CAMPUS CYBER

WAVESTONE

Sustainability

How can cyber do its part of the job?

Analysis of cyber impacts and suggested actions

January 2024

Why does cyber matter for sustainability?

Cyber teams must play their part in sustainable development, **going beyond Green IT**, by questioning the way they implement cyber in order to **reduce its impact** without compromising on the risk level.

Cyber represents a significant proportion of information systems **(+/-5% of the IT budget*)** and is **growing** rapidly to face new threats.

Cybersecurity controls have a **major impact** on the way **information systems are designed and operated**, hence their strategic importance for overall carbon footprint.

Wavestone and the Campus Cyber developed a methodology to **measure the impact** of cyber and identify **actions** that need to be taken to reduce carbon emissions with no compromise to risk.

This study is an **exploratory methodological framework**, unique in its approach, which aims to be **adopted** by the stakeholders and **enhanced** in the years to come.

*According to Wavestone's benchmark on 100+ organizations across all sectors, 5.3% of the IT budget is spent on cybersecurity on average.

Methodology: focusing on GHG emissions

To assess the impact of cybersecurity, we focused first on **greenhouse gases emissions (in CO_2eq) which are the consequences of a security control.**

Study scope

In scope:

- → PCs, servers and appliances: manufacturing and utilization
- → Data centers support infrastructure utilization
- → External services, including a share of the Cloud
- → Business travel: train and plane

Servers and workstations location have been taken into account with a location-based approach.

Out of scope:

- → Data centers: construction
- → Network infrastructure and offices: construction and utilization
- → Cybersecurity teams commuting & business travel by car

Sources

For cybersecurity values:

- → Wavestone information system data
- → Wavestone client information system data

For emissions factors:

- → ADEME* Base Empreinte
- → Boavizta
- → Dedicated hardware manufacturers data
- → Carbon Disclosure Project’s Cloud data
- → Wavestone studies data

The list of emission factors is in the appendix.

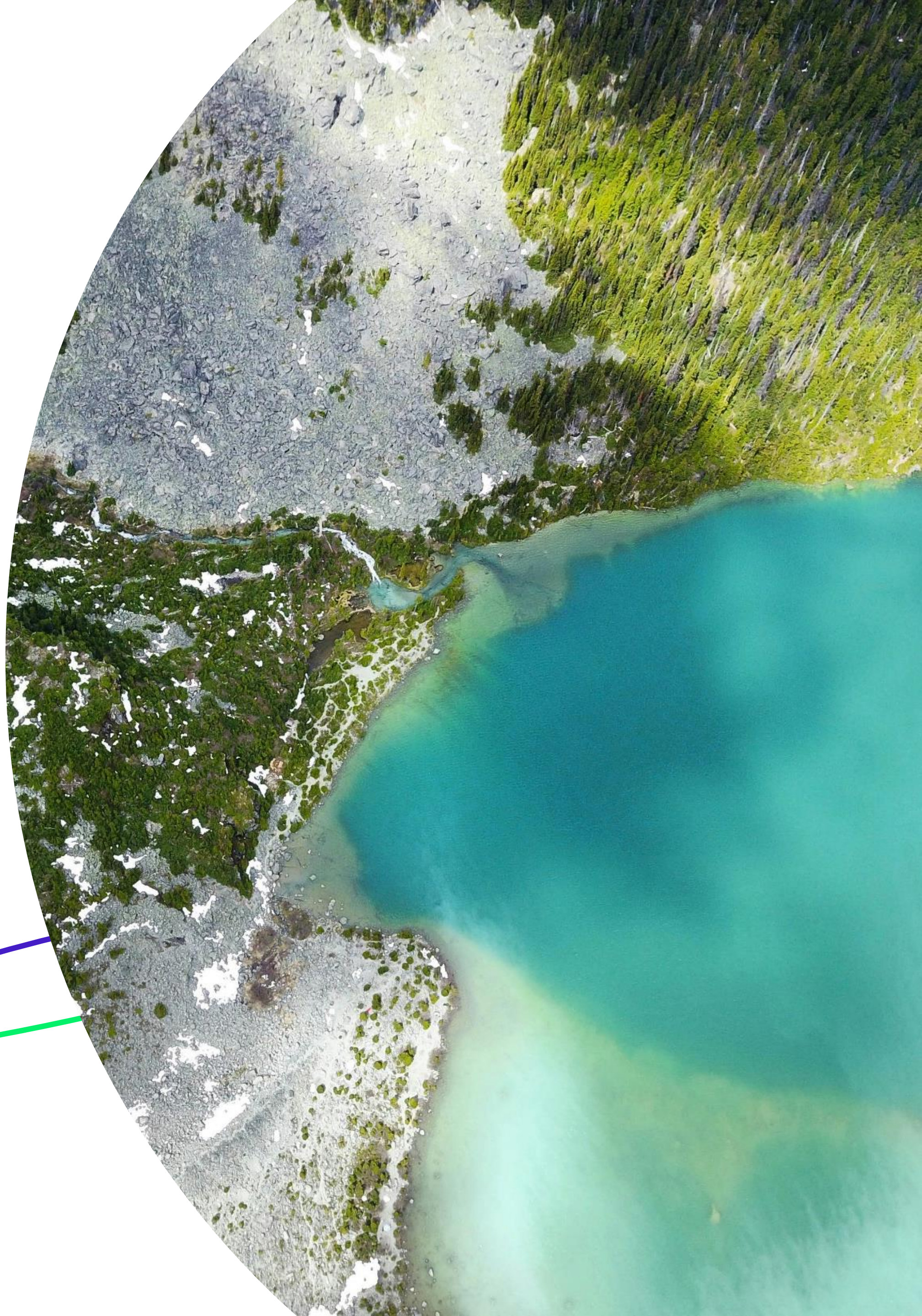
*ADEME: French Agency for Ecological Transition

Impacts on biodiversity, natural resources depletion, water/air/soil pollution, etc. are not in scope of this study because they are often correlated with emissions (as long as lifespan of IT equipment is maximized) and indicators to measure them are less mature

