



# How Cybersecurity-as-a-Service Will Benefit Your Business

WHITEPAPER

# How Cybersecurity-as-a-Service Will Benefit Your Business

---

We've all heard the phrase, "If it ain't broke, don't fix it." But what happens if cybersecurity is broken and you don't fix it? Unfortunately, that is the current state of much of the industry. As technology continues to move at a breakneck pace and more companies automate, support virtual workers, and transfer gigabytes of data to the cloud, the amount of data promises to grow exponentially.

Security and compliance are top-of-mind concerns for today's executive. According to the [Bureau of Labor Statistics](#), information security analysts job growth is projected at a whopping 31% over the next 10 years, much higher than the average job growth rate in all industries. Cybersecurity applications and solutions flood the market, generating millions of system alerts and vulnerability reports throughout the corporate world.

At the same time, reports of cybersecurity breaches, hacking incidents, and compromised financial systems are still alarmingly common.

The cybersecurity industry is in desperate need of disruption, disruption that will revolutionize the way security is viewed by all employees and how security problems are identified and resolved. The next generation of cybersecurity must be service-based, outcome-focused, and resolution-driven.





## Table of Contents

<b>How Cybersecurity-as-a-Service Will Benefit Your Business .....</b>	<b>2</b>
<b>An Industry Ripe for Transformational Change .....</b>	<b>4</b>
<b>Why Cybersecurity-as-a-Service is the Future .....</b>	<b>5</b>
<b>Why Existing Cybersecurity Solutions Don't Cut It.....</b>	<b>6</b>
TIME-TO-VALUE WITH CSAAS .....	6
<b>It's Time for Cybersecurity Disruption.....</b>	<b>7</b>
START WITH YOUR DESIRED BUSINESS GOALS .....	7
BUILD SOLID ARCHITECTURE, REMEDIATE SIGNALS, IGNORE THE NOISE .....	8
STRONG CYBERSECURITY STARTS WITH CULTURE.....	8
KEEPING UP WITH THE CYBER SKILLS SHORTAGE .....	9
<b>The Cyvatar Advantage: Cybersecurity-as-a-Service .....</b>	<b>10</b>



# An Industry Ripe for Transformational Change

---

When chief information security officers (CISO) step into their roles at an organization, they want to deliver secure, measurable outcomes. Unfortunately, most cybersecurity products do not deliver outcomes; they focus instead on identifying vulnerabilities. Today's cybersecurity industry is all about discovering potential risks and communicating those risks through regular alerts and reports.

Although identifying vulnerabilities is certainly an important part of cybersecurity, most organizations simply do not have the talent or resources to address and fix the identified issues. As a result, systems continue to get hacked amidst all the noise of vulnerability alerts.

A secondary issue is that many smaller companies are seeking an easy way to check off a compliance box to continue doing business. Compliance does not equal security, and missing this important point can put entrepreneurial companies at great risk. Unfortunately, many vendors will help small companies "get compliant," which is all well and good until they are compromised. Both, however, can be achieved with the right approach.

Today, cybersecurity is in everything and continues to expand. Companies are undergoing digital transformation and moving everything to the cloud. Businesses are working with a larger and larger remote workforce. All of these open new cybersecurity issues, and yet, most CISOs are forced to work with the same level of resources they had years ago.

As a result, companies are surrounded by more vulnerabilities than ever while facing a critical shortage of capable security professionals. Cybersecurity executives, products and consultants are all focused on finding the problems, and no one has the time to make the needed fixes. Corporate culture pushes security out of individual jobs and into the CISO's office, which bears all the risk, absorbs the company stress, and finds too few resources and support to bring the organization to an ongoing, secure state. Something must change moving forward.

# Why Cybersecurity-as-a-Service is the Future

Roll back a couple of decades and see the seeds of cybersecurity planted in Hollywood movies where hacking was portrayed as cool, thrilling and fascinating. One of the long-standing, security-focused conferences is the Black Hat, which has been around for more than two decades. Much of its content is focused on how to hack into and compromise systems in order to teach how to protect against these breaches. More than 4,000 cybersecurity companies have entered the market during this time, “making money off the insecurity of security.”

Many businesses and organizations embark on a cybersecurity initiative or program after a breach occurs, in hopes of preventing future instances. It’s a reactive mindset that forces all the players into the wrong spaces. A business gets hacked, then hires a CISO or purchases a cybersecurity product, which identifies multitudes of vulnerabilities. No industry remediation conferences exist to tell them what to do next. Many well-qualified CISOs are saddled with reams of compliance regulations and have third-party assessors pressuring them to get secure, prove the level of security, and document it all through extensive questionnaires--all with no staff. It becomes a no-win situation. Identified issues remain unresolved, and in many cases, the business stays vulnerable to the next attempted hack.

