

[www.sedesk.eu](http://www.sedesk.eu)

[cyberstartupobservatory.com](http://cyberstartupobservatory.com)

# The 1st Global Cybersecurity Observatory

## Europe

First Edition

April 2020



# Insight

## Blu5

Does more budget improve  
cyber-resilience? The Ugly Truth!

The logo consists of a large, bold, blue letter 'B' with a smaller, black number '5' positioned to its upper right.

[www.sedesk.eu](http://www.sedesk.eu)

# Does more budget improve cyber-resilience? The Ugly Truth!

## At a glance

- 6 minute read 🕒
- The current situation
- Eliminate complexity
- Increase visibility and control
- Implement automation
- Blu5 disruptive approach



Analysts are predicting years of growth in security spending, worldwide. Back in 2018, worldwide spending on information security products and services exceeded \$114 billion, an increase of 12.4% from 2017 [1]. Gartner forecast a five-year annual growth rate of 8.5% to reach \$170.4 billion in 2022 [2]. Despite this trend, however, the bad guys are growing stronger. More than 20 data breaches were reported per day in the first half of 2019 [3].

## The current situation

Was your CFO right when he asked you to revise your cyber budget? Possibly!

Historically, the lack of an adequate budget has been a key challenge in addressing cyber security issues in organizations, both private and governmental.

With the continuous rise in data breach numbers and digital transformation efforts, exposing enterprises to new cybersecurity risks across business industries, never before have companies and government institutions been investing so much money in cyber security, both in terms of technology and human resources.

There may be different reasons behind this trend: the fear of being successfully compromised, the regulatory pressure, the need to ensure business continuity or all of these together.



**“Gartner forecast a five-year annual growth rate of 8.5% to reach \$170.4 billion in 2022. Despite this trend, however, the bad guys are growing stronger. More than 20 data breaches were reported per day in the first half of 2019.”**



The current pandemic will exacerbate the situation, re-routing funds, but at the same time demanding higher attention to cyber threats. In these extremely challenging times companies are under stress, putting the IT department right at the center of a perfect storm.


So, why are increased investments in cyber security not enough to hinder the surge of cyberattacks? Money is not the only resource a business has available to enhance its cyber security posture. Effective investments have to be based on the understanding of the organization's security priorities.

Therefore, in order to determine the appropriate cyber security spending, CISOs and business leaders should start by making an assessment of the organization's current and future needs as well as capabilities:


- What is the organization's risk strategy?
- Where will the organization's investment be most effective?
- How can organizations make investments work?
- What can organizations learn from the Covid-19 emergency?

The key is to determine and provide the right amount of protection, at a reasonable cost, without significantly compromising business operations or culture.

To do that, organizations must view this effort through a number of lenses. Three of the most important are: the potential negative impact of risk, technology and cost.



"Money is not the only resource a business has available to enhance its cyber security posture. Effective investments have to be based on the understanding of the organization's security priorities."



**“The key is to determine and provide the right amount of protection, at a reasonable cost, without significantly compromising business operation.”**

Considering that a totally secure environment is impossible to create, an organization must determine the level of security it needs, commensurate to the maximum risk (reputational, operational, or financial) that it is willing to take. Further spending will only be justified by the estimated value of any additional security based on the business strategy and level of accepted residual risk.

For example, equipping every organization’s location, even those which are not critical to the operations, with next-generation expensive firewalls resulting in high configuration and management overhead, may not be the right solution. A more sensible solution would be to accept the possibility of a breach of non-critical systems rather than investing millions to protect low-value assets.

IT security teams have a lot of ground to cover and many think in terms of a layered approach to cybersecurity. It actually goes well beyond deploying layers of different security tools and technologies. For cybersecurity to be

effective, organizations must also consider how they leverage people and processes. Nowadays, organizations tend to have far too many cyber security tools in place overlooking duplicated features and integration.

All this makes it difficult to test, measure and manage security, heightening the risk of undermining protection. Piling more technology layers than necessary means more energy dispersion of the already rare skills needed to manage cyber security. Therefore, it really helps to have the right tools for the job.

Organizations see investments in time and resources increase without experiencing an equal or greater benefit in terms of security. Besides, organizations rarely use all the security tools and features they have purchased, due to the overwhelming and growing complexity.

