

The Observatory

GCC

September 2021



Insight

BLU5

Stop Reacting, Start Planting the Roots
for Cyber Resilience



Stop Reacting, Start Planting The Roots for Cyber Resilience

Authors: [Antonio Varriale](#), Group CTO and [Giorgia Somma](#), Business Development Manager at [Blu5](#)

At a glance

- 5 minute read 🕒
- Absolute security is absolutely impossible
- Gaining ground on the cyber attackers
- What is Cyber Resilience?
- An Inverse Logic approach



Absolute security is absolutely impossible

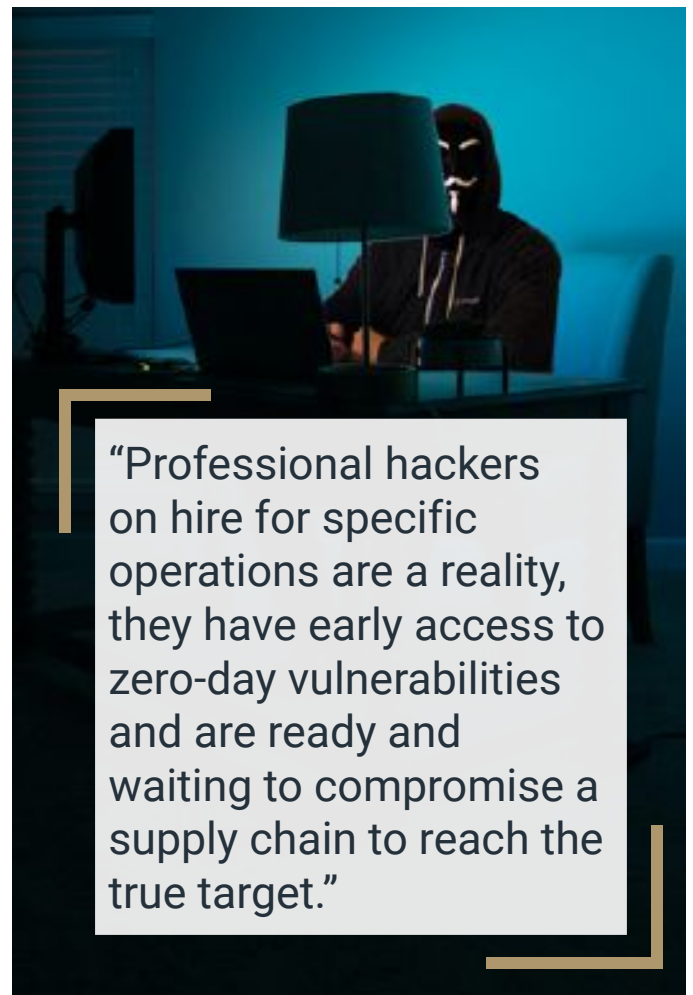
After all, it only takes one click to compromise an entire network. Continued diligence from users and investments from key stakeholders to foster a truly secure environment will be a required part of doing business in the years to come.

Gone are the days of checking off a box for the sake of compliance. Or, assuming that industry average risk ratings are good enough. This is exactly the type of mindset that cyber criminals are searching for when choosing their next target.

Threat actors are targeting new industries, using higher-pressure tactics to escalate infection consequences and

to render trusted detection methods too slow. Response options are becoming more complicated.

Attacks are growing and are more sophisticated[1]. Professional hackers on hire for specific operations are a reality, they have early access to zero-day vulnerabilities and are ready and waiting to compromise a supply chain to reach the true target.



“Professional hackers on hire for specific operations are a reality, they have early access to zero-day vulnerabilities and are ready and waiting to compromise a supply chain to reach the true target.”

According to Gartner's report on Top Security and Risk Trends for 2021, it is highlighted that ongoing strategic shifts in the security ecosystem are expected to have broad industry impact and significant potential for disruption[2].

