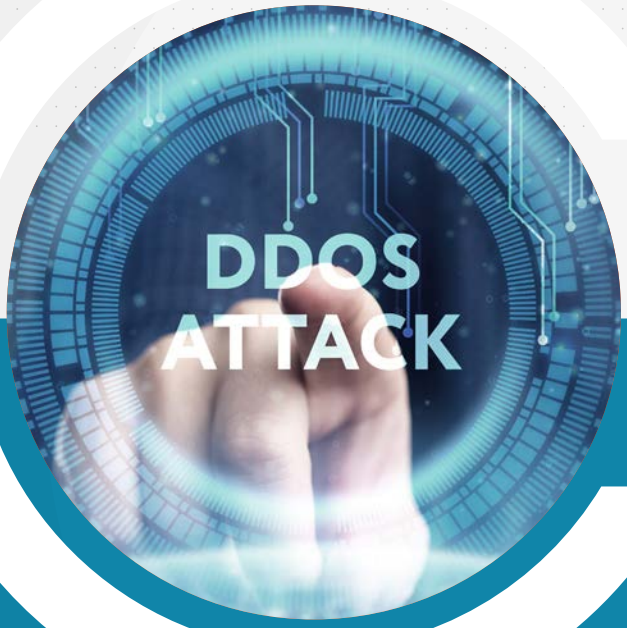
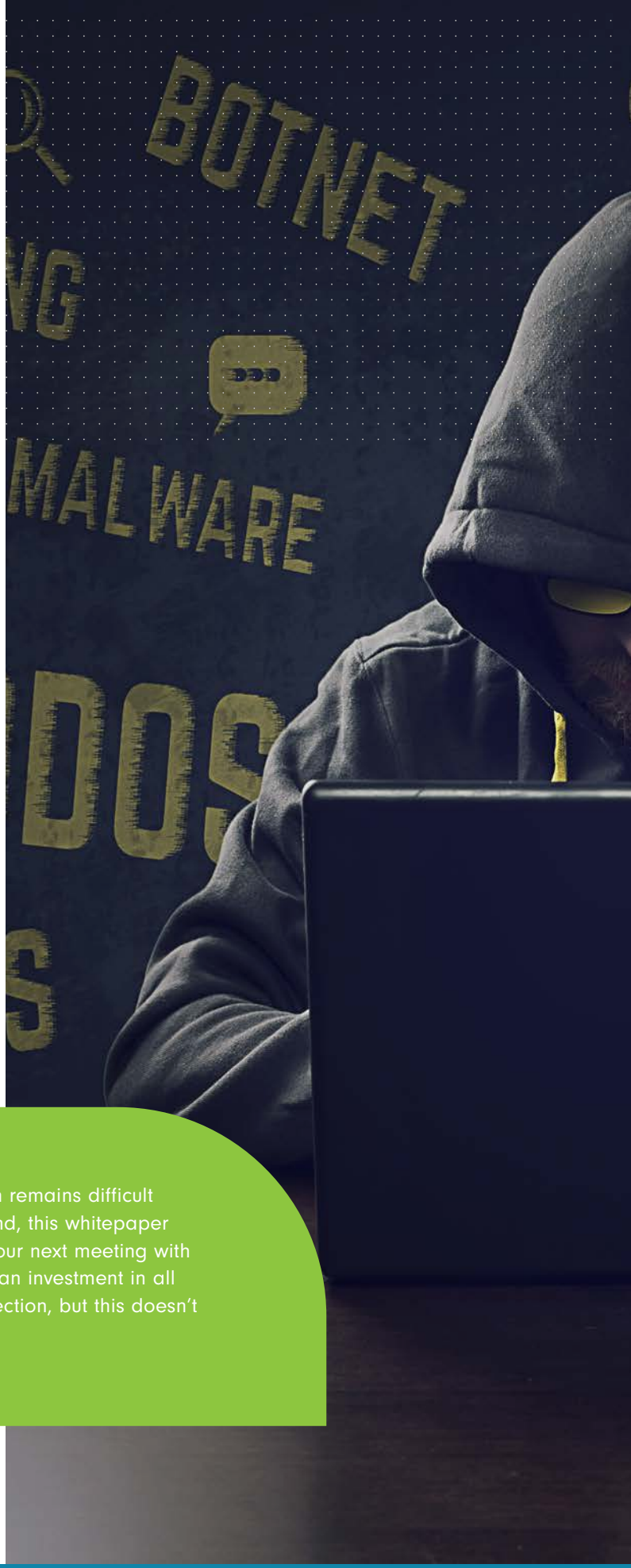


corero

Pitching DDoS Protection to Your Enterprise C-Suite

corero



Distributed denial-of-service (DDoS) attacks are increasingly a scourge of the corporate world. They attempt, and often succeed, at disrupting access to a business's website, servers, or cloud-based services. Any enterprise, that relies upon its Internet access, now needs a proactive approach to protect their organization's IT infrastructure against this growing threat.