Finally, another cost element when making purchasing decision, is the impact on the daily business operations in terms of deployment and running of all the systems and technologies.

One aspect is the implementation of way too strict security measures compromising the ability to operate the daily business seamlessly.

We came to the conclusion that spending more for cybersecurity at this point in time may even result in having a less resilient cyber posture.

In our daily work of providing ICT and cyber security solutions to businesses in a wide range of industries, including defense, banking and finance, energy and telecommunications, we have identified a number of actions that executives can take to slim down security budgets while improving security. They include the following:

## Eliminate complexity


Fall in love with simplicity! Try to resist the temptation to implement the many cyber security products available on the market.

Despite the fact that a layered security is currently considered a best practice for enterprises - a single layer defense no longer being enough - sometimes these layers, if not integrated and managed correctly, can have unintended consequences and even make an organization less secure than before.

With each new security layer come integration challenges, where one product might interfere with the functioning of another or create security policy conflicts. Get rid of unused software and tools and revise your security best practice, which may not be adequate for the coming future challenges.

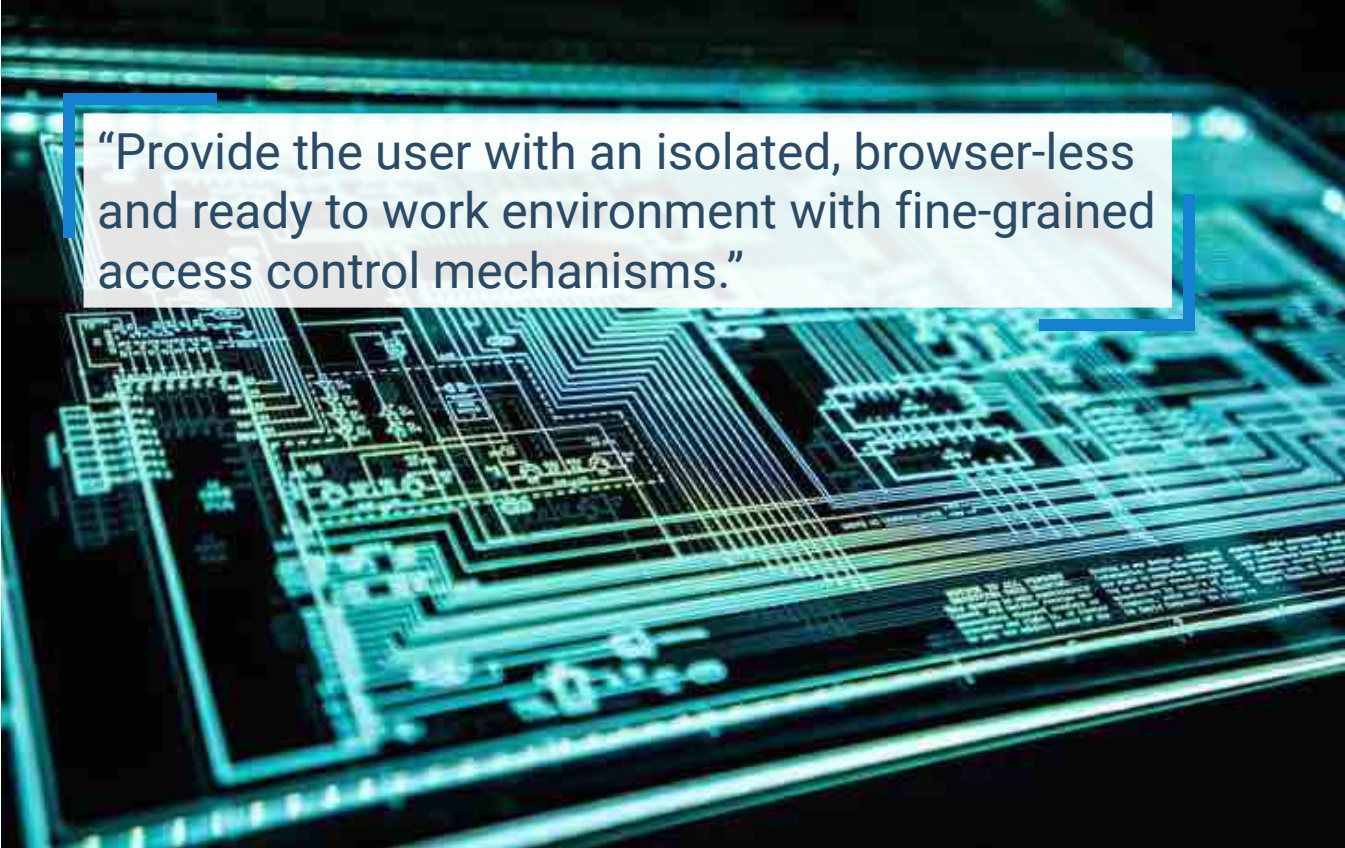
Henry Ford once said: "If it isn't there, it doesn't break".

