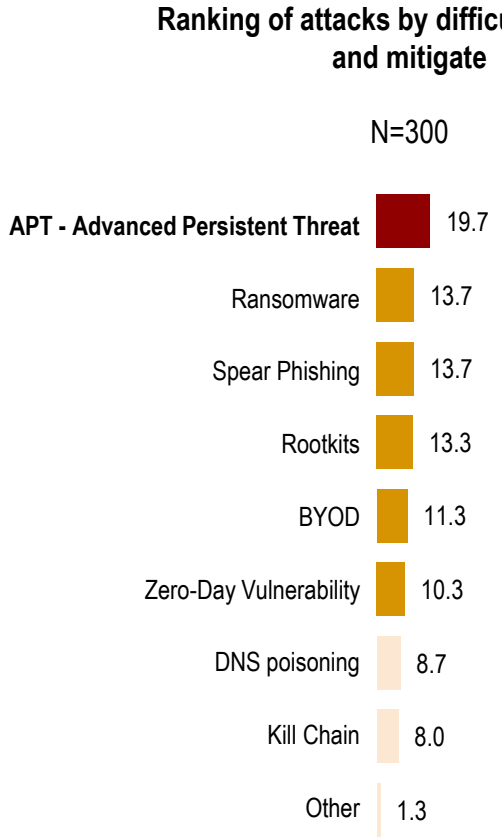


OTHER INFORMATION LAYERS:

- there are no significant differences by company size;
- have significantly more custom software companies with *high virtualization level* and those that had experienced *high impact* of previous attacks;

Q1. Does your organization have custom software to address each of the following attacks?

APTs are the attacks that seem to pose most of difficulties to the companies' security.



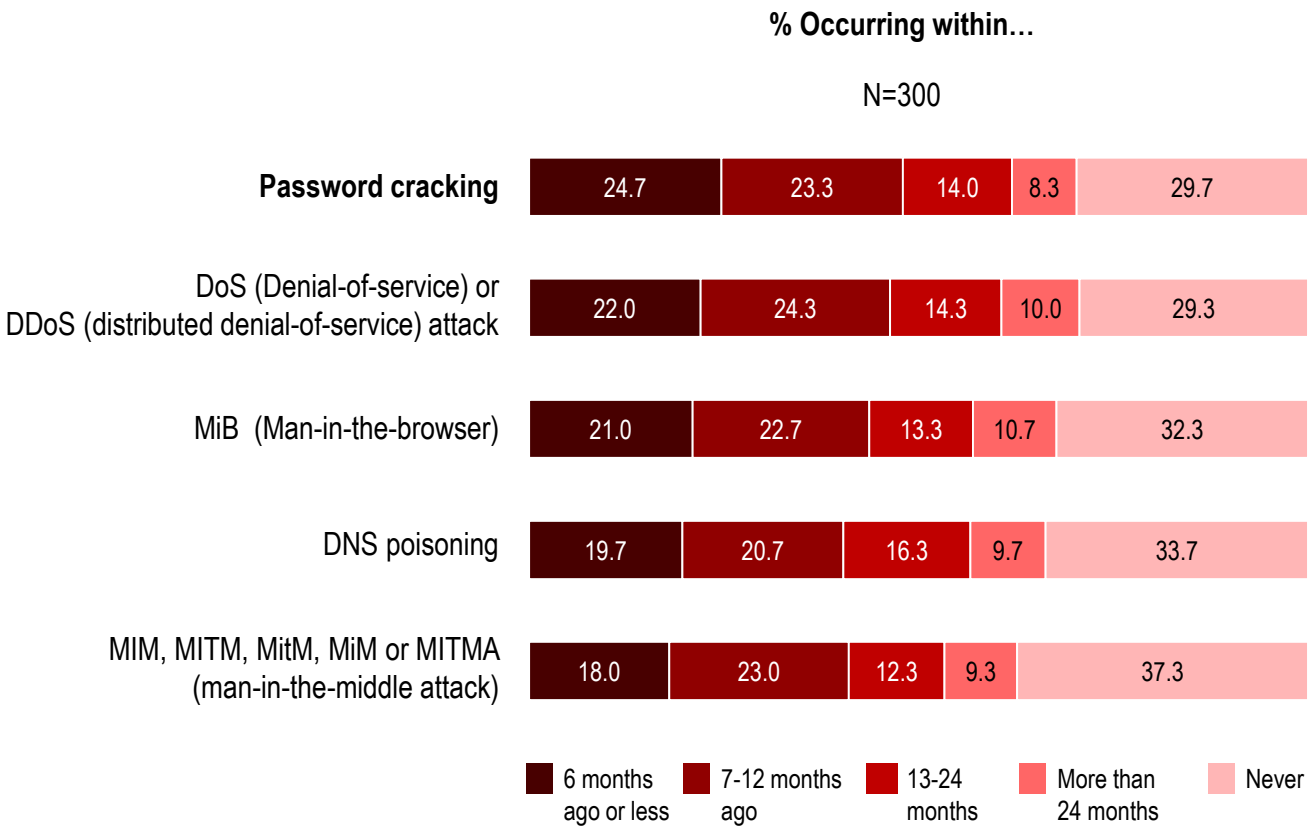
OTHER INFORMATION LAYERS:

- There are some risks towards *Ransomware* and *Rootkits* type of attacks – they rank relatively higher by difficulty compared to their ownership ranking seen previously;
- On the other hand, in the case of *Zero-Day Vulnerability* and *DNS poisoning* companies although feeling more confident, more are using software to protect from them.

- Companies with *limited attach experience* consider *Ransomware* and *Rootkits* as being more difficult to tackle. The latter is perceived as more difficult by companies with not so recent attack experiences.

Q2. In your opinion, what attack type is the hardest to detect and mitigate?

Password cracking is the attack experienced most recently by a quarter of all companies interviewed. *Man in the middle* attack are experienced least from the set analyzed.



Q3. When did your organization last register each of the following online attacks?