Gaining ground on the cyber attackers

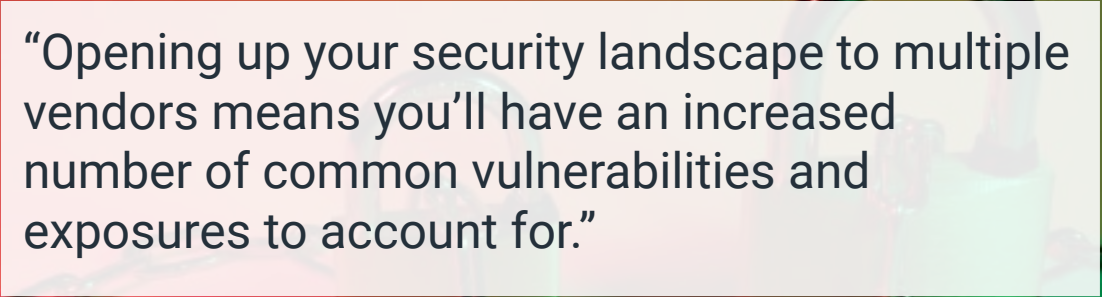
Managing security and keeping up with the latest attack trends is expensive and far from foolproof. Many attacks go undetected for months, threats are constantly evolving and motives have changed, from being a hobby to a financially rewarding activity. Despite an increase in awareness and a general shift from reactive to proactive security measures[3], security teams are still playing catchup when it comes to protection whilst cyber-criminals quickly adapted their tactics to suit the changing attack surface.

For too long, organizations have focused on building layers of protection for networks, systems, and data being under the illusion that such strategy would keep the bad guys out. The reality


is that today security leaders have too many tools in place. "In the 2020 CISO Effectiveness Survey, Gartner found that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more[4] and cyber-attacks are still on the rise.

Opening up your security landscape to multiple vendors means you'll have an increased number of common vulnerabilities and exposures to account for. That can be costly and time consuming. Auditing for compliance will involve extensive document collection, moving between platforms, and generally take up much more of your internal resources to perform effectively. According to Gartner report, 80% of organisations believe that consolidating vendors is the right path to reduced costs and increased security. [5]

All this considered, organisations and their users will never be completely free from cyber risk, so trying to eliminate it all, with a layered security approach, would not only be impossible, but would also impede agility, since an environment with an acceptable level of risk enables innovation.



“Opening up your security landscape to multiple vendors means you’ll have an increased number of common vulnerabilities and exposures to account for.”



“Cyber resilience involves accepting the fact that no cybersecurity solution is perfect or capable of protecting against every possible form of cyber threat.”

As a matter of fact, a true shift in the security paradigm is required: move from a cybersecurity posture to a cyber resilient one. In brief, rather than spending increasing time and resources to keep the bad guys out in an unequal and losing battle, simplify the security infrastructure to what is really necessary and strive to become cyber resilient.

Cyber resilience involves accepting the fact that no cybersecurity solution is perfect or capable of protecting against every possible form of cyber threat. To achieve cyber resilience, organizations should move away from fragmented security infrastructures toward one that is optimized to operational needs, and can empower IT teams to continuously maintain operations despite adversities.

What is Cyber Resilience?

The resilience concept has been used for decades in several disciplines, such as medicine, physics, social sciences, materials science, to measure the ability to quickly recover from traumatic events.

The same concept has been recently introduced in the digital world under the name of Cyber Resilience. Notwithstanding the fact that its definition is widely accepted as a measure of how well an enterprise can manage cyberattacks or data breaches, while continuing to operate its business effectively, the way the Cyber Resilience should work in a real infrastructure is still quite unclear and subjective.

As usually happens in marketing and sales operations, once a new concept becomes viral and starts originating new market opportunities and trends, vendors rapidly start reshaping their offer to meet the new customers' expectations. As for the Cyber Resilience concept, we find that quite everybody is aligned with its definition. However, the practical application of the digital recipe feels much more like an unbridled reuse of traditional solutions, sometimes accompanied by expensive new enhancement features, rather than being a real paradigm shift aimed at simplifying the security infrastructure and at deploying real benefits.

The final result is a very expensive arms race, which doesn't really provide companies with the ability to continue to operate their business even in the event of an attack. On the contrary, in most of the cases, this approach just generates extra costs and it undermines the companies' adaptability and recoverability.

According to most of the cyber security players, Cyber Resilience includes four main components: protection, recoverability, adaptability and durability.