Too often we see companies buying a technology to meet a compliance need, or fill a security gap, or tick off an item on a list, overlooking the budgeting, system implementation and management.

A photograph of a laptop keyboard and screen. The screen displays a colorful, abstract image. A white text box with a blue border is overlaid on the image, containing the quote: "Try to resist the temptation to implement the many cyber security products available."

**"Try to resist the temptation to implement the many cyber security products available."**





**“Provide the user with an isolated, browser-less and ready to work environment with fine-grained access control mechanisms.”**

Administrators need to understand how the initial configuration and the subsequent changes might affect business processes, as well as other security systems.

## **Increase visibility and control over your IT eco-system**

The company staff and ecosystem is often one of the weakest links in the cybersecurity chain. To prevent cyberattacks on the endpoints, too often operations teams introduce over-restrictive security layers, hindering the daily activity and productivity of its workforce on one side and resulting in fighting back irresponsible human behaviors trying to circumvent these measures on the other.

Besides, security officers lack visibility into their eco-system security processes. Not only do suppliers create a new entry point into the company’s network for cyber

criminals to exploit, it also means every supplier’s employee is now a potential target to breach the company’s network.

The key is implementing a secure network access strategy where there is no implicit trust but rather a level of trust calculated on an initial assessment of the identity, the system and the context, regardless of whether entities are inside or outside of the company perimeter.

So, despite recognizing the importance of security awareness programs to secure the human element, we mostly believe in a much more straightforward and thorough approach, which consists of tackling the problem from the root.

By providing the user with an isolated, browser-less and ready to work environment with fine-grained access control mechanisms, not only does it reduce user liability but will increase productivity and network security.

## Implement automation

The rapid expansion of network infrastructures and hence the exponential growth of data traffic is outpacing IT capabilities. As a result of network complexity, companies spend a large amount of time and money configuring and managing their networks. Scheduled maintenance accounts for 80% of network outages [4]; enterprise networks spend around 70% of its IT budgets only to maintain the status quo [5].

Automation is the cornerstone strategy to focus on increased network agility and reliability while controlling operational expenditures (OpEx) and capital expenditures (CapEx).