MiB and DNS poisoning attack have greater impact on help desk/support, while DoS and Password cracking on IT time support. Commercial loss is less mentioned, being not as visible to IT maybe. Still, employee productivity ranking high, points to potential commercial losses.

Business Areas Ranked by highest average impact (irrespective of attack type)

Business Areas most impacted on average

Business Areas least impacted on average

	N*=66 %	N*=74 %	N*=54 %	N*=63 %	N*=59 %
	DoS or DDoS attack	**Password cracking**	**MIM, MITM, MitM, MiM or MITMA**	**MiB**	**DNS poisoning**
Increased Help Desk/Support Calls	28.8	27.0	29.6	**34.9**	**39.0**
Employee productivity	30.3	23.0	**35.2**	**34.9**	32.2
Increased time for IT support	**33.3**	**32.4**	22.2	31.7	33.9
System Downtime	30.3	23.0	22.2	33.3	**35.6**
Data leakage	22.7	21.6	27.8	33.3	33.9
Regular business processes interruptions	28.8	21.6	25.9	**34.9**	27.1
Lost data / files	30.3	28.4	22.2	27.0	25.4
Increased System Reimage	25.8	17.6	**33.3**	30.2	25.4
Expenses for remediation specialist services (lawyers, IT security professionals, etc.)	21.2	28.4	24.1	28.6	25.4
Commercial loss (lost contracts, due compensations, etc.)	19.7	21.6	31.5	23.8	27.1

T2B*: 7. Very high impact + 6.

Base*: Respondents that experienced this type of attack in the past 6 months

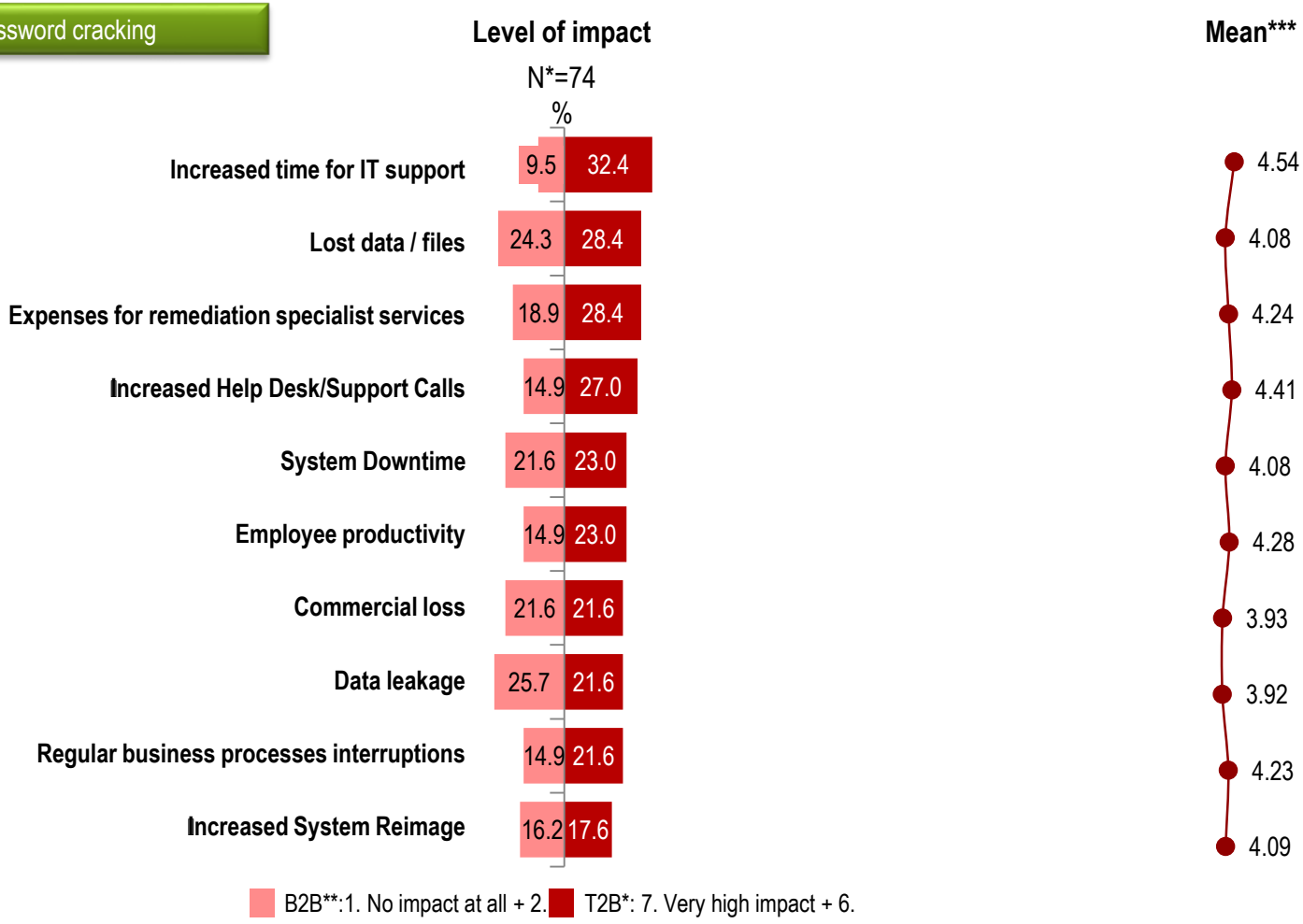
Mean***: Scale: 1. No impact at all … 7. Very high impact

Small base size – Treat results with caution

Q4. For each of the areas below please estimate the extent of impact of the last [INSERT Q3_i] attack that your organization experienced.

Time for IT support is the area impacted most by *Password cracking* type of attacks while reimaging system is less affected.