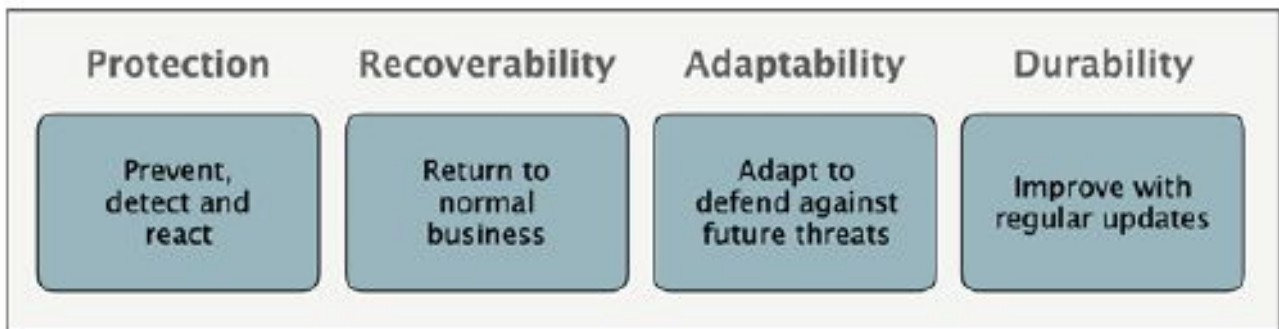
This representation may seem an effective extension of the traditional cyber security strategies (prevention, detection, reaction, ...). However, it is based on a mere quantitative enrichment of standard operations and best practices for dealing with continuous adaptation to a changing security landscape.

The real point is that, sooner or later, even the most structured organizations could be defeated in this game of power and eventually the threats would become successful attacks. The question is: "What happens to your business when your cyber security measures fail?"

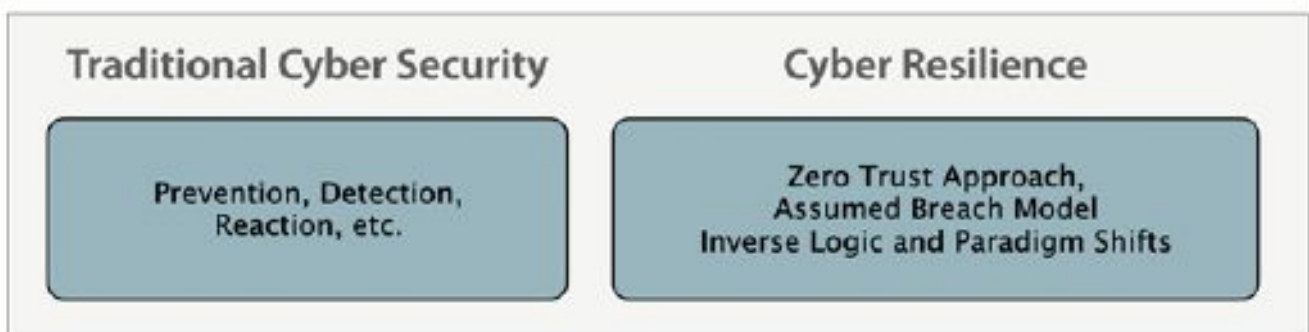
From a customer's perspective, a cyber resilient strategy should work even when the cyber security measures are bypassed and your infrastructure is compromised.