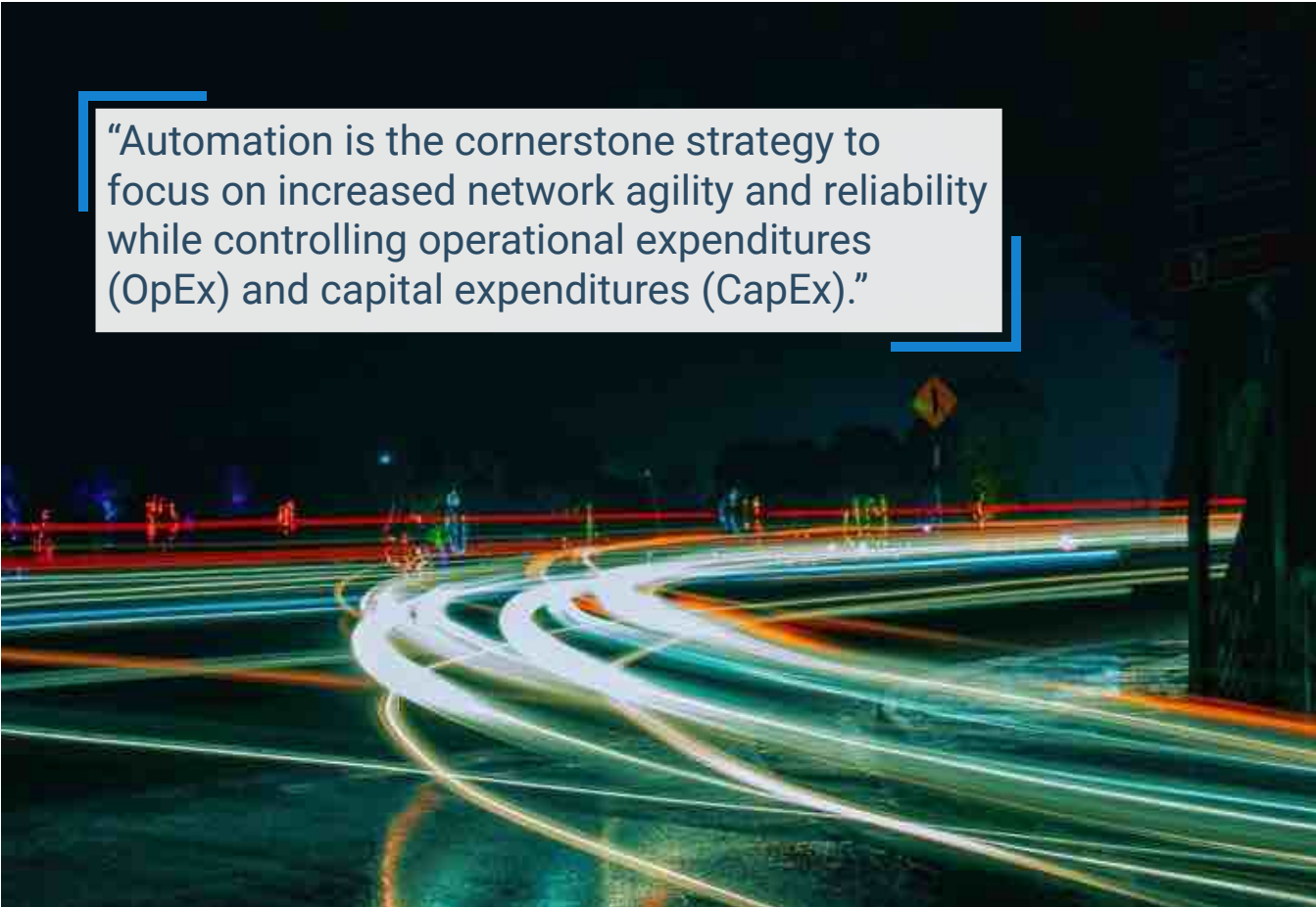
To improve operational efficiency both of IT teams and end-users, organizations can automate routine and complex tasks

that may be time-consuming, repetitive, or error prone.

By automating the complex processes of configuration, deployment, and operation of network services, IT teams can slash operations costs and introduce services more quickly and be prepared to manage network changes to exceed users' expectations.

So, yes, you will have to devote some of your budget to cybersecurity, but by asking the right questions you will make wiser investments rather than feeling pressured to simply throw money in the general direction of the problem.

Since you cannot change the incentives and resources that make cyberattacks appealing and effective, you can nonetheless limit the success rate of cybercriminals' attacks.



**“Automation is the cornerstone strategy to focus on increased network agility and reliability while controlling operational expenditures (OpEx) and capital expenditures (CapEx).”**