Whenever a DDoS attack strikes, companies spend significant time and resources bringing their technical assets back online. In the interim, users and/or customers can't access their systems or services. In a competitive modern marketplace, this could be a death knell to their company.

Even with this serious risk, many enterprises aren't investing in DDoS protection to ensure 24-7 availability of their IT infrastructure. A **recent Corero survey** of tech professionals found that 58% of their employers use internally developed DDoS solutions, including naively relying on corporate firewalls. Only around one-third use either cloud-based or on-premises specialist DDoS solutions.

Convincing the C-Suite to sufficiently invest in DDoS protection remains difficult for the Security Operations professional. With that goal in mind, this whitepaper provides valuable information to use as ammunition during your next meeting with the executive team. Minimizing the risk of downtime requires an investment in all aspects of your SecOps footprint, including DDoS attack protection, but this doesn't need to scare your decision makers.

Convincing the C-Suite of the Threat of DDoS Attacks

With many enterprise executive teams hesitant to increase spend on IT security, SecOps personnel must leverage a fact-based approach to make them aware of the inherent risks. Getting buy-in from your CISO is likely to be easier than the other members of the C-Suite, especially those controlling the purse strings. So, providing examples of DDoS attacks on similar organizations, and hard statistical data on the damage they cause, is the right approach.

Remind any executives not responsible for technology divisions that DDoS attacks aren't just an IT issue. Significant downtime affects the entire organization, including sales, marketing, customer support and more, with brand reputation and revenue loss at stake.

> "Business leaders and CISOs must work together to identify and protect the "crown jewels"—those corporate assets that generate the most value for a company."
>
> **- McKinsey Cybersecurity Report**

Like other forms of cybercrime, DDoS is continuously evolving, with new attack techniques and threats making them harder to defend against. Stopping the impact from these sophisticated attacks requires a proactive approach, from a well-supported SecOps team. Failure to do so exposes any business to a host of short-term and long-term implications, including downtime, revenue loss, customer churn, regulatory issues, and more.

Unfortunately, the risk to businesses from DDoS attacks continues to increase. **A recent study from Cisco** noted that their frequency increased by 2.5 times over the past three years. With average sizes approaching the gigabit per second benchmark, undefended businesses are at risk of any attack taking their assets completely offline. Peak attack sizes are also significantly higher; already having exceeded the terabit per second mark.

More nefarious cyber actors are now using criminal extortion, requiring businesses to pay a ransom in order to prevent their DDoS attacks. With more companies now leveraging remote working and the IoT, the number of potential attack vectors is also trending upwards.

Given this increasingly dire scenario, businesses must take a proactive approach to their DDoS protection strategy. Preventing attacks from happening is now significantly more cost-effective and beneficial than costs, time and resources required to recover from the damages after the fact. Ultimately, your company's C-suite will be thanking you for fully understanding the nature of this acute risk to business continuity, and how to prevent it.

The Business Benefits of Proactive DDoS Protection

Since traditional cybersecurity tools, like firewalls and IPSs, are not equipped to effectively handle DDoS attacks, deploying specialist protection remains the wise approach. A solution combining on-premises and service-based approaches effectively fits within any business's technical infrastructure. This approach is most effective at detecting and mitigating DDoS attacks, of any type or size. Importantly, choosing the right protection option can also ensure no adverse performance issues to a company's existing IT operations:

1. Flexible Deployment:

As DDoS threats continue to evolve, deploying a future-proof DDoS protection solution becomes essential. This ensures a company has a flexible platform that delivers 24/7 monitoring with real-time alerting and automatic response to any DDoS threat, today and into the future. Additionally, automated signature creation and regular updates ensure proactive protection against new and emerging types of DDoS attack.

2. Support for High Traffic Networks:

Any DDoS solution must not cause any performance hits to the enterprise network. This is especially the case with latency-sensitive applications, like IoT or VOIP. The best DDoS protection options support high traffic network environments, with low latency, while protecting against network-layer DDoS attack vectors. Simply put, they deliver critical protection without disrupting network capacity or latency.

