Taking the Case for Advanced DDoS Protection Upstairs
TABLE OF CONTENTS

INTRODUCTION ........................................................................................................................................... 3
  In This Brief Guide, You Will Learn........................................................................................................... 3
  You Are the Guardian of Your Network .................................................................................................. 4
  Problem .................................................................................................................................................. 5
  What Senior Leaders Need to Hear From You ......................................................................................... 5
  Presenting the Arbor Solution .................................................................................................................. 7
    The Solution Is Intelligently Automated, Customizable, and Future-Ready .............................................. 7
  Top 5 Tips for Promoting a DDoS Solution Internally ............................................................................ 9
  Let Arbor Help You Make the Case .......................................................................................................... 10
    Example of Quantitative Risk Analysis .................................................................................................. 11
  Success Stories You Can Share ................................................................................................................. 12
INTRODUCTION

You recognize the need to implement an advanced solution for DDoS protection. You know it’s time to invest in an integrated system that reduces complexity and increases automation. It’s necessary to have this in place to decisively address attacks that might otherwise bring your network down and harm your business.

But how will you persuade your fellow stakeholders to invest in the solution you’ve evaluated and are about to champion? When you go upstairs, metaphorically speaking, the case is no longer deeply technical. Now, it must be about business and financial impact – dollars and cents.

This brief guide is designed to give you some compelling messages that you can take to your senior executives as you argue the case for DDoS protection. What’s essential to recognize is that you are making a case about risk management with serious monetary implications.

But it’s also about your ability to vividly demonstrate – and report on – your actions as a guardian of your network infrastructure. It’s about how you can elevate yourself in the eyes of your fellow stakeholders by communicating to them on their terms.

In This Brief Guide, You Will Learn...

1. How you will be personally benefit by taking this case to executive team
2. How your executive team stands to benefit in terms they understand
3. How quantitative risk analysis strengthens your case
4. How other companies have capitalized on integrated, DDoS solutions
You Are the Guardian of Your Network

Before you consider how you might engage your senior team in a discussion on why an advanced approach to DDoS is essential and why it matters to them, it’s important to understand why it matters to you personally. Here are some key reasons, network operations and security leaders are willing to vigorously champion these solutions:

You Get Personal Time Back by Relying on Intelligently Automated Systems

Perhaps you’ve experienced the time, labor and pain associated with fighting DDoS attacks in an inefficient way. In the absence of an intelligently automated, integrated solution that allows you to reduce the complexity associated with DDoS protection, you are destined to devote significant resources in unproductive ways.

By reducing complexity and increasing automation, you eliminate an extraordinary number of otherwise manual tasks. You no longer spend days and hours fighting or mitigating the damage of an attack. You don’t want to get called in at 2 am or pulled away from your kid’s soccer game to deal with the problem. Now you can leverage intelligent automation to massively reduce the personal investment of time required.

You Scale Up Your Efforts to Increase Productivity and Revenue

When your DDoS solution is automated and integrated, you can scale your operations – bringing new levels of productivity to your efforts and maybe even support the production of new revenue streams. That enables you to grow your business.

Service providers are constantly seeking new ways to grow and set themselves apart in a crowded field. Even as the commoditization of Internet access and voice systems takes hold, managed DDoS protection services enables you to bring your organization new value-added service. Relying on Arbor, you can scale those services.

You Elevate Your Stature and Reputation in the Eyes of Key Stakeholders

By deepening your relevance to the organization, you elevate your reputation within it. What if you had the ability to present your decisive actions in a compelling way? Now you can say, “We stopped a 40 gigabyte DDoS attack that was under way for two days. Here’s the proof. Here’s a report that demonstrates we maintained the availability of our services. It saved us an estimated $2 million.”

By demonstrating your command of how the solution aligns with the business strategy and risk reduction, you get the attention of senior leaders. Using the FAIR framework – factor analysis of information risk – to make your case, you can credibly drive it home. (See “How to Reduce and Analyze the Risk of DDoS Attacks”) This framework allows you to convert qualitative risk into quantitative impact. With assistance from Arbor specialists, you can show how you are enabling the execution of key business initiatives while reducing risk exposure and the associated costs.

The organization relies heavily on you – though it may not always recognize your heroic acts in its defense. Unbeknownst to your fellow stakeholders, you are constantly thwarting attacks. Now, you can highlight the business impact of your work through guidance reporting to senior leaders.

You Are the Guardian of Your Network

SECURITY
What Senior Leaders Need to Hear From You

What's in it for them? That's the question leaders like you must contemplate before engaging senior leaders on the case for an advanced DDoS protection solution. Just recognize: They have no time for technical jargon. They trust you. They are relying on you. But they still need to hear – in language that resonates with them – why this investment is a necessary one. Here are some of the key points for you to present:

Problem
Modern DDoS attacks represent an asymmetric threat to the enterprise. It’s never been easier to launch a DDoS attack and new threat actors have emerged as the barriers to entry have dramatically fallen. It might cost as little as five dollars for the tools and exploits required to launch an attack. But the cost to the enterprise can run into the hundreds of thousands of dollars for these attacks – perhaps more in certain circumstances.

The modern DDoS attack is multi-vector and complex. We can no longer rely upon the existing solution to this problem which involves a great many inefficient, yet “heroic,” acts to defend the enterprise's network infrastructure.

Existing firewalls and/or Intrusion Detection devices cannot stop all DDoS attacks – in fact they can make matters worse as there are specific types of DDoS attacks designed to take them down.