If a breach results in a lawsuit, legal teams will be calling cybersecurity professionals as expert witnesses. Why? Because the harmed party of the lawsuit will be looking for evidence that the company knew it was vulnerable and did nothing to prevent the incident. It’s one of the major issues surfacing with today’s “identify, alert, report and abandon” cybersecurity cycle.

It’s easy to understand how things got to where they are today, but it’s time to shift gears. It’s time to find a disruptive solution--one that will change how cybersecurity approaches the challenges of today and the future to be more effective, compliant and secure.







# Why Existing Cybersecurity Solutions Don't Cut It

Cybersecurity is not viewed as “everyone’s issue” but a problem to be dealt with by an understaffed, overwhelmed CISO, a value-added reseller, or a managed security service provider. The three most common scenarios are summarized below.

## TIME-TO-VALUE WITH CSAAS

The average tenure of a CISO is about 17 months, and the story is often the same from company to company. If resources are available to hire a team, that process alone can take three to six months to find qualified professionals. More often than not, a CISO is going it alone and may spend three to four months doing proof of concept across technologies to review, test and select a solution. Once that decision is made, a limited staff needs to install, configure and assess the new system.

Since resources are scarce, the entire process can be discouraging and many CISOs go in search of the next position when the layers of bureaucracy and company politics bring their efforts to a grinding halt. Due to the shortage of experienced security professionals, there are always dozens of offers waiting for the disgruntled CISO. Unfortunately, the scenario often plays out in nearly the same manner at the next business.

Thousands of cybersecurity companies repackage existing off-the-shelf solutions and attempt to bring them into businesses. However, the services usually consist of sending alerts and notifications and finding vulnerabilities. They often cannot and will not fix discovered issues, expecting the client to manage remediation. Unfortunately, most do not have the resources to do so internally and many clients may question what value is actually added in these relationships.

Most managed security service providers (MSSPs) offer monitoring services, again, sending alerts to the customer as their deliverable. With no resources and expertise, the original problem remains. In some cases, if an incident has already occurred, an MSSP will provide remediation services. However, this is a reactive, after-the-fact service and may fail to achieve future protection and prevention.

# It's Time for Cybersecurity Disruption

---

According to a recent survey, 55% of respondents see more than 10,000 alerts per day and 27% try to handle more than a million alerts per day. That is a staggering number of vulnerabilities and attempting to manage that level of noise is clearly overwhelming.

Cyvatar, a subscription-based cybersecurity-as-a-service company, is focused on trending down these alerts through a four-pronged approach: starting with desired outcomes, remediating highest priority vulnerabilities, shifting corporate culture to make security everyone's job, and training future security professionals properly. As high-priority issues are fixed, the number of vulnerabilities decreases, making it possible to create a compliant and secure system.

## START WITH YOUR DESIRED BUSINESS GOALS

Although there are many amazing cybersecurity products and technologies available, they cannot be one-size-fits-all. It's time to move the starting point to a company's particular desired outcome.

By understanding what you want to achieve and what outcome is most important, you can apply the right technologies, maintain ongoing security, and provide executive-level reports that distill out the most important measurable outcomes to follow.

It's critical to understand your business and clearly define specific outcomes that protect critical and sensitive data. At that point, solutions that make the most sense in that specific case can be employed.



## BUILD SOLID ARCHITECTURE, REMEDIATE SIGNALS, IGNORE THE NOISE

It's important to start with a solid architecture and properly installed security products. Unfortunately, many companies fail on both these fronts. For example, one business had placed their demilitarized zone (DMZ), or physical subnetwork that contains external-facing components, outside of its firewall. In addition, role sets were not configured correctly, and its mail server was improperly sitting on an internal network, allowing outside traffic to access both the mail and DNS server.

All of these architectural issues need to be fixed before installing cybersecurity tools, which then need to be installed, configured and assessed to actually remediate risk to achieve a clean state.