3. Scalable High Availability:

In a competitive modern economy, any SecOps tool – especially one focused on DDoS attacks – must protect the availability of critical business systems and services. It needs to ensure enterprise network administrators enjoy both high availability and flexible, scalable, deployment options. It ultimately enables IT infrastructure to serve as an engine for growth, instead of a bottleneck.

4. Real-Time Incident Response:

Considering the adverse impact of any successful DDoS attack, a protection tool must support optimized real-time incident response. A feature set that includes comprehensive security event management along with a thorough and detailed reporting engine enables any attack to be quickly analyzed, ensuring DDoS contributes to broader cybersecurity threat awareness, helping to prevent other malicious incidents in the future. In addition, this actionable information facilitates compliance audits, an important business consideration for many enterprises.

Options for Implementing DDoS Protection

Enterprises are faced with a variety of options for deploying DDoS protection. Of course, each approach comes with its own set of advantages and disadvantages. Any decision likely depends on the specific requirements of the organization, especially when choosing between an on-premises solution and one located in the cloud.

On-Premises DDoS Protection

An on-premises DDoS protection solution provides enterprises with the most control and visibility. At the same time, due to the levels of Internet bandwidth used by most Enterprises, any high-volume DDoS attacks, at the larger end of the spectrum, can overwhelm the available capacity. On-premises appliances can appear more costly and require a higher maintenance outlay. However, they return significant value for companies with strong compliance requirements, including governmental, financial institutions and those delivering applications as a service. Additionally, their low latency is critical for companies relying on VOIP and IoT applications.

Hybrid DDoS Protection

A hybrid approach to DDoS protection combines the strengths of an on-premises solution with the multi-terabit scalability of the cloud. In short, it's an ultra-fast, low-latency, solution for the vast majority of attacks, that seamlessly scales to very high capacity, but only when warranted. You can expect additional management overhead compared to a cloud-only solution, but this is compensated by the elimination of downtime, comprehensive visibility and actionable security intelligence which becomes available.

Ultimately, an enterprise's tolerance of downtime, sensitivity to latency, regulatory considerations, and the frequency of cyber-attacks all contribute to the final decision on the type of DDoS protection chosen. Work this through with your CISO, to determine the right approach for your DDoS defenses.

Cloud-Based DDoS Protection

A cloud-based DDoS protection service is the first choice for many organizations. The simplicity of using a service, versus deploying on-premises, is compelling. Combined with advertised capacities larger than any currently known attacks; all at a lower cost with fewer managerial responsibilities, this seems like the ideal solution. For some this can be true, but there are significant disadvantages of just relying on this approach, including, times-to-mitigation measured in minutes, high latency, less control and visibility, limited actionable security intelligence and a potential conflict with regulatory, or data sovereignty, compliance requirements.

Additionally, when it comes to cloud-based DDoS services, there are increasingly two options available. Newer always-on services, or traditional ones that are available on-demand. Let's look at the pros and cons of each:

With a traditional on-demand service, traffic only gets diverted in the event of an attack. It's a simple, low-cost solution, with minimal maintenance requirements. In this case detection is either via remote monitoring, or manual intervention, and is followed by a BGP initiated swing of the impacted traffic. Either way, an attack will already have done the majority of its damage before any mitigation is able to be activated and downtime is inevitable. This also results in a significant increase in latency for the impacted traffic during attack time, so is especially not suited to real-time traffic.

The emerging always-on approach to cloud DDoS protection helps to minimize mitigation delays when activating. This is the major advantage when compared to an on-demand service and still offers the benefit of simplicity. However, costs are significantly higher, as you are paying for your traffic to always be transported via the cloud provider's network. Also, be sure to distinguish between always-on and always-protected services. The former can mean your traffic is always routed through the provider's network in the cloud, but that they rely on out-of-band detection and redirection inside their cloud, which can still lead to damaging mitigation delays. Plus, this type of cloud protection also introduces significantly higher latency compared to an on-premises solution.