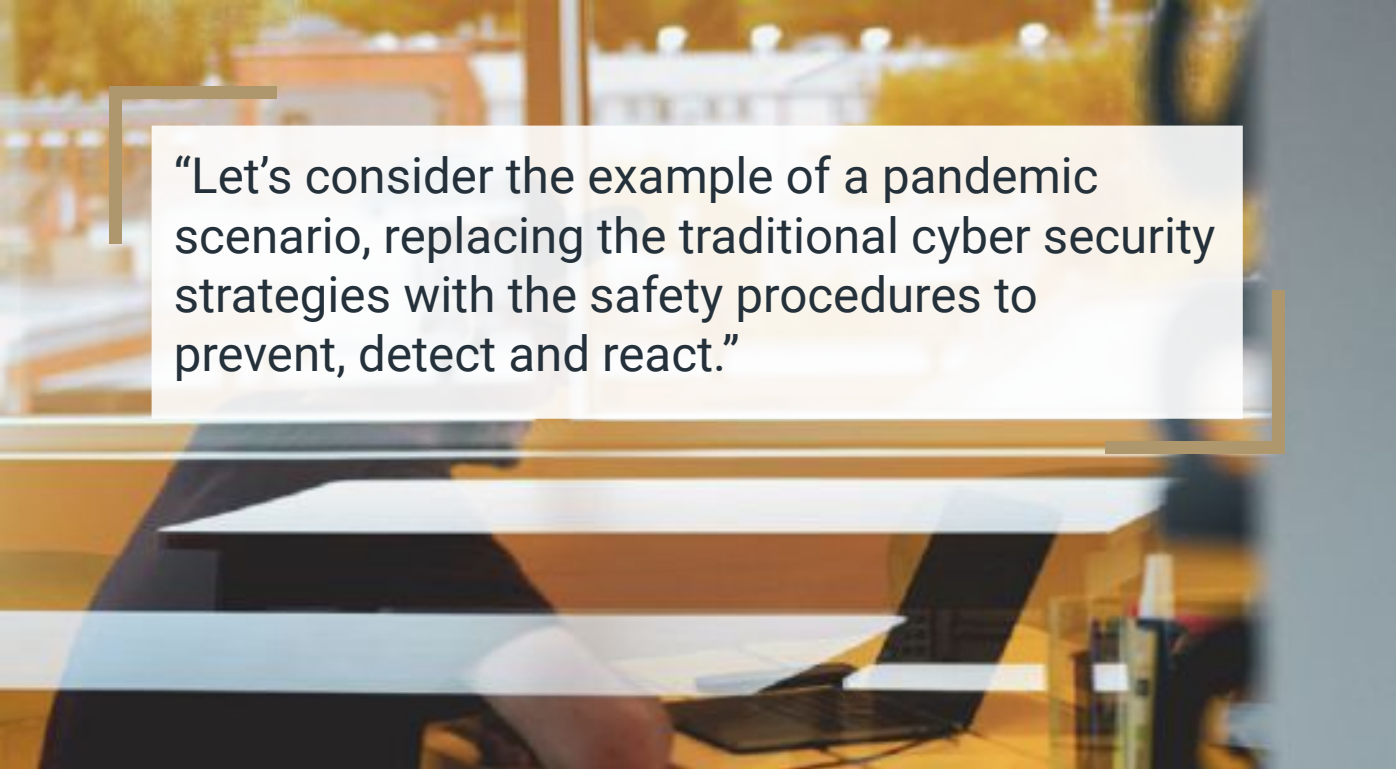
Under this assumption, a more accurate representation of Cyber Resilience can be designed. Customers deserve much more than a questionable extension of traditional cyber security strategies. Cyber Resilience shall provide a parallel way of stepping forward when the traditional line of defense doesn't deliver.

Cyber Resilience includes four main components:



A parallel way of stepping forward when the traditional line of defense doesn't deliver:





“Let’s consider the example of a pandemic scenario, replacing the traditional cyber security strategies with the safety procedures to prevent, detect and react.”

Let’s consider the example of a pandemic scenario, replacing the traditional cyber security strategies with the safety procedures to prevent, detect and react.

In this context, prevention is a set of procedures to minimize the risk of infection, such as social distancing, the use of masks and other physical protections, obsessive hand washing, object cleaning, ...

Detection is the ability to find whether objects or individuals have been or are currently contaminated with the infectious organisms.

Reaction is the capability to take an immediate action once the infection has been detected, such as hospitalizing people, ...

According to the first representation, based on a vendor perspective, Cyber Resilience should just enhance and extend the procedures above in order, for example, to improve the process when a second wave of infection comes up

(adaptability) or to regularly update the procedures with new restrictions and rules (durability), ...

However, once the processes above fail and a person gets infected, there is no guarantee on their effective recovery and, in some cases, the outcome may be lethal.

On the other hand, in the second representation based on a customer’s perspective, a Cyber Resilience strategy assumes that all the procedures above may sooner or later fail (assumed breach model), so any person as well as any object is potentially an infection vector (zero trust).

Under these assumptions, a change in rules is required (paradigm shift). For example, a vaccination strategy guarantees that people keep living their normal lives (i.e. operating their business effectively) even when the traditional prevention, detection and reaction procedures (i.e. traditional cyber security) fail, thus providing a parallel course of action.

Clearly, Cyber Resilience is not just an extension nor an improvement of the traditional security processes, techniques and solutions. A real paradigm shift is required to play the cyber game in a new and disruptive way.