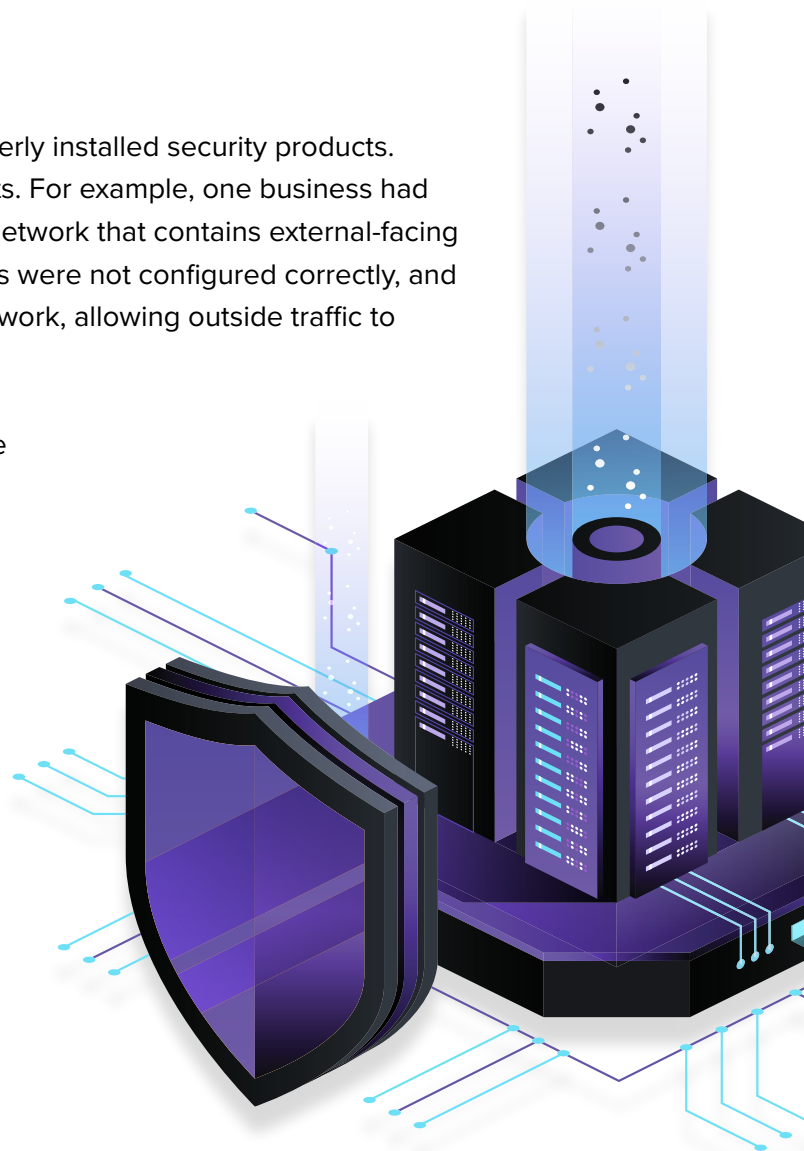
The majority of the alerts sent by monitoring software are simply flagging harmless noise. However, the sheer volume of noise can make it difficult to hear the signals or find the true vulnerabilities. By remediating the signals, you'll not only minimize vulnerabilities but you'll decrease the noise as well.

## STRONG CYBERSECURITY STARTS WITH CULTURE

Cybersecurity cannot be only the CISO's job; it needs to span across the entire organization. Everyone needs to be empowered to adopt an ongoing culture of security.

Along those lines, security cannot be viewed as a one-and-done process. Cybersecurity professional Bruce Schneier said in the early 2000s that "security is a process, not a product." It's a continuous improvement process that needs to be ongoing to be successful.

New vulnerabilities will continue to surface, and companies must have a way of monitoring, remediating and protecting critical assets, data and systems on a continuous basis.