Business Areas Impacted - Password cracking



Base*: Respondents that experienced this type of attack in the past 6 months

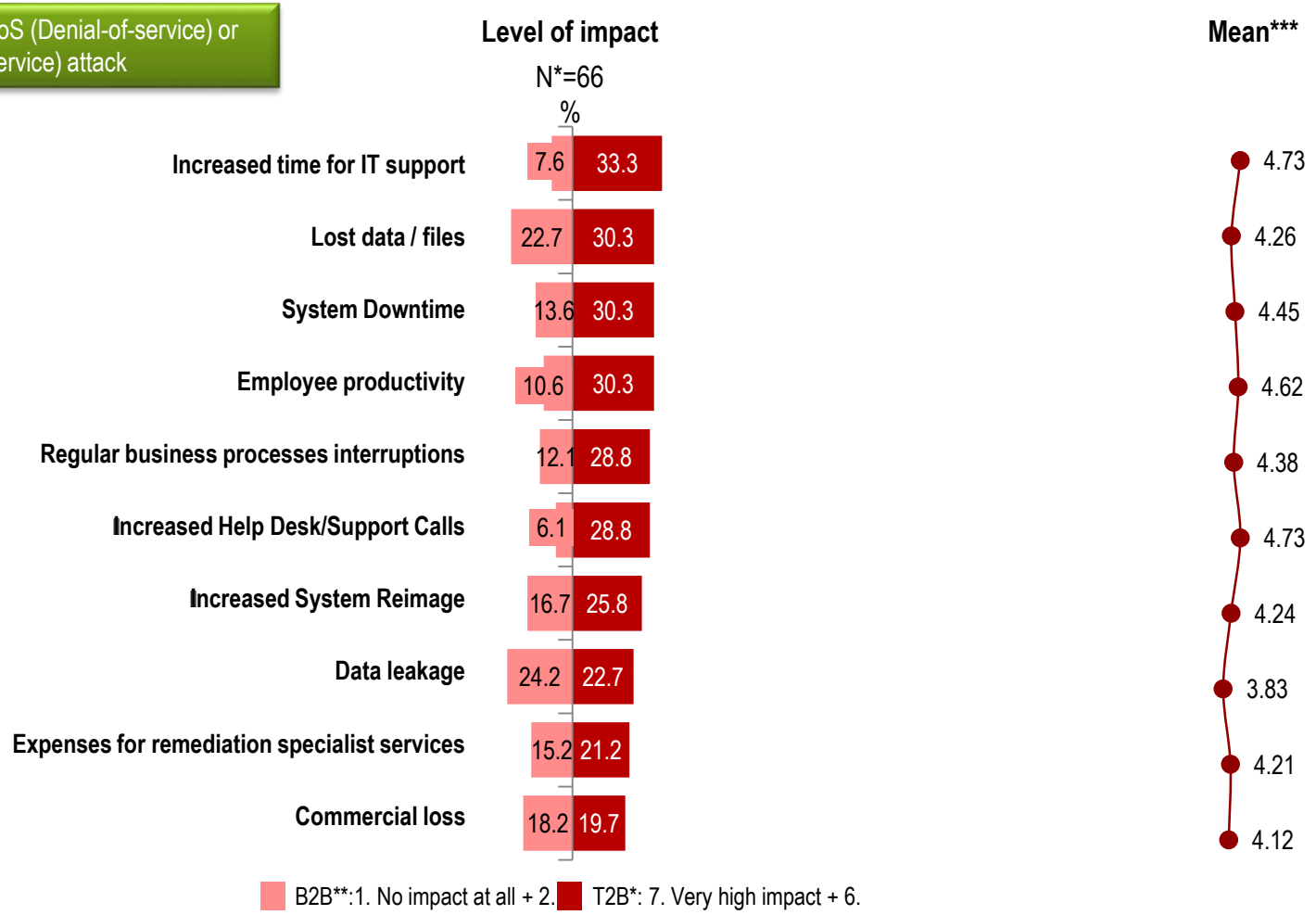
Mean***: Scale: 1. No impact at all … 7. Very high impact

Small base size – Treat results with caution

Q4. For each of the areas below please estimate the extent of impact of the last [INSERT Q3_i] attack that your organization experienced.

Similarly for DoS attacks - IT support is the area impacted in the case of most, but also losing data, system downtimes/employee productivity

Business Areas Impacted - DoS (Denial-of-service) or DDoS (distributed denial-of-service) attack



Base*: Respondents that experienced this type of attack in the past 6 months

Mean***: Scale: 1. No impact at all … 7. Very high impact

Small base size – Treat results with caution

Q4. For each of the areas below please estimate the extent of impact of the last [INSERT Q3_i] attack that your organization experienced.

MiB attacks impact almost all areas equally.

Business Areas Impacted - MiB (Man-in-the-browser)

