corero

Growing, Growing, Gone?

Managing cyber risks as your business expands.

Managing cyber risks as your business expands

The old adage "more money, more problems" rings especially true in the business world. As your company grows, it doesn't just attract more revenue and acclaim—it also becomes a bigger target.

This escalation isn't just about market competition; it encompasses security vulnerabilities as well. Nowadays, it's all too common to see headlines about major businesses suffering data breaches or grappling with service disruptions from DDoS attacks. DDoS attackers, who can also be indiscriminate in their choice of targets, pose a significant risk to companies across all sizes and sectors. Perhaps your business operates in IT, finance, healthcare, or education—sectors that frequently find themselves targeted due to their critical operations and data-intensive activities.

So, it's crucial to ask yourself:

As your company scales,

is your team prepared to handle disruptions without pulling resources away from essential projects?

Are you keeping up

with the latest threat intelligence and attack methods to safeguard your systems effectively?

How about keeping pace

with new regulations and laws concerning cybersecurity?

Do you fully understand

the impact that downtime and service disruptions could have on your business's trust and finances?

While not exhaustive, these critical questions are essential for every growing business to consider as they aim to bolster resilience against an increasing number of cyber threats.

ARE YOU PREPARED TO MEET THIS CHALLENGE?

The strategic importance of up-to-date threat intelligence

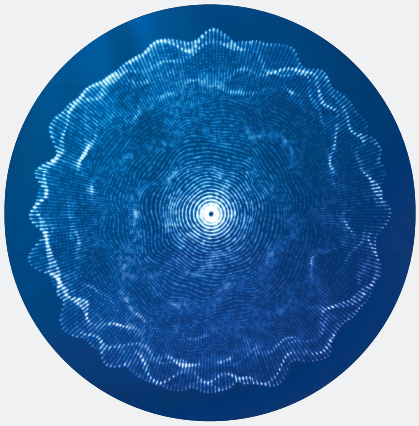
Staying current with the latest threat intelligence and understanding emerging attack methods is fundamental to ensuring your network is resilient and services remain operational.

The ability to quickly adapt and respond to new threats is not just advantageous—it's essential for maintaining uninterrupted service and customer trust.

Are you and your team equipped to continuously monitor and adapt to these cyber threats?

If not, is there someone within your organization

who can take on this critical role, or would it be more efficient, and effective, to engage with an external service provider?



Many service providers offer threat intelligence

that not only fine-tunes your protection solutions but also delivers insights, analysis, and high-level reporting.

These services help demonstrate the value

of maintaining robust protection solutions, underscoring the importance of your investment in cybersecurity.

Outsourcing this responsibility could enhance your defenses and ensure that your network security stays a step ahead of potential attackers, thus preserving service availability and protecting your business's reputation.

Are you adapting your cybersecurity strategies to meet evolving regulations?

As businesses grow, especially within European and U.S. markets, the importance of complying with emerging regulations such as the Digital Operational Resilience Act (DORA) and the guidelines from the Cybersecurity and Infrastructure Security Agency (CISA) cannot be overstated.

ESMA
European Securities and Markets Authority

DORA, enacted by the European Securities and Markets Authority (ESMA),

requires all entities in the financial sector to develop robust mechanisms for digital operational resilience.

This includes safeguarding against a wide range of Information and Communication Technology (ICT) disruptions and security breaches.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

In the U.S., CISA underscores the necessity for critical infrastructure sectors to boost their defenses against cyber threats,

which includes deploying comprehensive cybersecurity measures to detect, prevent, and respond to potential threats like DDoS attacks—pressing concerns in both European and American contexts.

Complying with DORA and CISA isn't just about fulfilling legal obligations.

It's about proactively strengthening your digital operations' resilience.

Businesses must adopt advanced and effective cybersecurity practices
to ensure uninterrupted service and maintain customer trust.