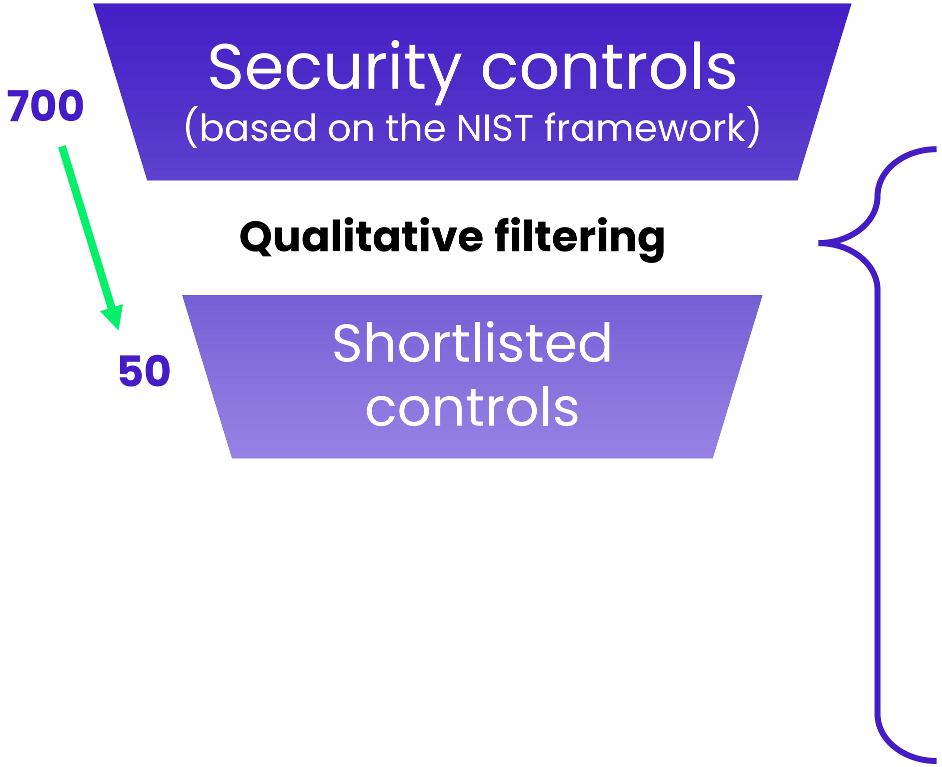
1.

What are the most emissive security controls?

Methodology & findings



Starting from 700 security controls of NIST Cybersecurity framework international standards, we identified the 50 most emitting controls

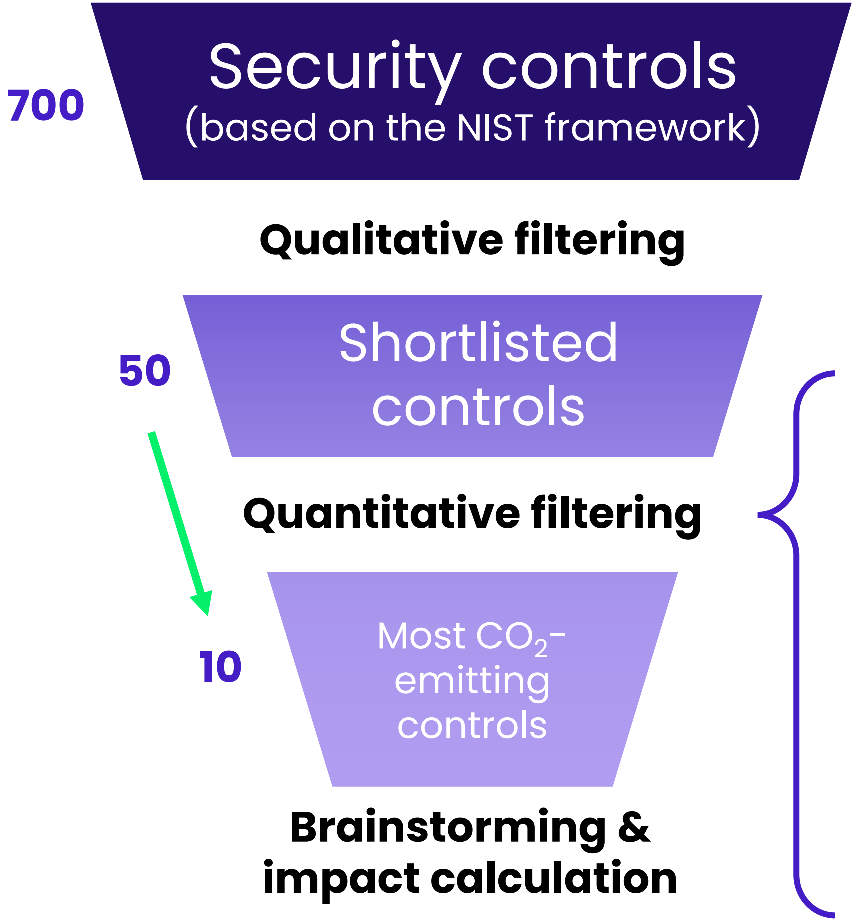


The **50 most emitting controls** were selected if the answer was positive to one or more of the following questions (based on the ADEME/Arcep* breakdown of the carbon footprint of the digital world):

1. Does it require a significant number of **endpoints**?
2. Does it require a significant number of **servers** and computing power?
3. Does it require a large amount of **network equipment** and **bandwidth**?

*The digital environmental footprint in France, ADEME/Arcep, 2022

Based on these 50 shortlisted security controls, we identified the TOP 10 most emitting controls



700

Security controls
(based on the NIST framework)

Qualitative filtering

50

Shortlisted controls

Quantitative filtering

10

Most CO_2-emitting controls

Brainstorming & impact calculation

Among the 50 shortlisted controls, the **TOP 10 most emitting controls** was selected based on the calculation of the emissions using:

- **Real-life data** from Wavestone and its clients' figures (including data centers locations)
- **Emission factors** from the ADEME*, Boavizta**, manufacturer data, etc.

*ADEME: French Agency for Ecological Transition
**Boavizta: Working group on digital footprint

→ These **results have to be calculated for each company**

→ These initial results enable us to **identify the first paths of action**

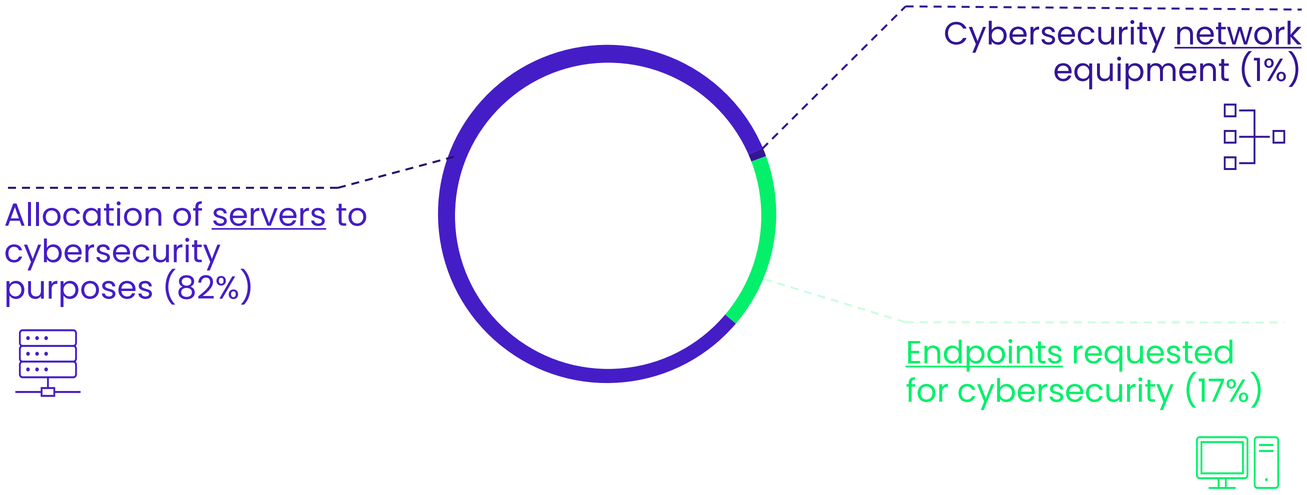
How much do the emissions of the 50 shortlisted security controls represent against IT emissions?