Base*: Respondents that experienced this type of attack in the past 6 months

Mean***: Scale: 1. No impact at all … 7. Very high impact

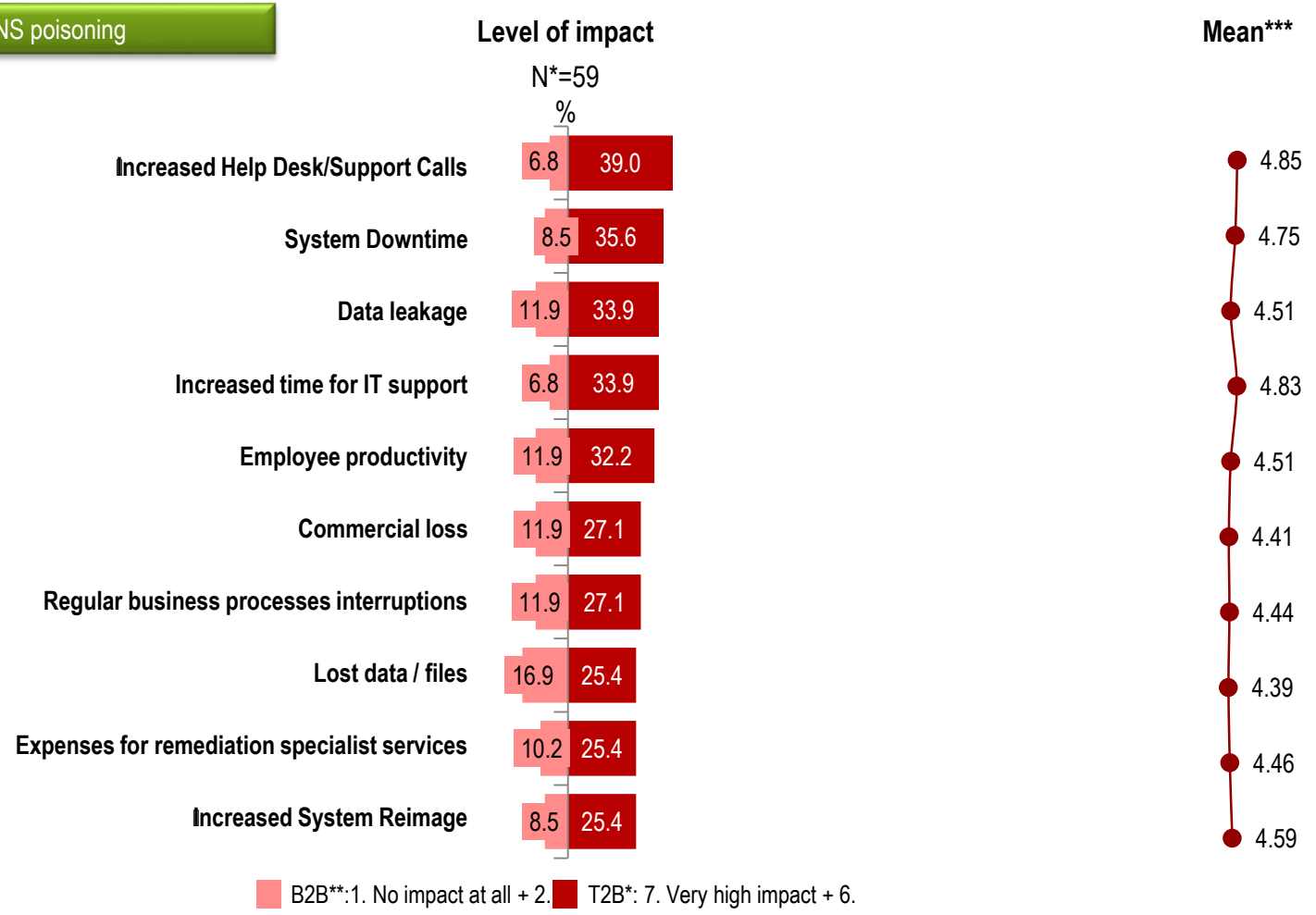
Small base size – Treat results with caution

Q4. For each of the areas below please estimate the extent of impact of the last [INSERT Q3_i] attack that your organization experienced.

When DNS poisoning attacks happen, reaching for the Help Desk is needed mostly.

Bitdefender

Business Areas Impacted - DNS poisoning



Base*: Respondents that experienced this type of attack in the past 6 months

Mean***: Scale: 1. No impact at all … 7. Very high impact

Small base size – Treat results with caution

Q4. For each of the areas below please estimate the extent of impact of the last [INSERT Q3_i] attack that your organization experienced.

MillwardBrown

In the case of man-in-the-middle attacks, productivity and system reimage are the two most impacted areas.

Business Areas Impacted - MIM, MITM, MitM, MiM or MITMA (man-in-the-middle attack)

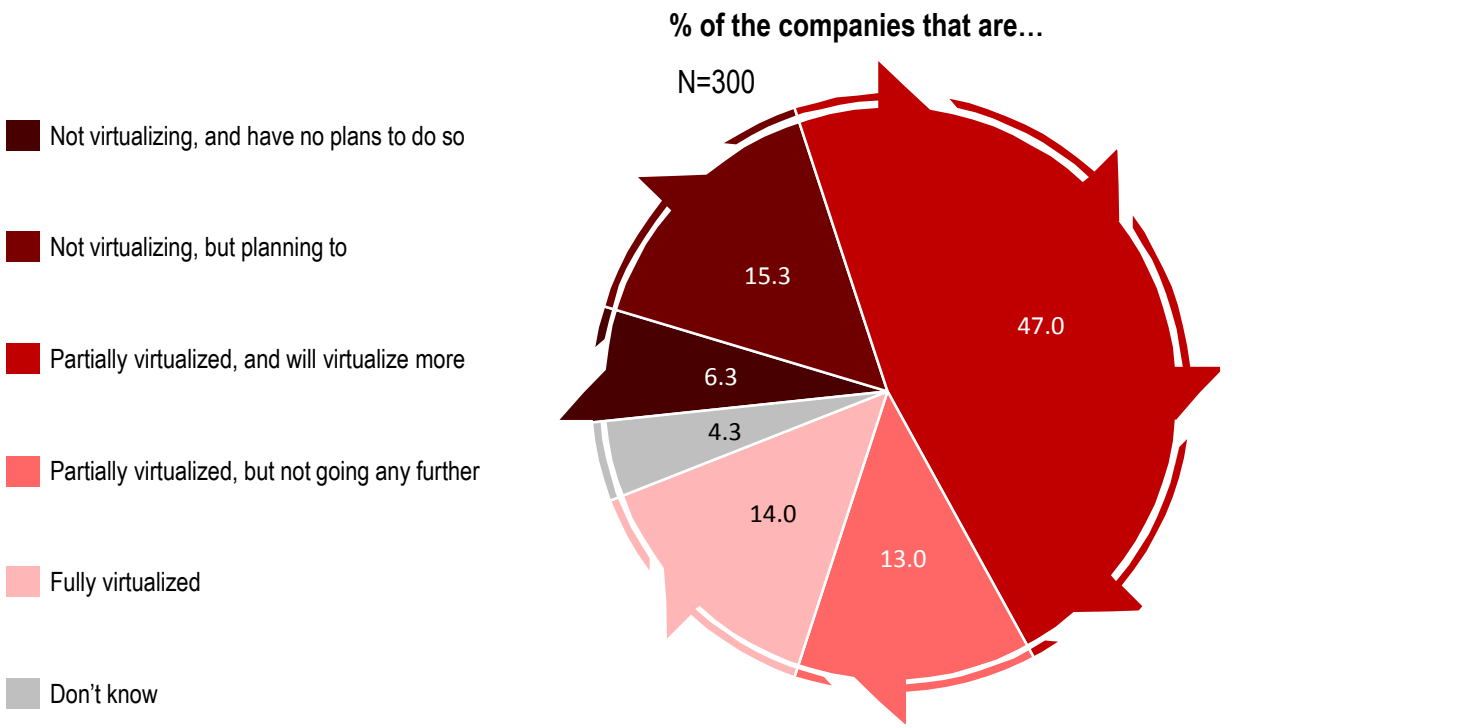
Base*: Respondents that experienced this type of attack in the past 6 months