This involves crafting sophisticated strategies to handle cyber incidents
such as DDoS attacks, which can significantly impact operational capabilities and customer service access.

This proactive stance on digital operational resilience, influenced by both DORA and CISA, emphasizes the necessity for businesses to continually reassess and enhance their security infrastructures.

Doing so not only ensures compliance but also bolsters operational readiness and preserves customer trust in a rapidly evolving digital landscape.

By maintaining a commitment to these regulatory standards, your business can ensure that its growth is secure and sustainable, ready to meet the challenges of an increasingly interconnected world.

HOW CONFIDENT ARE YOU IN YOUR COMPANY'S COMPLIANCE AND READINESS TO ADAPT TO THESE REGULATIONS?

Protecting trust as you grow

The link between a company's reputation and its online reliability is unmistakable.

Trust, the bedrock of customer loyalty, is not easily earned and can be swiftly damaged by just a single incident of service interruption.

Cyberattacks and other causes of downtime don't just disrupt business operations; they can also deeply impact customer trust.

These disruptions lead to significant revenue loss, as businesses face halted transactions and service failures that can amount to substantial financial setbacks.

Moreover, such interruptions can severely damage a brand's reputation, fostering perceptions of incompetence that drive customer churn and invite negative publicity.

Operational disruptions further extend the impact, straining everything from communication systems to supply chain management, thereby increasing operational costs and reducing overall efficiency.

There are also heightened legal and compliance risks, with potential litigation and substantial fines compromising both trust and financial health.

The path to recovery often involves costly investments in cybersecurity technologies and strategies, emphasizing the need for proactive measures.

As your business scales, the risk magnifies. The broader target on your back calls for a critical evaluation:

Is your investment in cyber defense keeping pace

with your growth and the escalating risk profile?

Failing to adequately bolster your network security

can leave your business vulnerable to cyber threats, risking not just financial loss but also reputational damage.

These challenges underscore the necessity for businesses

to continuously evaluate and adapt their security posture, ensuring their infrastructure and services are robust enough to withstand the evolving threat landscape.

By doing so, they align with their growth trajectory and the increasing complexity of cyber threats,

maintaining the integrity of their services and nurturing customer trust and loyalty.

LEARN MORE

Picking your protection team — go internal or outsource?

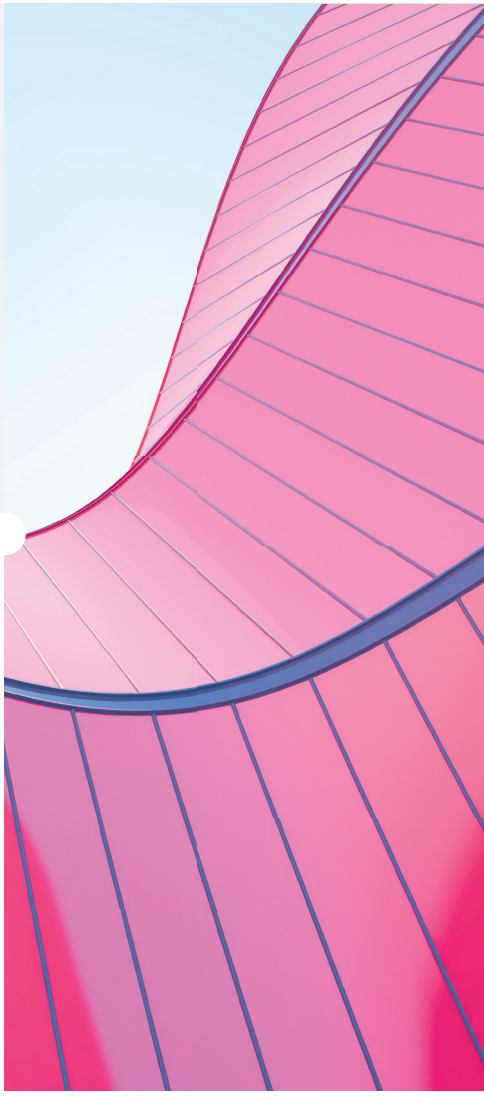
When it comes to safeguarding your business from cyber threats such as DDoS attacks, one of the big decisions you'll face is whether to handle network security with an internal team or to outsource it to a trusted partner.