The **greenhouse gases emissions** of the **50 shortlisted security controls** were calculated to estimate the overall impact of cybersecurity.

An estimated

5% to 17%

of IT emissions*, (but 5% of the IT budget)



Cybersecurity greenhouse gases emissions resulting from the 50 shortlisted security controls as measured in our organizations

As this is a view by technical asset, it excludes consulting and travel.

*Redundant servers and contractor workstations are not taken into account because they are not included in the scope of cybersecurity budget.

What did we learn? Debunking cybersecurity emissions' myths

2 security topics generate 50% of cybersecurity-related emissions…

■ Data (5%)
Data in motion and data at rest protection
Cryptography

■ Network (5%)
Network mapping and segmentation
Anti DDoS

■ Governance (3%)
Cyber staff workstations
Cybersecurity awareness
Travel

■ Other topics (8%)
Incident management, risk, etc.

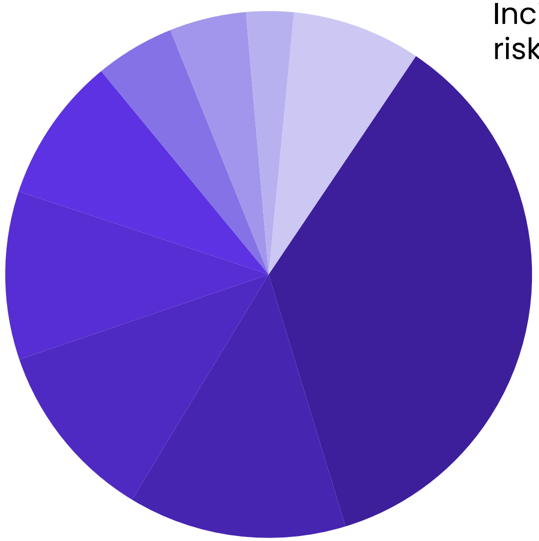
■ Vulnerability (9%)
Vulnerability scans
Pentests
Antiviruses
Patch management

■ IAM (10%)
Authentication
Vaults
PAM

■ Detect (11%)
Log generation
Log collection and storage
Log analysis

■ Endpoints (13%)
Contractor workstations
Administrator workstations and VDIs

■ Resilience (36%)
Redundancy capabilities in different regions
Backup servers
Backup PCs



Emissions % by NIST topic

…but not the one we thought

It emits **more** than we may think ⬆

Resilience capabilities
36% of cybersecurity emissions

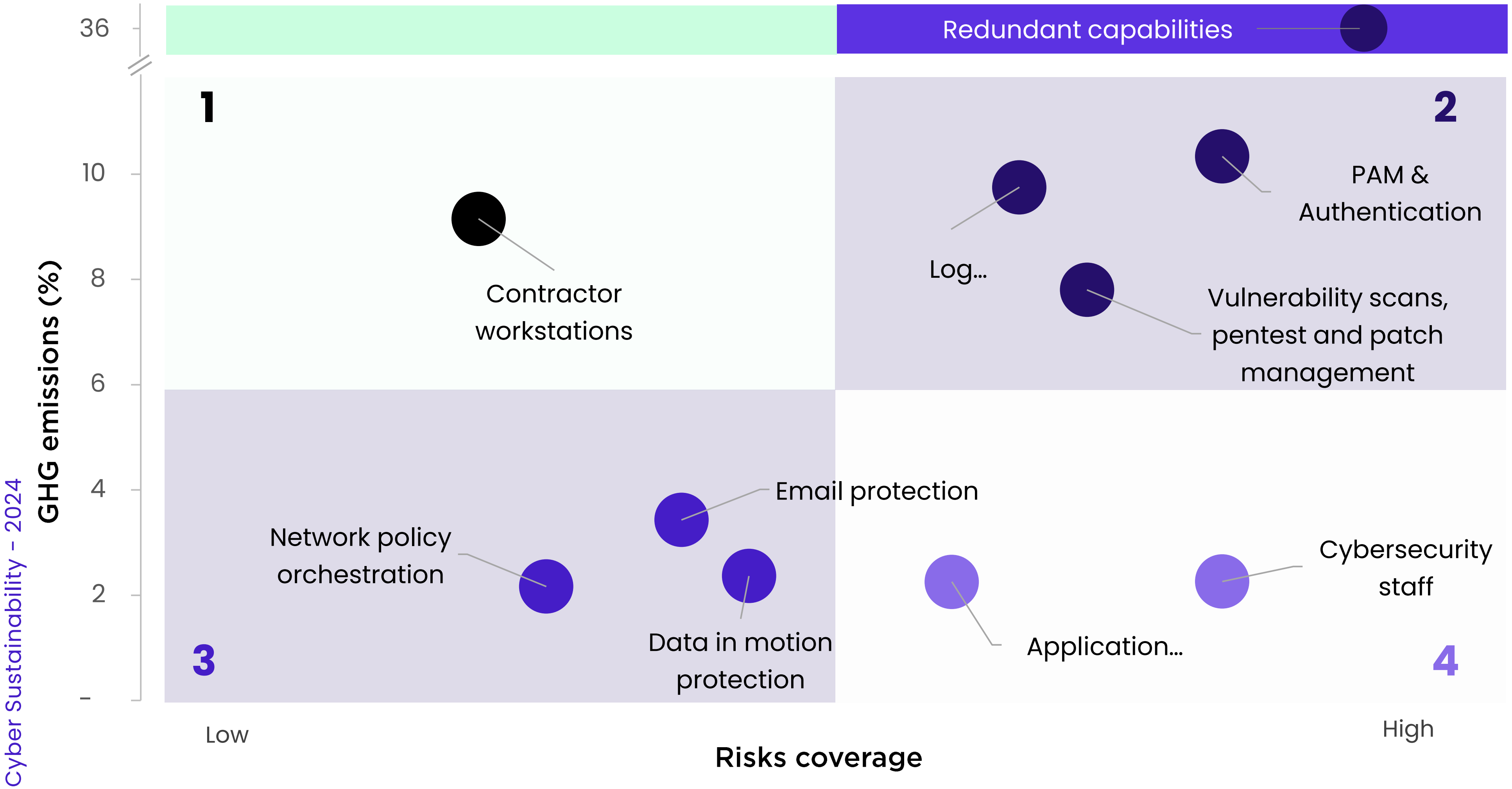
Contractor workstations
9% of cybersecurity emissions