Mean***: Scale: 1. No impact at all … 7. Very high impact

Small base size – Treat results with caution

Q4. For each of the areas below please estimate the extent of impact of the last [INSERT Q3_i] attack that your organization experienced.

Only 14% of the companies investigated are fully virtualized.

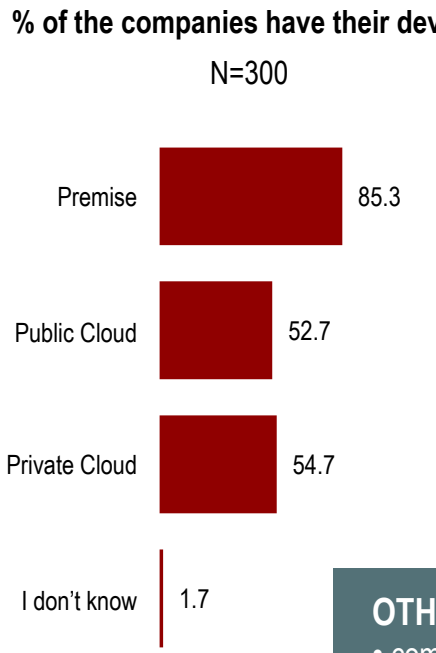


OTHER INFORMATION LAYERS:

- higher virtualization levels are recorded among companies with *wider range* of custom software and among those recording a *higher impact* of attacks.

Q5. Which of the following statements best describes where your organization is in terms of its current virtualization level and future intentions?

Confirming the state of virtualization, only about 15% of companies are having devices on cloud.

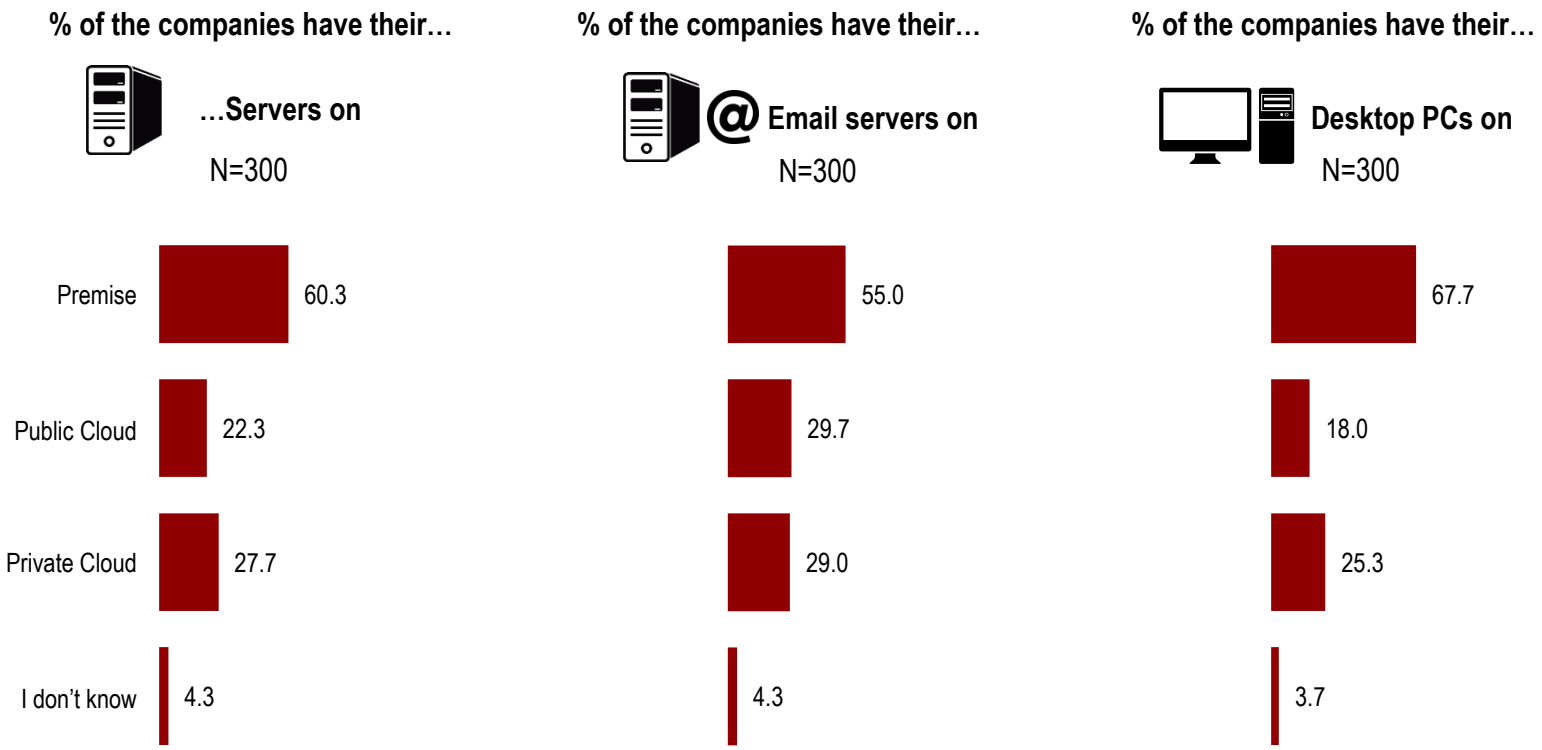


OTHER INFORMATION LAYERS:

- companies with extensive attacks experience are having more devices on cloud (either private or public).