corero

SmartWall Provides Enterprises with Flexibility and Scalability

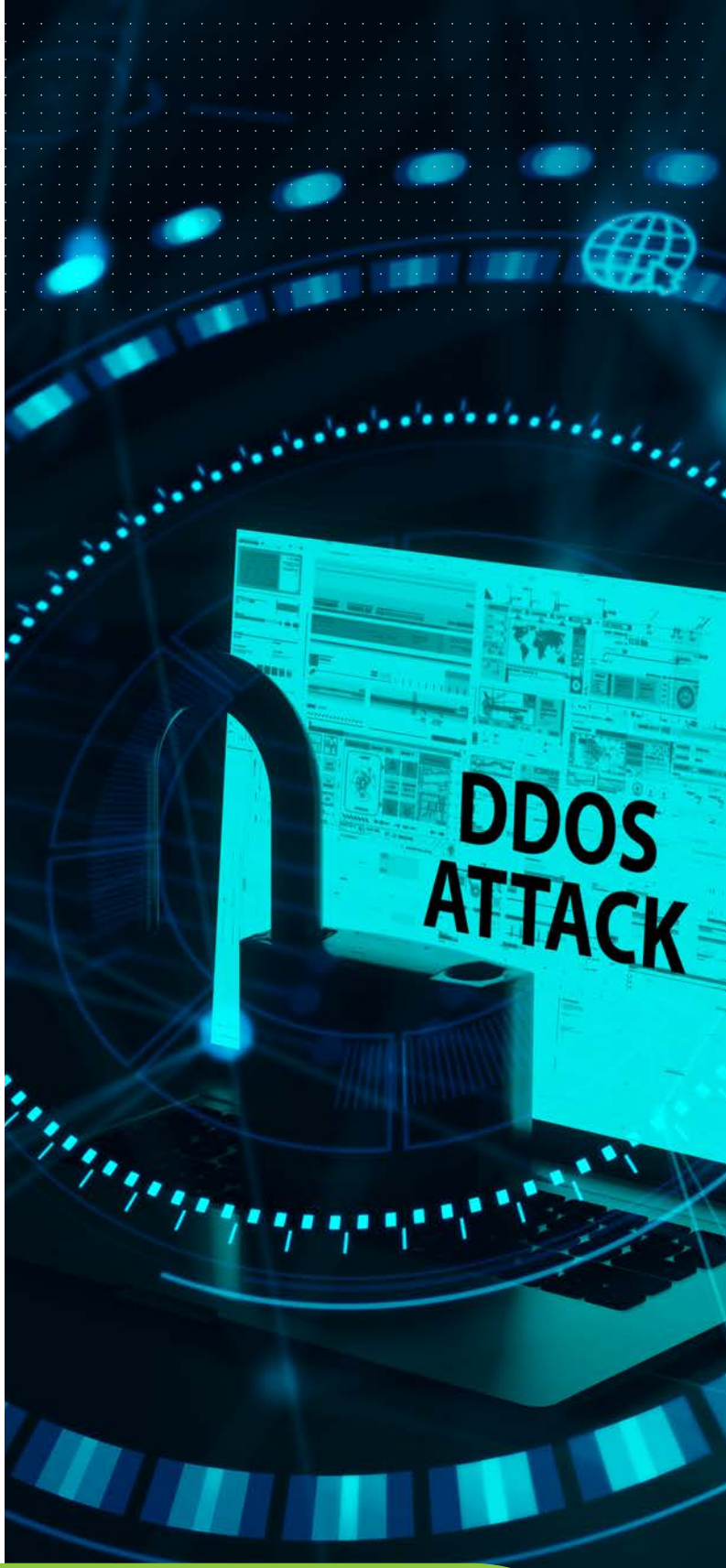
Enterprises searching for a state-of-the-art and flexible DDoS solution should have Corero's SmartWall on their short list. SmartWall delivers critical real-time responses, with automatic mitigation happening the instant an attack is detected. Its scalability ensures attacks of all types and sizes are dealt, with before any adverse impact to business operations.

SmartWall also boasts an industry-leading reporting engine delivering actionable information to your SecOps team 24x7. Executive leaders also gain the peace of mind that their business operations are comprehensively protected from the scourge of DDoS.

Corero SmartWall provides flexible deployment options based on business needs. This includes on-premises appliances for the fastest, lowest-latency protection. Additionally, SmartWall offers similar protection directly at the network edge, for supported infrastructure devices, without the need to deploy any appliances. Finally, the SmartWall Threat Defense Cloud enables a hybrid protection solution combining on-premises speed and accuracy, with cloud scale for defense against the largest of attacks.

Connect with our team at Corero to discuss your organization's specific needs for DDoS protection. Rest assured, we have a flexible and scalable solution to ensure cyber criminals can't disrupt your business operations.

CONTACT US



US HEADQUARTERS

Corero Network Security Inc.
293 Boston Post Road West, Suite 310
Marlborough, MA 01752
Tel: +1 978 212 1500
Email: info@corero.com

EMEA HEADQUARTERS

Corero Network Security (UK) Ltd.
St Mary's Court, The Broadway,
Amersham, Buckinghamshire, HP7 0UT, UK
Tel: +44 (0) 1494 590404
Email: info_uk@corero.com