It emits **less** than we may think ⬇

Cyber threat intelligence
<2% of cybersecurity emissions

Encryption
<1% of cybersecurity emissions

We mapped the 10 most emitting controls according to their risk coverage in our context to assess their level of priority



1

Medium risk coverage, high CO2 impact

2

High risk coverage, high CO2 impact

3

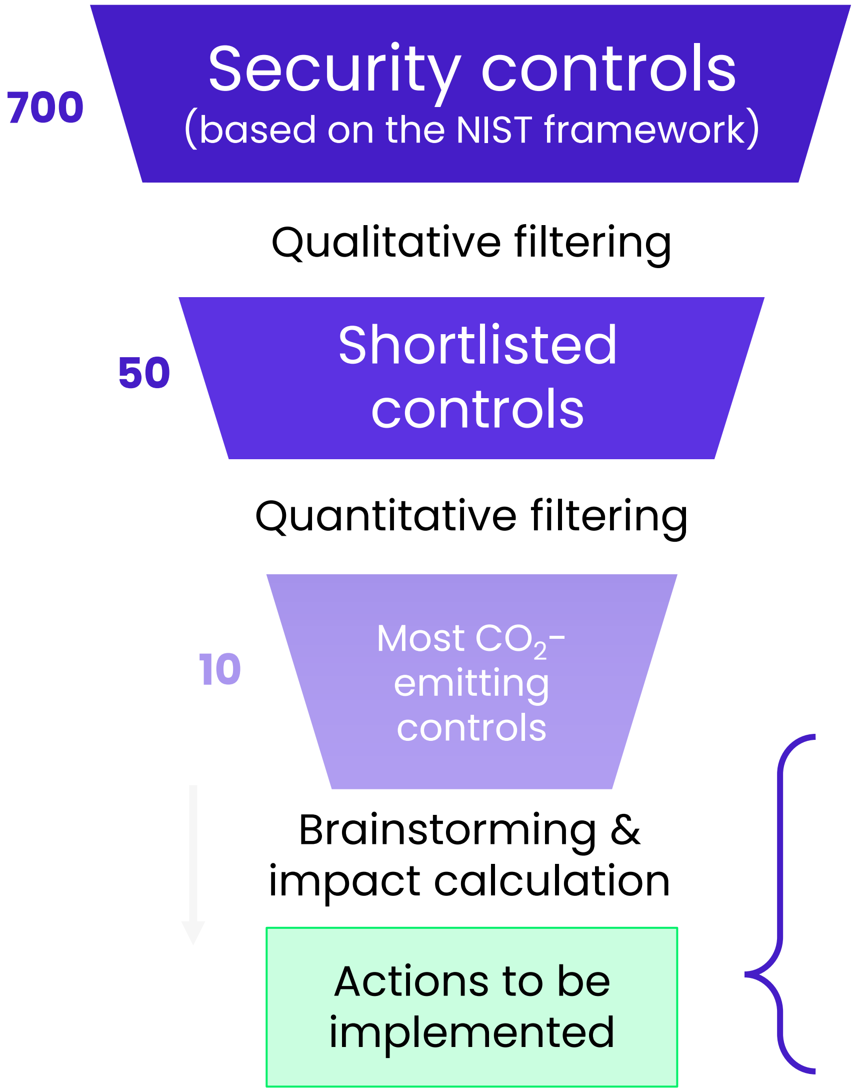
Medium risk coverage, low CO2 impact

4

High risk coverage, low CO2 impact

Risk has been assessed by a vision from Wavestone experts, and depends on each organization's context

We identified the TOP 4 actions to optimize the most emitting security controls



700

Security controls
(based on the NIST framework)

Qualitative filtering

50

Shortlisted controls

Quantitative filtering

10

Most CO_2-emitting controls

Brainstorming & impact calculation

Actions to be implemented

To find actions to be implemented:

- **Brainstorming workshops** have been organized with Wavestone experts to list ideas
- Actions have been identified to **reduce emissions** while keeping the **same risk level**

Optimizing security controls to decrease emissions by 5% to 10%, with a constant level of risk

1. Optimizing **redundancy** capabilities and **backups**
   Example: Initiate a redundancy capacity optimization project and reduce backups retention duration

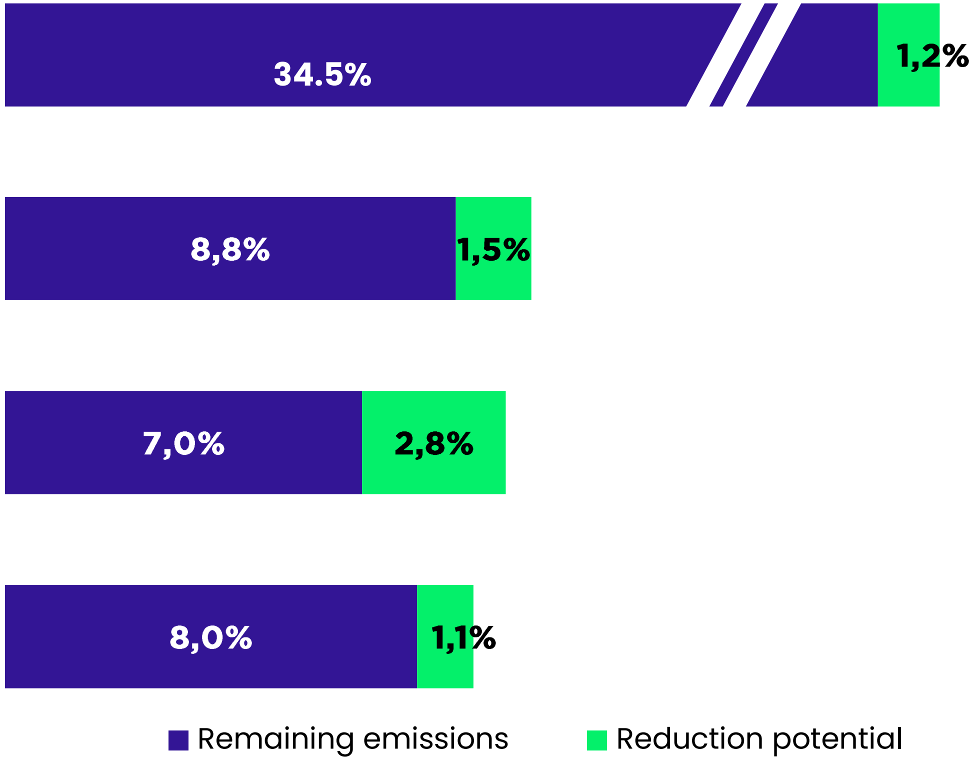
2. Consolidating **IAM solutions**
   Example: optimize privilege access and password vaults applications by consolidating use-cases on fewer solutions

3. Reducing the volume of **logs**
   Example: reduce verbosity, storage time and quantity

4. Providing specific **contractors with VDIs** instead of dedicated workstations
   Example: Only provide a workstation to contractors working on critical projects or independent contractors

All actions and assumptions are detailed in the appendix.