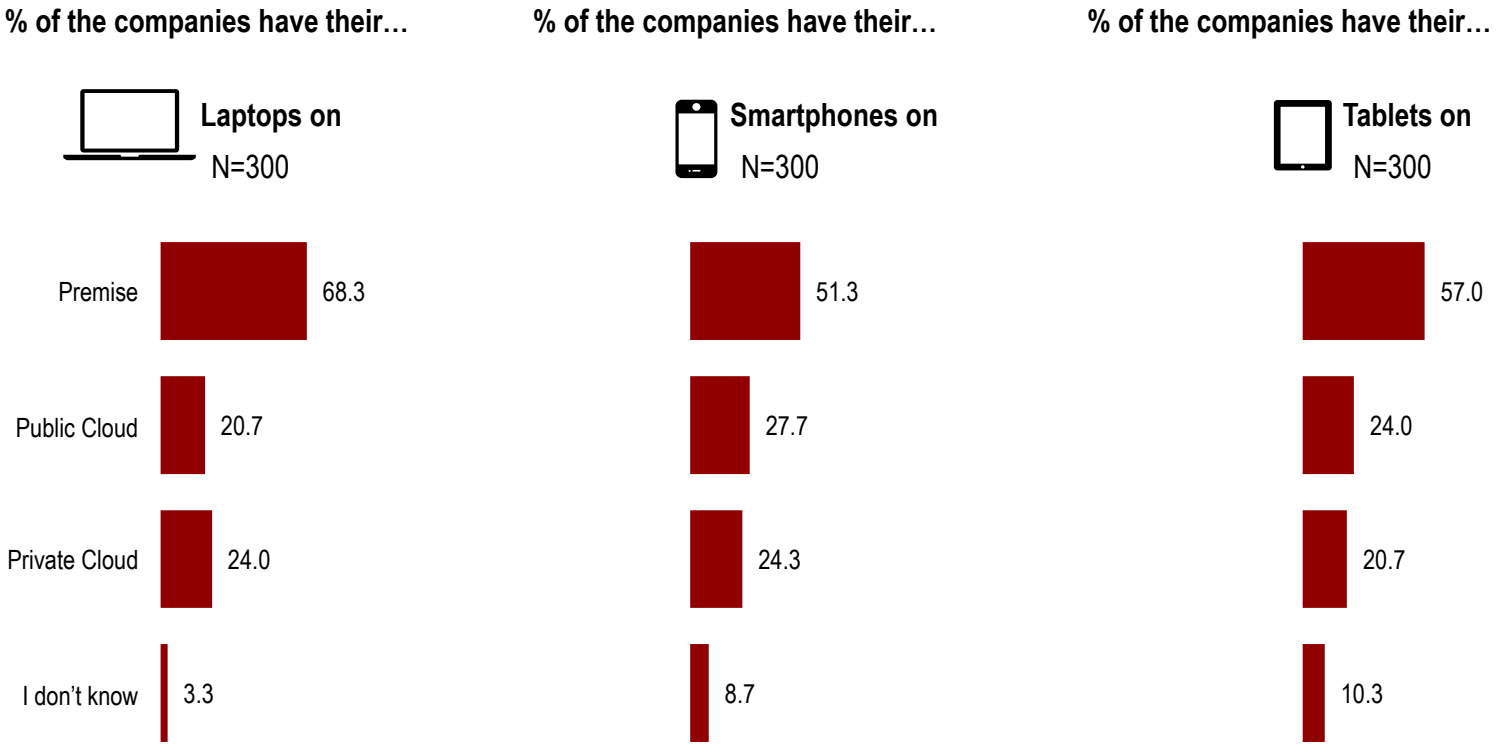
Q6. What type of security solution does your organization have for each of the following internet connected devices?

Still the majority of companies have their devices on premise. Private cloud is used slightly more.



Q6. What type of security solution does your organization have for each of the following internet connected devices?

In case of laptops we notice the highest number of companies keeping them on premise. Target audience is less aware of the state of their company smartphones and tablets compared to other devices.