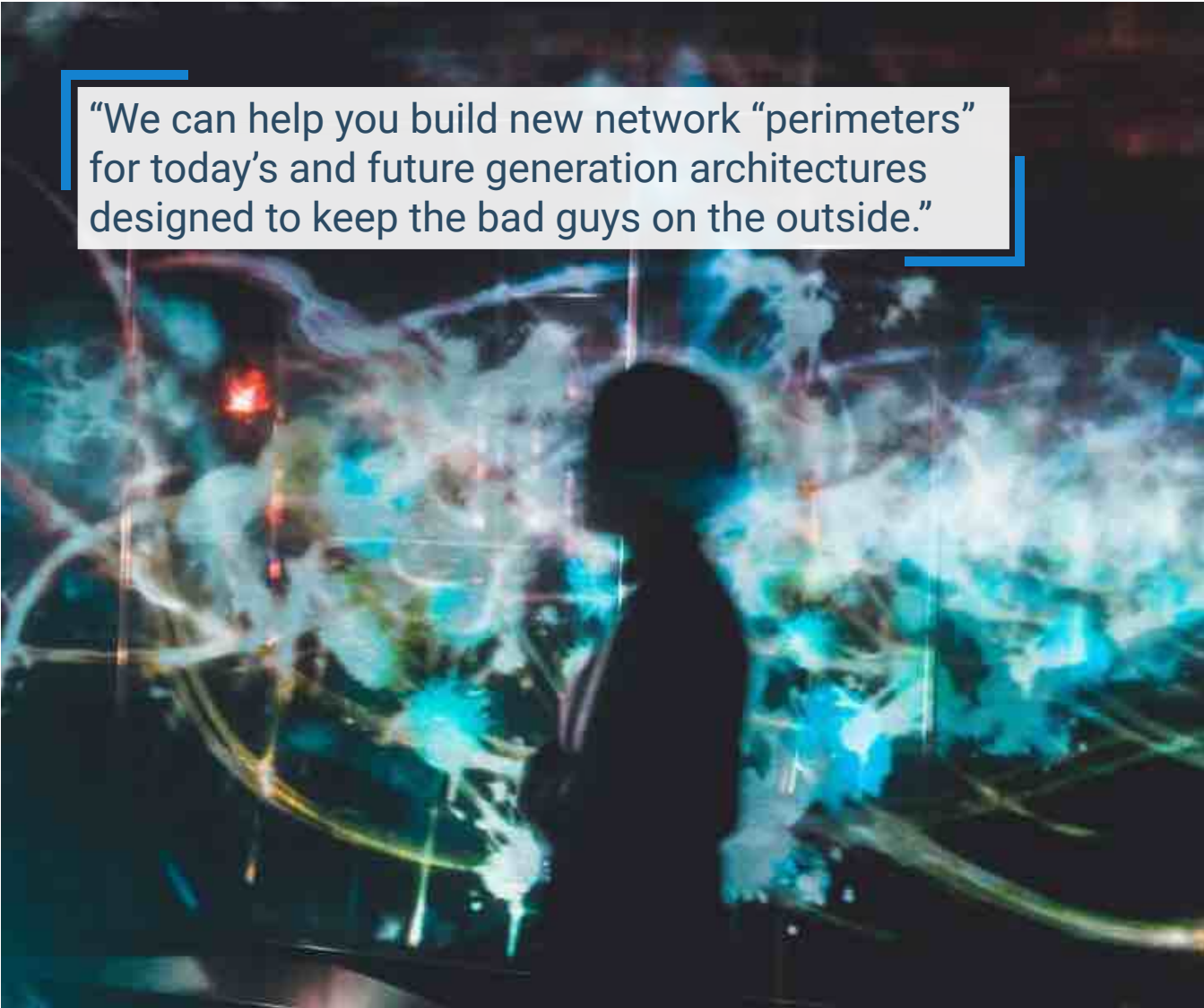
If your top priorities for cyber security spending align with these priorities, consider how we can help.

Following the guidelines outlined above we can help you build new network “perimeters” for today’s and future generation architectures designed to keep the bad guys on the outside.

Blu5 is proposing an alternative approach to threat detection and prevention. With simplicity as its core and ROI as continuous destination, we support businesses in their digitization challenges improving cost efficiency without sacrificing security.

References:

- [1] Gartner: Forecasts Worldwide Information Security Spending to Exceed \$124 Billion in 2019
- [2] Gartner: Forecast Analysis: Information Security, Worldwide, 2Q18 Update
- [3] Risk Based Security: 2019 on Track to Being the ‘Worst Year on Record’ for Breach Activity
- [4] Visible Ops: The Visible Ops Handbook (summary available at [http://www.wikisummaries.org/wiki/Visible\\_Ops](http://www.wikisummaries.org/wiki/Visible_Ops))
- [5] RSM: The high cost of maintaining the tech status quo in manufacturing



**“We can help you build new network “perimeters” for today’s and future generation architectures designed to keep the bad guys on the outside.”**



The  
Cybersecurity  
Observatory

Europe - *First Edition*

[www.sedesk.eu](http://www.sedesk.eu)