Both options have their strengths and weaknesses, and the right choice depends heavily on your company's specific needs, capabilities, and the ever-changing nature of attacks.

Having your own security team offers a lot of perks, like having complete control over your security strategies and the ability to tailor your defenses to fit your specific needs.

An internal team is deeply integrated into your company's culture and operations, which can lead to faster responses to threats as they arise.

However, this option requires a substantial investment—not just financially but also in continuously educating and training your team to keep up with the latest in cyber tactics.



On the other hand, outsourcing your network security can bring in a level of expertise and experience that can be hard to cultivate in-house.

Businesses that specialize in purpose-built solutions for protecting against threats like DDoS attacks often possess a broader understanding of the cybersecurity landscape across various industries.

This can be particularly beneficial as they bring tried and tested strategies to the table.

Financially, outsourcing can be more cost-effective compared to the overhead associated with maintaining a sophisticated in-house team.

These firms can also scale their services quickly in response to growing threats or business expansion, something that can be more challenging and slower with an internal team.

However, outsourcing does come with downsides;

such as potentially having less control over your operations and slower response times during critical periods, depending on the level of service the partner provides.

There's also the aspect of data privacy and compliance with industry regulations, which can be more complex when working with an external partner.

A key point to consider is the support structure—whether your company has access to ancillary support when it's most needed.

Outsourced partners usually offer round-the-clock support and can mobilize additional resources swiftly, which can be crucial during a major security breach.

The time it takes to mitigate threats is also a critical factor.

While in-house teams may have immediate access to your systems, they might not always possess the latest tools or know-how, unlike outsourced firms that are equipped with cutting-edge technologies and strategies for quick action.

Deciding whether to go with an internal team or an outsourced partner involves weighing these factors against the backdrop of your business operations and strategic goals.

AS CYBER THREATS GROW MORE SOPHISTICATED, HAVING THE FLEXIBILITY TO ADAPT YOUR SECURITY APPROACH WILL BE KEY TO MAINTAINING ROBUST PROTECTION.

Your knight in shining armor

So, you've made it this far and you're probably wondering, "What's the solution?

Well, not to toot our own horn too loudly, but it's us.

We offer a unique managed DDoS protection service with our purpose-built SmartWall ONE™ solution, designed to seamlessly integrate with your business

Wherever you stand—whether you're leveraging existing infrastructure or in need of a hybrid approach—we're ready to meet you there.

With SmartWall ONE™, you're not just investing in technology; you're gaining a partner in innovation and reliability.

Tailored for businesses grappling with both cyber threats and regulatory compliance, our solution ensures your service stays uninterrupted and ahead of any legal curve.

Corero's SmartWall ONE™ Fully Managed Service enhances this protection by offering round-the-clock DDoS management from our team of experts.

Imagine the peace of mind that comes with this service, all available for a fixed yearly subscription.

In addition to Corero SmartWall ONE™ managed services, which provide the threat intelligence you need to shift from a reactive to a proactive cybersecurity strategy, we deliver a truly 'white-glove' experience.

This approach lifts the weight of DDoS threats off your shoulders, allowing you to focus on what you do best—running and growing your business, without disruptions.

By choosing SmartWall ONE™, you're not just securing peace of mind.

You're choosing a strategic partner committed to keeping you resilient, compliant, and competitive in today's fast-paced market.

In your case, success doesn't have to mean more problems.

Discover how we can safeguard your business today.

Ready to secure your operations effortlessly?

SPEAK WITH A SPECIALIST

[Visit **corero.com** to discover how we can safeguard your business today.]