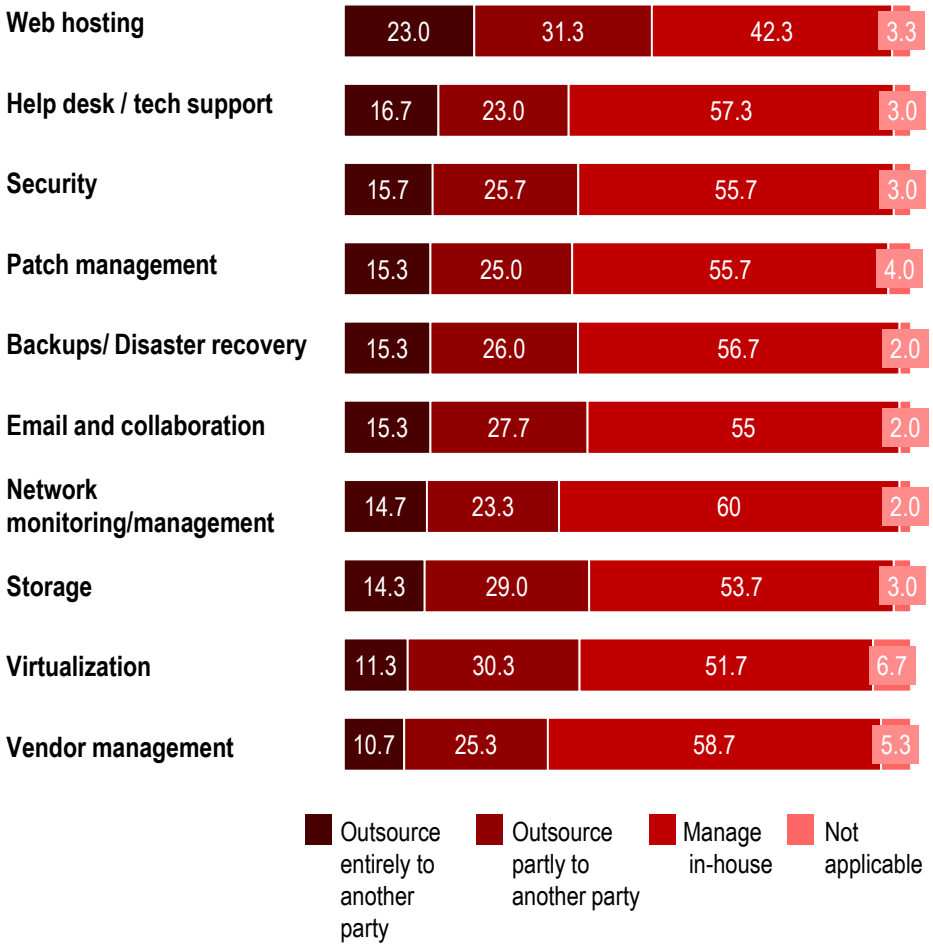
Q6. What type of security solution does your organization have for each of the following internet connected devices?

Within the companies interviewed, only 15% of them outsource their IT entirely. Web hosting is the function outsourced most, while Vendor management the least.