Example of results[1]



As a % of total initial cyber emissions

Complexity[1]

	Complexity
1	●●●○
2	●●●●
3	●●○○
4	●○○○

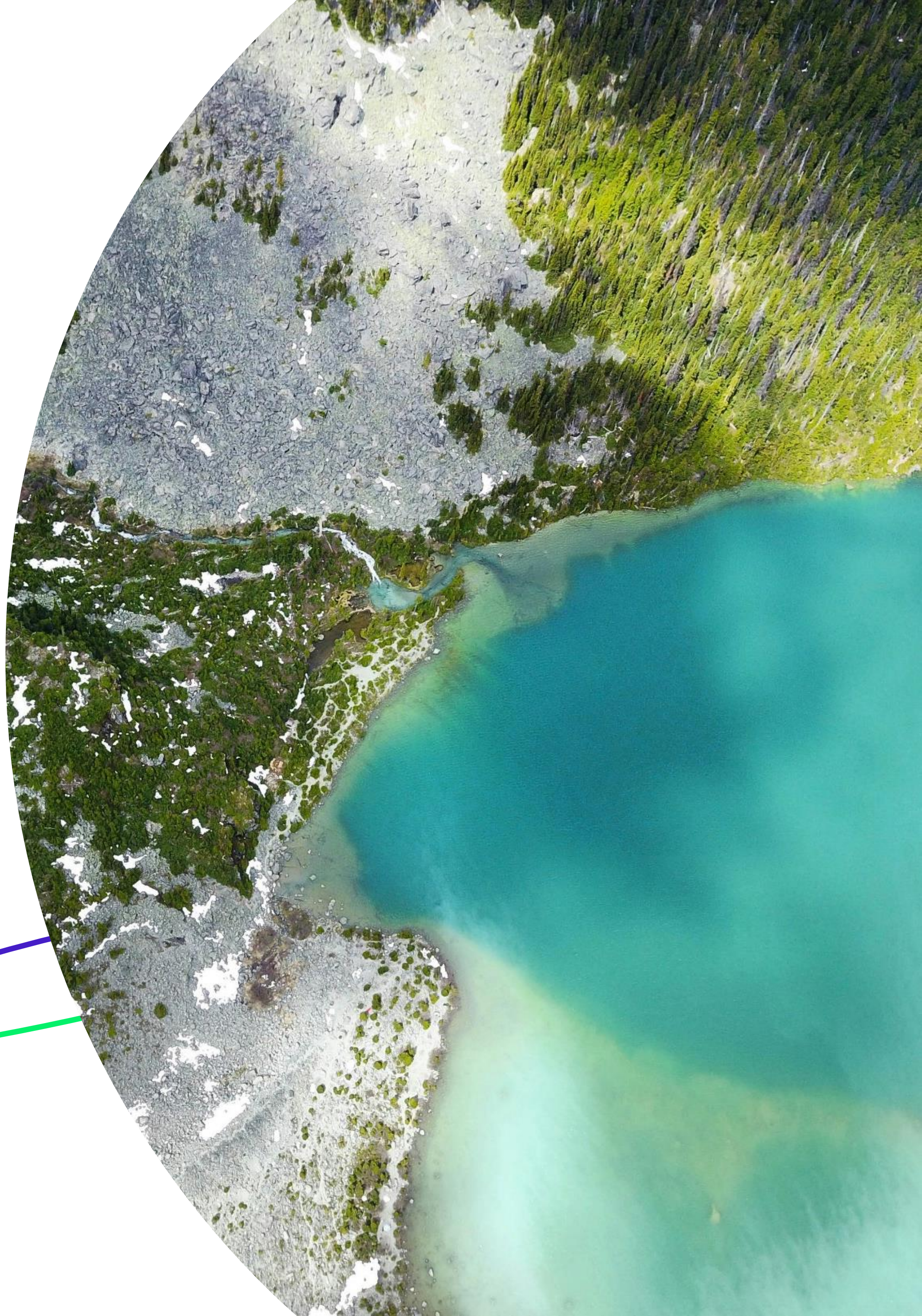
Co-benefits have also been identified such as a **reduction of run costs** or an infrastructure that is **easier to manage**.

[1] depends on each organization and context. This is an initial estimation that should be investigated further.

2.

What actions can we take?

A three-step approach



Ideas for reducing cyber emissions

And how to act on them

ACT NOW
IT & Cyber actions

MAINTAIN THE APPROACH
Sustainable security by design

INFLUENCE AT SCALE
Cyber ecosystem actions

ACT NOW

Assess your existing controls emissions

Evaluate the CO_2 impact of existing cyber requirements using this methodology

Estimate the emissions of the security controls that are already implemented to take effective actions to reduce them

How to do it?

Run a quick assessment with the in-house Excel questionnaire (duration: 1 hour)

Run an in-depth assessment with interviews to have precise estimates (duration: 15 to 50 days)

Implement green IT measures that have no risk impact

Optimize the **number of devices**

Ensure **software** is adapted requirements and use **applications** to their **full capability**

Ensure **data generation** is adapted to requirements

Raise awareness among staff on sustainability topics

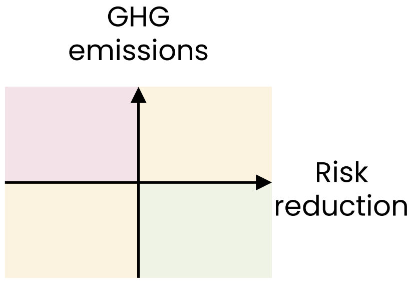
Adopt a **responsible purchasing policy**

MAINTAIN THE APPROACH

Make sure sustainability is incorporated in run activities

Implement sustainability criteria in day-to-day risk analysis

Update the risk analysis method to take greenhouse gases emissions into account



How to do it?

If a mitigation control matches one of these 2 questions, then it's significant and you need to estimate the impact more precisely using ADEME's emission factor:

1. Is it in one of the **TOP 10 most emitting security controls**?
2. Does it require a significant number of **endpoints, or servers and computing power, or** n**etwork equipment and bandwidth**?

Continuously monitor cybersecurity greenhouse gases emissions

Complete the run security dashboard with greenhouse gases emissions indicator

How to do it?