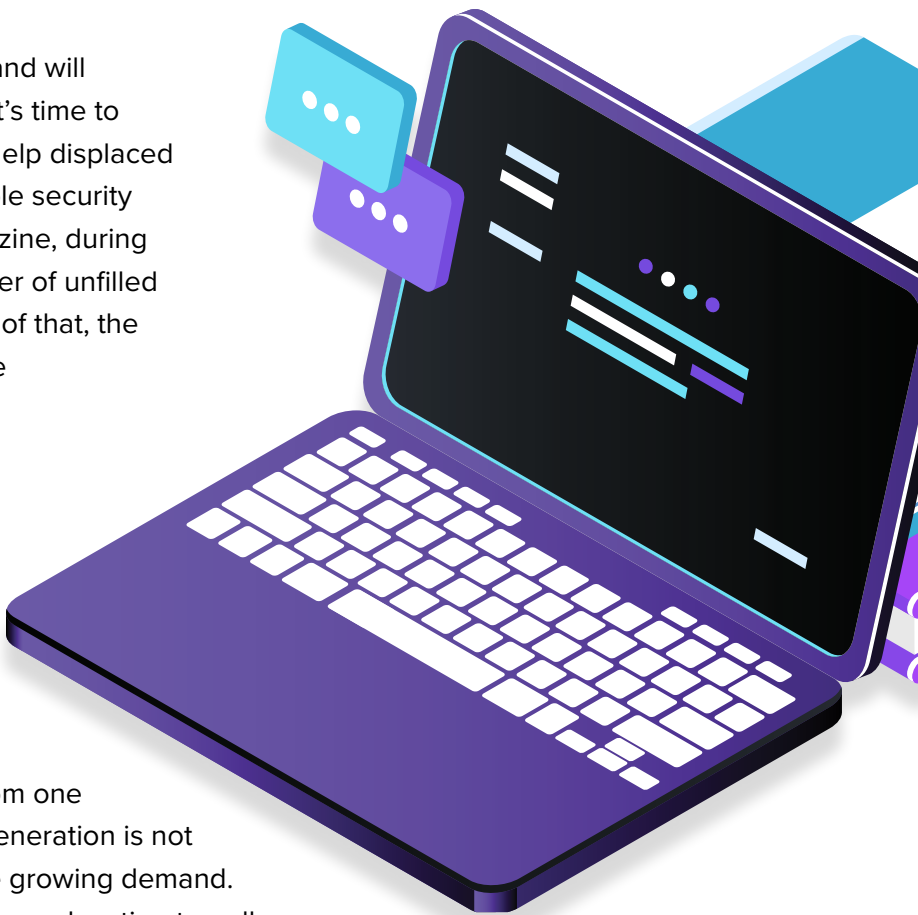


## KEEPING UP WITH THE CYBER SKILLS SHORTAGE

It's clear that cybersecurity is a growing field and will continue to be in demand for years to come. It's time to ramp up training and education programs to help displaced professionals from other fields become capable security professionals. According to Cybercrime Magazine, during the period between 2013 and 2021, the number of unfilled cybersecurity jobs grew to 3.5 million. On top of that, the article reported that fewer than one in four are even qualified.

The industry and technology is changing rapidly, and even seasoned CISOs are struggling to keep up with the latest developments, especially when it comes to artificial intelligence tools that can assist with cybersecurity remediation.

Currently, IT security recruiters are stealing from one company to staff another while the younger generation is not obtaining the training they require to meet the growing demand. It's time for professionals, businesses and higher education to pull together and truly address this huge systemic issue through future training and continuing education initiatives.



# The Cyvatar Advantage: Cybersecurity-as-a-Service

---


Based on decades of expertise in the industry, Cyvatar's management team has worked to build a disruptive solution: cybersecurity-as-a-service (CSaaS).

We procure, install, configure, assess, and remediate cybersecurity issues. We have the products, the staff, and the experience and expertise. Ultimately, that leads our customers to a positive outcome. In today's environment, it is significantly more expensive to recruit and train an internal staff, purchase products, and then install, configure and assess them on your own. By taking advantage of Cyvatar's subscription-based cybersecurity-as-a-service, customers will save money.

When you start a conversation with our team, we'll begin by breaking down the costs of what you need. Depending on your organization's size, that might be one or two full-time equivalents (FTE) to complete the whole process and manage it. We'll then take the cost of an FTE for a year plus the cost of the products required for your custom solution. The pricing comparison is transparent. You'll quickly see that your costs to manage cybersecurity internally will be far more expensive--even if you happen to find an experienced CISO that stays with you through the end of implementation--than the monthly subscription price for Cyvatar's services.

In addition, Cyvatar can scale your cybersecurity solution as your needs grow. We've vetted best-of-class technology solutions for certain applications and company sizes and can provide economical solutions that deliver a compliant, secure and clean state on an ongoing basis.

This, in turn, frees up your staff to focus on operations. Different team members can oversee the security aspects related to their jobs or departments and provide input, but they don't have to actually manage or remediate vulnerabilities.



We provide outcome-based subscriptions. Everything we do at Cyvatar is measured so executives outside of cybersecurity can know how much money your company has spent and exactly what was delivered. We communicate clear metrics across our dashboard, and we focus on your top priorities.

For example, if a customer comes to us and wants multi-factor authentication (MFA) across the entire organization, that customer can enter how many users they would need into Cyvatar's platform and calculate their own cost. If the cost is agreeable, the customer purchases the subscription, and we take care of the rest. They don't have to review products; we've selected pre-vetted and best-in-class technology solutions. We come and install, configure, assess, remediate and maintain (ICARM). The whole process for an actual customer took roughly two to three months to establish a secure MFA state.

Cyvatar's default executive dashboard has 20 controls, which are prioritized to give each company a unique roadmap for next steps. Different businesses are in different places. If you have nothing, we'll start with securing your assets and then moving through IT vulnerability management. If you have that foundation laid, we can assess your assets, remediate and patch as needed, starting from the top priority, or your highest risk.

# To Wrap It Up...

---

Cybersecurity is a hot industry with growing demand for the best professionals. The industry as a whole has had to scramble to keep up with the changing demands, the evolution of technology and AI sophistication, and the needs of its customers. As a result, many opportunities for improvement exist throughout the entire industry.

Cyvatar's mission is to fulfill a desperate need for compliant and secure solutions, focused on remediation, working as a partner to CISOs or company executives seeking a more stable and secure state for their organizations with cybersecurity-as-a-service. Visit our website at [cyvatar.ai](https://cyvatar.ai) to start your CSaaS journey with us today.

**[Check out our latest eBook! | 8 Epic Cybersecurity Fails >](#)**