Bitdefender

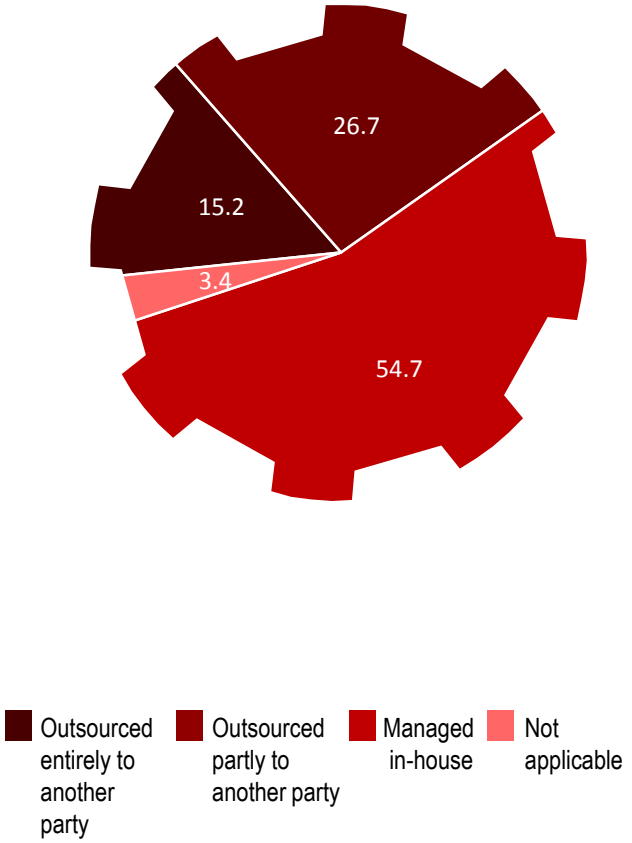
% IT Functions Handling Type

N=300



% Overall handling of IT

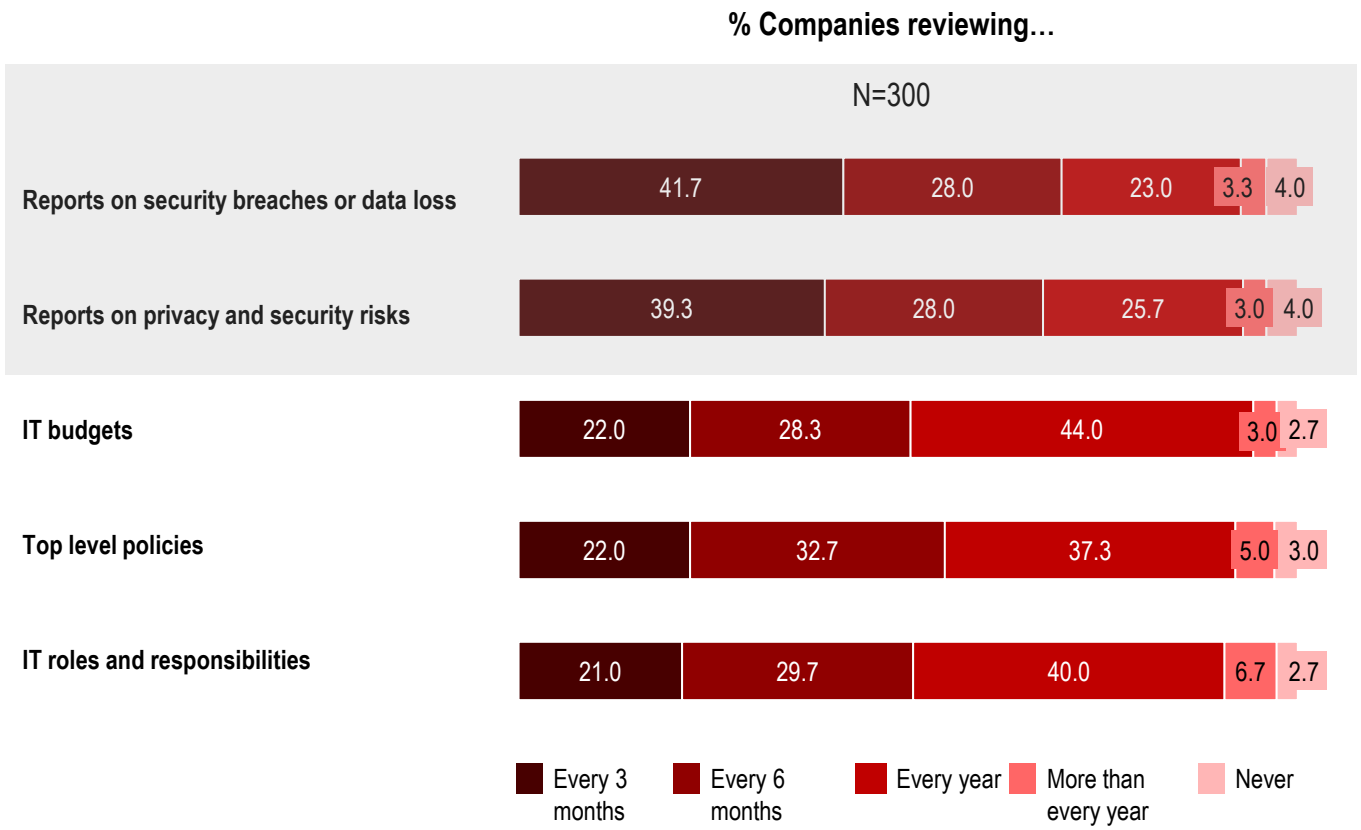
N=300



Q8. Which of the following best describes how your organization handles the IT functions below?

MillwardBrown

There is a constant focus on security, activities in this area are reviewed most frequently.

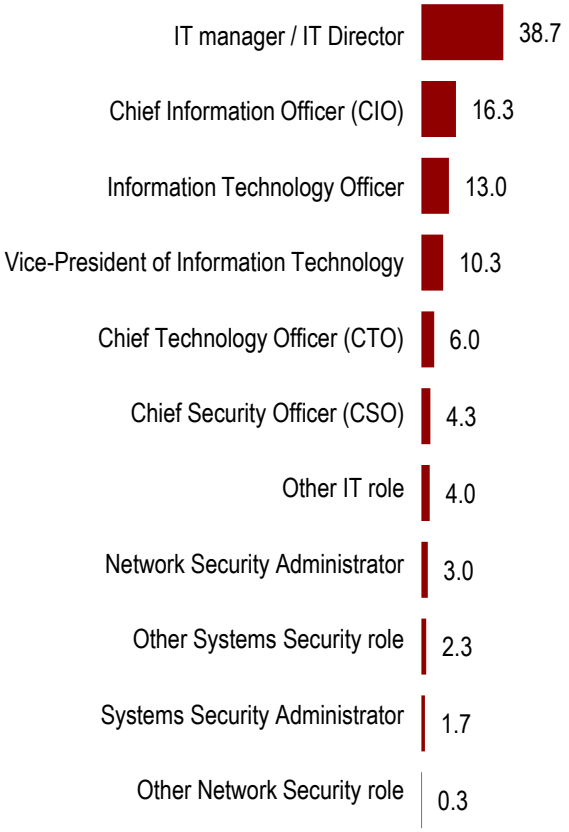


Q11. How often does your company review each of the following aspects related to the IT or IT&C department and its activities?

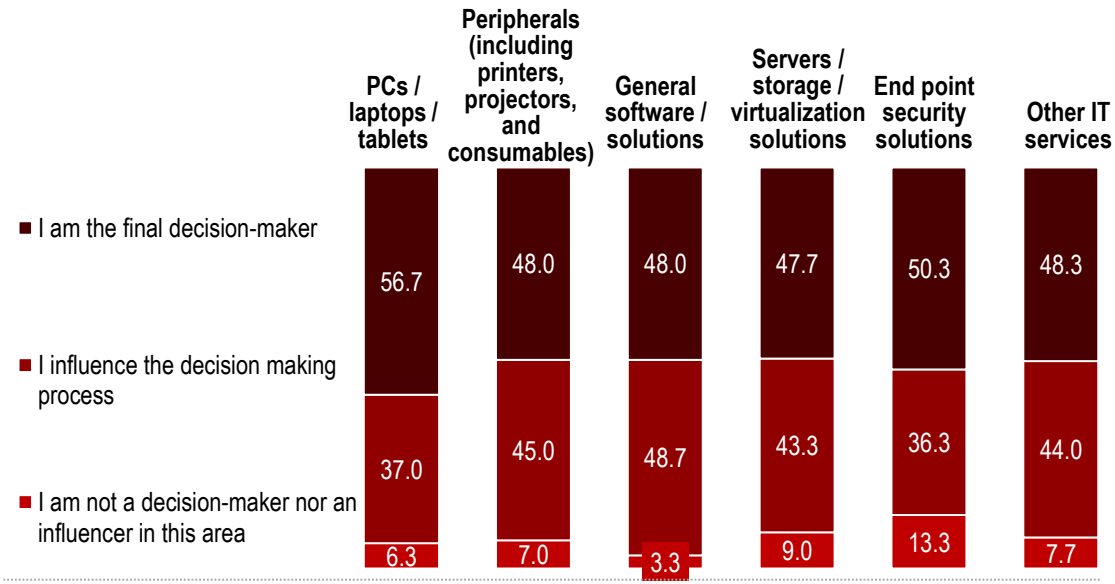
Sample Profile

N=300
%

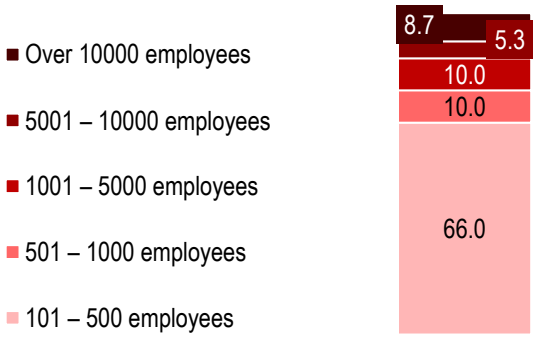
Current position



Role in procuring…



Number of employees



Thank you!