Steer and monitor greenhouse gases emissions to continuously reduce the environmental impact, either by doing:

1. **Continuous assessment with Green IT support**: set up indicators on greenhouse gases emissions on the cybersecurity dashboard
2. **Spot assessment every 2 years**

Invite the cyber ecosystem to contribute to the transition

Further actions to reduce the impact of cybersecurity require the involvement of other stakeholders of the cyber ecosystem. Inviting them to contribute to the transition can unlock significant emission reduction opportunities.

Normalization organizations

NIST, ISO, etc.

Incorporating sustainability in the cyber norms and standards

Regulators

ECB, National Cyber Agencies, etc.

Assessing the impact of each cybersecurity requirement to **promote the least carbon-intensive regulation options**

Software & equipment providers

Ensuring the efficiency of **solutions and equipment provided**, ensuring a sustainable-by-design approach, for example by avoiding planned obsolescence providing offers adapted to smaller needs

Academic research

Incentivising academic research to measure the **efficiency of existing protocols (encryption, authentication, etc.)** and developing **new sustainable cyber solutions**

A long journey for cybersecurity to play its part

ACT NOW
IT & Cyber actions

MAINTAIN THE APPROACH
Sustainable security by design

INFLUENCE AT SCALE
Cyber ecosystem actions

Join the Campus Cyber working group

to share your in-house results and contribute to enhancing the methodology

cybersustainability@cyber4tomorrow.fr

CAMPUS CYBER

	Gérôme BILLOIS Partner	(+33) 6 10 99 00 60 gerome.billois@wavestone.com
	Nicolas GAUCHARD Senior Manager	(+33) 6 67 39 65 70 nicolas.gauchard@wavestone.com
	Hugo BÉRARD Consultant	(+44) 7471 142 802 hugo.berard@wavestone.com

With contributions from: **Constance LINQUIER, Mario GRIPPAY-GONZALEZ**

APPENDIX
Action Sheets

Actions to reduce emissions: Redundancy & backups

Original security control:

Redundancy capabilities between data centers in different regions and backups are set up.

Example of actions to reduce emissions:

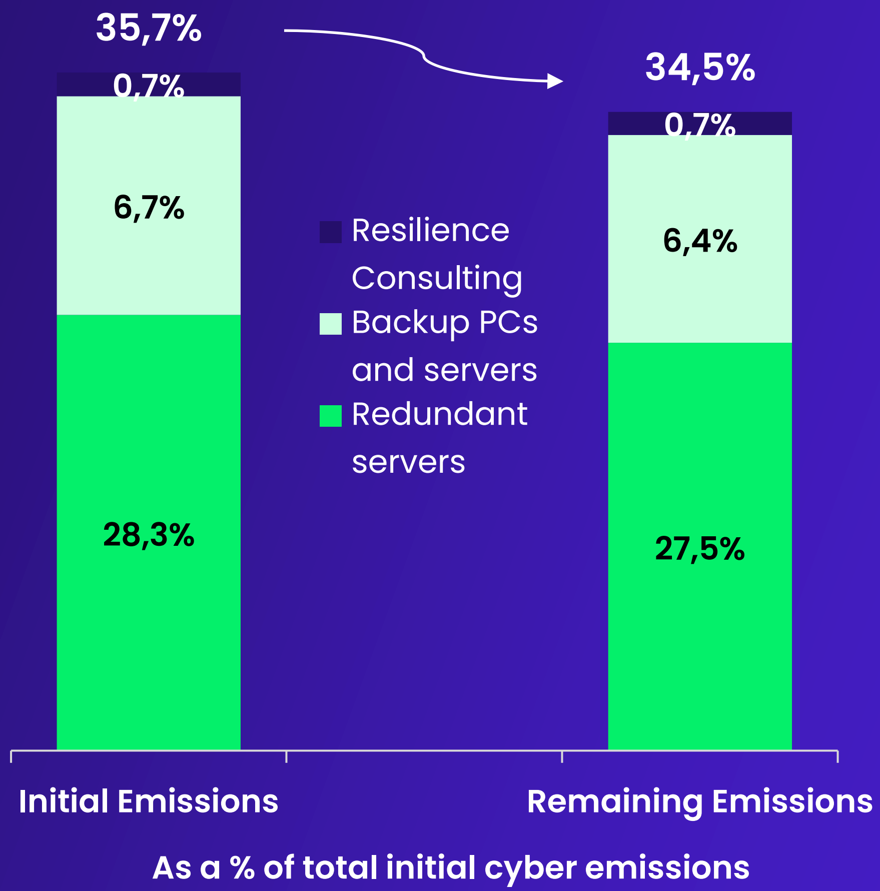
- Initiate a **redundancy capacity optimization project**: do not duplicate everything, review applications confidentiality, ensure that applications decommissioning is done properly
- **Optimize backups**: reduce retention duration, minimize the number of backups, optimize storage methods
- **Reduce the number of backup workstations**

Every organization should pick the most relevant actions depending on its context

Example

Reduction potential with the following actions:

- Reduce redundant data by 3%
- Decrease backups PCs and backup servers by 5%



Complexity ●●●○

Actions to reduce emissions: Identity and access management

Original security control:

The organization has an identity lifecycle management solution and an authentication tool to control the identities of the users of the information system.

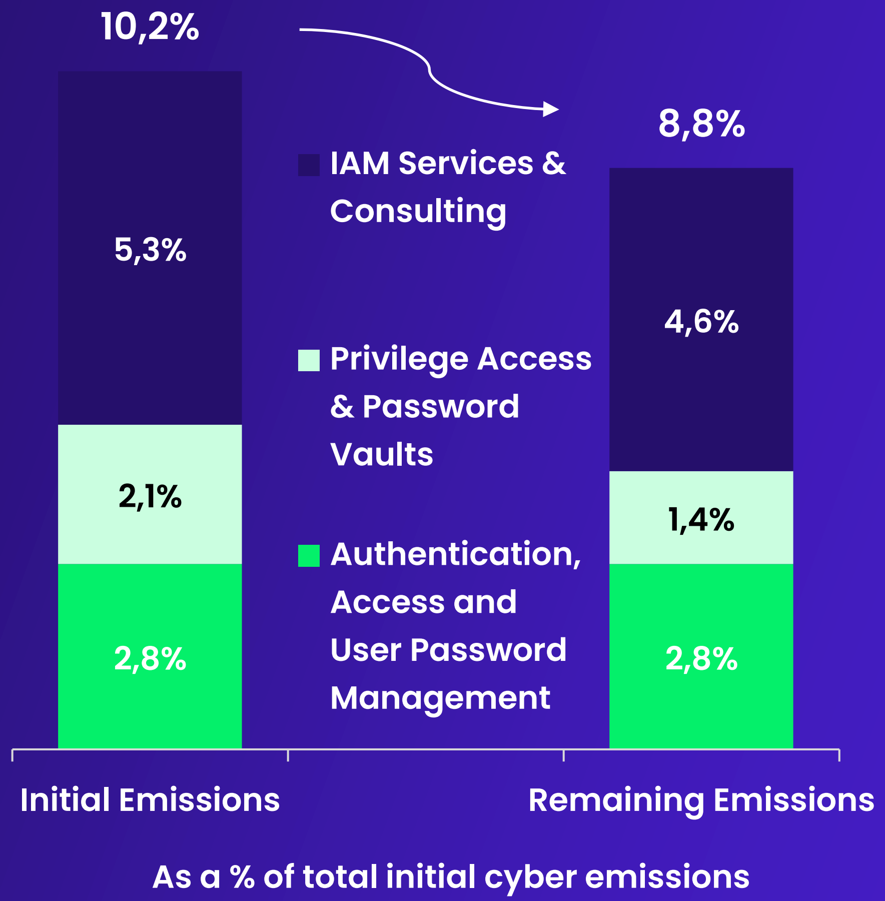
Example of actions to reduce emissions:

- **Rationalize technologies** and authentication methods
- Implement **authentication methods that do not require dedicated physical equipment**
- **Optimize privilege access and password vaults applications**: consolidate use-cases on fewer solutions to optimize infrastructure and avoid duplication in multiple geographical areas

Every organization should pick the most relevant actions depending on its context

Example

Reduction potential with the following action: Optimize Privilege Access & Password Vaults and related Services and Consulting by 33%



Complexity ●●●●

Cyber Sustainability - 2024

Actions to reduce emissions: Log management

Original security control:
Logs are collected, centralized in a SIEM and analyzed to detect security events.

Example of actions to reduce emissions:

- **Optimize the volume of logs collected and stored**: reduce verbosity, storage time and quantity
- **Use an MSSP** (Managed Security Service Provider) to used shared resources with other companies

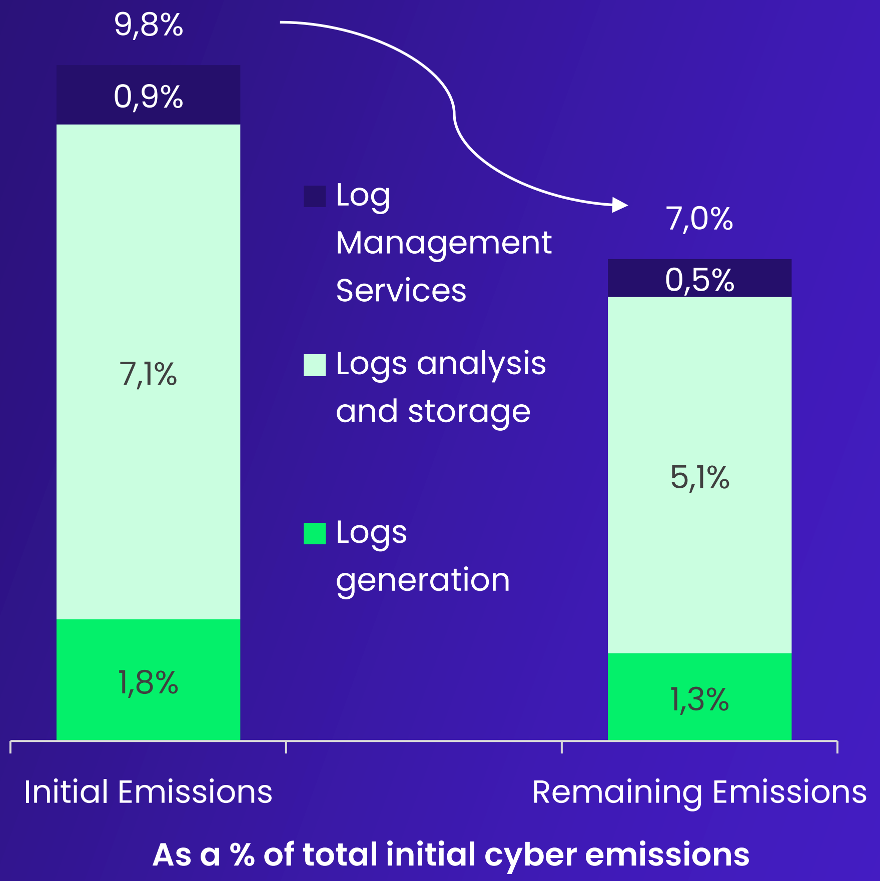
Wavestone Testimony

By reducing the verbosity of the logs and avoiding unnecessary logs duplication in different locations, we have been able to reduce the volume of logs collected and stored by 56%.

Every organization should pick the most relevant actions depending on its context

Example
Reduction potential with the following actions:

- Reduce the volume of logs collected and stored by 20%
- Use an MSSP to optimize by 10%



Complexity ●●○○

Actions to reduce emissions: Contractor workstations

Original security control:

Every contractor must be provided with a dedicated workstation.

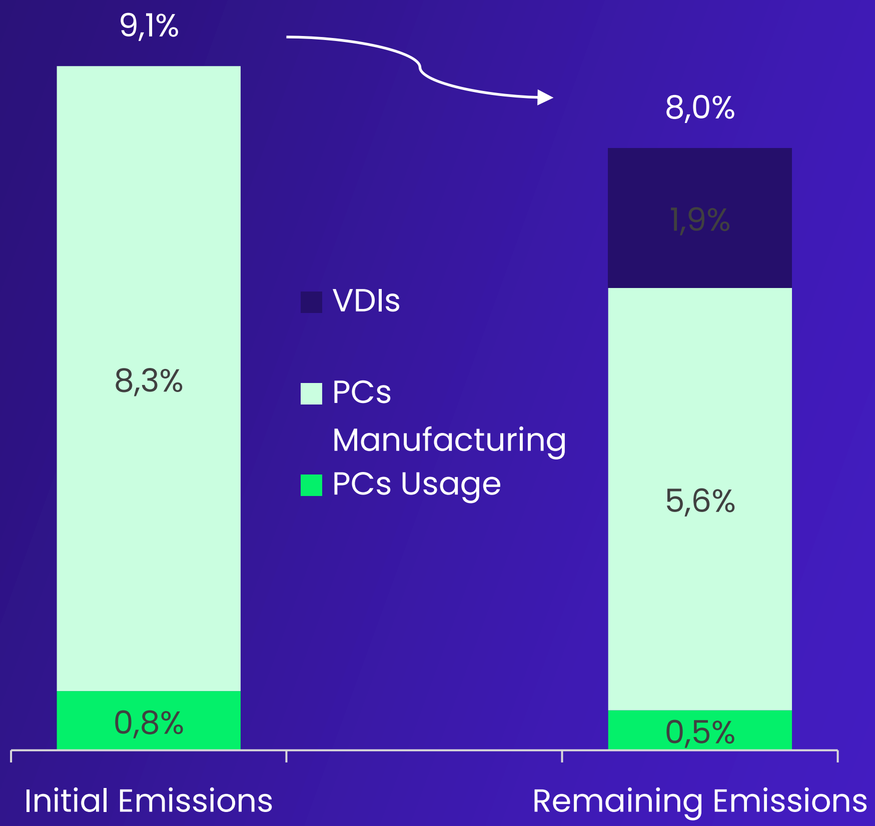
Example of actions to reduce emissions:

- **Provide as many contractors as possible with a VDI**, rather than a dedicated workstation
- Only provide **contractors working on critical projects** or **independent contractors** with a workstation

Every organization should pick the most relevant actions depending on its context

Example

Reduction potential with the following action: Provide a VDI to 40% of the contractors, rather than a dedicated workstation



As a % of total initial cyber emissions

Complexity ●○○○

APPENDIX
Glossary & Methodology

Glossary

Term	Definition
Emission Factor	An emission factor is a coefficient which allows to convert activity data into greenhouse gases emissions.
CO2eq	CO2eq is a metric measure used to estimate the emissions from various greenhouse gases converted in carbon dioxide equivalents based on their global warming potential.
ADEME (Base Empreinte)	ADEME is the French Environment and Energy Management Agency which consolidates emission factors in a database known as the Base Empreinte.

Methodology: Overarching Assumptions

Category	Assumption
Devices	For each cyber staff, the assumption is that they have one mobile device.
Cyber solutions	As an assumption, 6 virtual CPUs on average rely on 1 physical CPU.
Appliances	Due to a lack of information available for proxies, reverse-proxies, web application firewalls, IPS and IDS, it was assumed that the manufacturing emissions and electricity consumption was the same as for a firewall.
Devices	Workstations, even when they are not used for cybersecurity purposes, still need to generate logs and run antiviruses. Therefore, for all workstations that are not purely used for cybersecurity purposes, an assumption was taken that: • 0.25% of these workstations are dedicated to log generation. • 0.75% of these workstations are dedicated to antiviruses. These are Wavestone internal estimates.
Other servers	Servers, even when they are not used for cybersecurity purposes, still need to generate logs and run antiviruses. Therefore, for all servers that are not purely used for cybersecurity purposes, an assumption was taken that: • 0.75% of these servers are dedicated to log generation. • 2.25% of these servers are dedicated to antiviruses. These are Wavestone internal estimates.

Methodology: Emission Factor Values

Category	Name	Source	Emission Factor	Unit
Electricity mix	All Carbon Intensity of the Electricity Mix per Geographical area (kgCO2eq/kWh) are taken from the ADEME Base Empreinte	ADEME Base Empreinte	N/A	N/A
Devices	Laptop Manufacturing Emissions - All Sizes	Boavizta 2022, Statistical Study	232	kgCO2eq
Devices	Laptop Energy Consumption - All Sizes	Boavizta 2022, Statistical Study	20	kWh/year
Devices	VDI manufacturing emissions linked to the underlying server and network	Wavestone calculation based on ADEME data	128	kgCO2eq
Devices	VDI annual electricity consumption linked to the underlying server and network	Wavestone calculation based on ADEME data	26.9	kWh/year
Devices	Lifespan of a VDI underlying server	ADEME Base Empreinte	5	years
Devices	Workstations hard drive manufacturing emission	Extrapolated from a Cornell University Study	4.74	kgCO2eq
Devices	Annual electricity consumption of a monitor	Manufacturer data	44.5	kWh/year
Devices	Manufacturing emissions of a monitor	Manufacturer data	430.7	kgCO2eq
Devices	Average lifetime of a hard drive	ADEME Base Empreinte	5	years
Devices	Smartphone manufacturing emissions	Manufacturer data	50.16	kgCO2eq
Devices	Smartphones electricity consumption	ARCEP Study 2022	2	kWh/year
Servers	Rack manufacturing emissions	ADEME Base Empreinte	550	kgCO2eq
Servers	Average manufacturing emissions for cyber servers	Internal study based on constructor data of known cybersecurity servers	1269	kgCO2eq
Servers	Average electricity consumption of cyber servers	Internal study based on constructor data of known cybersecurity servers	1556	kWh/year
Servers	Average manufacturing emissions of backup servers	Internal study based on constructor data of known cybersecurity servers	2073	kgCO2eq
Servers	Average electricity consumption of backup servers	Internal study based on constructor data of known cybersecurity servers	2013	kWh/year
Cloud	Average emissions of Cloud services	2021 CDP Report	75	kgCO2eq/k€
Consulting	Average emissions of digital consulting for Fixed Fee	Internal study	35.49	kgCO2eq/k€
Consulting	Average emissions of digital consulting for Time and Material	Internal study	4904.37	kgCO2eq/FTE
Appliances	Emissions linked to manufacturing of a firewall	Extrapolated from ADEME Base Empreinte	59	kgCO2eq
Appliances	Yearly electricity consumption of a firewall	Extrapolated from ADEME Base Empreinte	90	kWh/year
Travel	Average emissions from air travel	ADEME Base Empreinte	0.187	kgCO2eq/km
Travel	Average emissions from rail travel	ADEME Base Empreinte	0.0033	kgCO2eq/km

Methodology: Emission Factor Details

Category	Name	Assumption Explanation
Servers	Manufacturing emissions for a rack	To calculate the yearly manufacturing emissions for a rack, the assumption taken for the lifespan of a rack is that it is the same as a server.
Servers	Average manufacturing emissions and electricity consumption of servers	The emission factor used for redundant servers is the average of the emission factor taken from the constructor data of known and existing cybersecurity servers.
Servers	Estimated number of racks by number of servers	To estimate the number of racks, an internal assumption was used that a rack can host 18 servers on average.
Consulting	Average emissions of digital consulting for Fixed Fee and for Time & Material	To calculate the average emissions of digital consulting, two different factors were used depending on the type of project. For Fixed Price engagements, the emission factor per k€ was used. For Time & Material engagements, the emission factor per FTE was used. Furthermore, the weighted average of emission factors of strategy vs IT & management external services was incorporated in the calculation, based on the emissions of strategy vs IT & management external services.
Appliances	Emissions linked to manufacturing of a firewall	The share of total manufacturing emissions compared to the share of total usage emissions from servers was extrapolated and applied to firewalls. The calculation employed ADEME's emission factor which states that firewalls emit on average 80.7 kgCO2e through their lifetime.
Travel	Average emissions from air and rail travel (2018)	To calculate the average emissions linked to travel, the assumption was taken that a cyber FTE travels as much as an IT FTE.