An Inverse Logic approach to keep ransomware at bay

Blu5 solutions support organizations to become cyber resilient maintaining continuity of operations by adopting an Inverse Logic approach focused on the following principles:

1. **Reducing the complexity of the secure infrastructure** by eliminating outdated technologies focused on mitigating security issues rather than eradicating the causes
2. **Building access paths only after applying successful controls**, abolishing the concept of predefined routes exposed to the WAN
3. **Services are virtually running on the endpoint for use** rather than giving access to the entire company network

4. **Applying access control at the source** authorizing the good guys instead of detecting the bad guys

Contact [Blu5](#) to discuss how you can start building cyber resilience into your security strategy.

References:

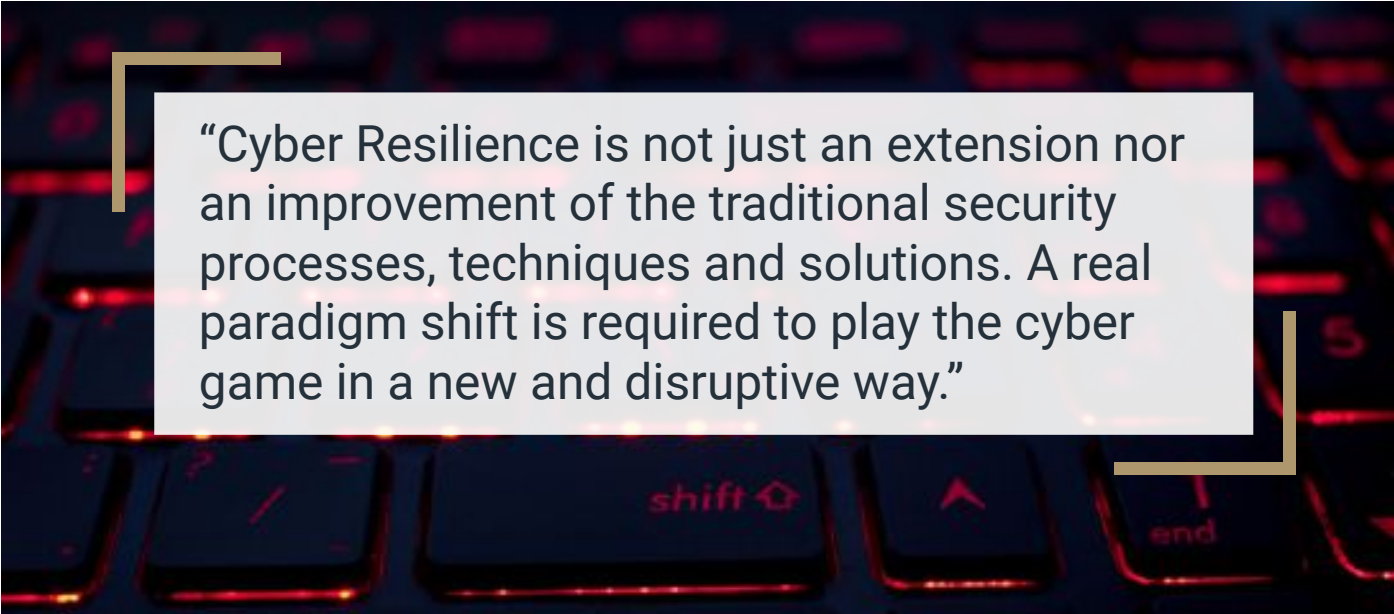
[1] CSO Global Intelligence Report: State of Cybersecurity 2021, 30th July 2021. (<https://www.csoonline.com/article/3627274/cso-global-intelligence-report-the-state-of-cybersecurity-in-2021.html>)

[2] Smarter with Gartner: Gartner Top Security and Risk Trends for 2021, April 5th 2021. (<https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021>)

[3] Fireeye-Madient Annual threats report: M-Trends 2021

[4] Gartner: Top Security and Risk Management Trends 2021, 30th March 2021 (<https://www.gartner.com/document/3999990>)

[5] Smarter with Gartner: Gartner Top Security and Risk Trends for 2021, April 5th 2021. (<https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021>)



“Cyber Resilience is not just an extension nor an improvement of the traditional security processes, techniques and solutions. A real paradigm shift is required to play the cyber game in a new and disruptive way.”



The
Cyber Security
Observatory

GCC - Third Edition