Solely relying upon the company’s Internet service provider (or Managed Security Service Provider) to stop all types of DDoS attacks in their cloud-based scrubbing centers does not offer comprehensive protection. The ISP/MSSP will be needed to stop large DDoS attack that exceed the enterprise’s internet bandwidth. But the ISP/MSSP will struggle to detect and mitigate “low and slow” application layer attacks that are designed to escape cloud-based detection; for these types of attacks an on-premise DDoS attack protection solution is required.

These trends and patterns raise enormous financial and reputational risks for the enterprise. In recent years, attacks have escalated and the number of companies experiencing severe network downtime problems has risen. One recent attack took down a large ISP known as Dyn – and took down customers such as Netflix, CNN and Amazon Web Services as well. The problem took 11 hours to fully resolve.
Solution
A fully integrated and intelligently automated DDoS attack protection solution – one that can severely reduce the risk associated with DDoS attacks.

Payoffs
The risk associated with DDoS attacks carries significant quantitative and financial implications. That’s why it’s vital to take action to reduce exposure. With an advanced, intelligently automated DDoS attack protection solution, you can:

Reduce Costs Associated With Lost Productivity and Revenue
When networks are down, the company’s ability to operate is compromised. Employees without network availability are unable to produce. Customers may be unable to interact or transact or employ our services. What if the network or a key application is down for an hour? What if it’s down for several hours? What are the costs and consequences for their enterprise?

Reduce Costs to Mitigate Attacks
Every time a DDoS attack is successfully perpetrated, costs compound in relation to in-house and outsourced mitigation procedures. Considerable resources – people, time, and money – are deployed to undo the damage done by the attack while trying to ensure it was not merely a diversionary strike with a greater motive.

Reduce Costs Associated With Network Investments
By maximizing utilization and eliminating “junk on the network,” you can reduce hardware costs and related expenses.

Reduce Costs Associated Damaged Brand and Reputation
Just consider the reputational costs experienced in recent years by companies like Equifax and Target when hackers penetrated the network. The public relations disaster not only tanked stocks, it undermined the customer’s trust in the brand – with massive financial implications.

Reduce Opportunity Costs
It’s critical to recognize that you can reduce opportunity costs by ensuring the company’s business and digital transformation strategies can be fully executed. Without DDoS attack protection, they are at risk.
Presenting the Arbor Solution

When presenting the Arbor solution, you’ll want to focus on a few key points:

Arbor provides an integrated, intelligently automated, on-prem and in-cloud solution that will immediately detect and respond to a DDoS attack – ensuring you minimize and mitigate its impact.

At the same time, you’ll rely on Arbor’s ATLAS – a unique threat analysis research infrastructure – and Arbor’s deeply experienced Security and Engineering Response Team (ASERT), world-class security researchers and analysts who are focused on assessing global threats and providing actionable intelligence to protect your business.

The Solution Is Intelligently Automated, Customizable, and Future-Ready

[Diagram showing the Arbor solution in action]

Figure 1: Arbor’s Intelligent Automation in Action.
Intelligently Automated

The Arbor solution is an intelligently integrated combination of on-premise and in-cloud DDoS attack protection that’s continuously backed by global threat intelligence.

- On premise, the Arbor APS product is an always on product that can automatically detect and stop all types of DDoS attacks.
- In the cloud, Arbor Cloud is a fully managed DDoS attack protection service offering 7 Tbps of mitigation capacity via 17 worldwide scrubbing centers.
- Via Cloud Signaling, the Arbor APS continuously sends customized, local attack policy information to the Arbor Cloud. In the event of a large attack, the attack traffic will automatically be routed to an appropriate Arbor Cloud scrubbing center. In which case, preconfigured attack countermeasures, including previously sent APS local attack policies, will automatically stop the DDoS attack within minutes.
- Post attack, a comprehensive set of reports are provided which detail all attack activity.
- All of these products and services are continuously armed with the global threat intelligence offered by ATLAS and ASERT.

This industry-leading, intelligently automated solution is designed to provide the most comprehensive protection from the modern day DDoS attack.

Customizable

Arbor has the industry’s broadest portfolio of DDoS attack protection products and services that enable organizations of any size to customize a solution to meet their technical and financial requirements of today – and the future. As the threat of DDoS and your network environment evolves, you can customize an Arbor DDoS protection solution to fit your needs.

Future Ready

Arbor has Advanced DDoS attack protection solutions designed for the networks and threats of today and tomorrow. As your network environment, human resources and the threat of DDoS attacks evolve, you can trust Arbor to customize an intelligently automated DDoS attack protection solution that fits your technical and financial needs – helping you to address the continuum of risk.

As a company that’s defending 1,200 customers – service providers and enterprise networks – in 107 countries, Arbor is a pervasive force in the world of network security.
Top 5 Tips for Promoting a DDoS Solution Internally

1. Clarify Management’s Goals and Objectives
   Understand the collective and personal objectives that are motivating key decision makers. That helps prepare you to make a case that addresses their felt needs.

2. Build a Concise Case that Locks onto the Demonstrable Risks and Potential Consequences of Standing Still
   With just three key pain points in mind, you can identify what’s unsafe and unsustainable about the status quo. By exploring the implications of inaction, you can create motivation – even a sense of urgency – that sets the stage for a consensus-driven decision.

3. Discuss, Don’t Pitch
   Your fellow stakeholders value you as an advisor and specialist, not a pitchman or persuader. By asking questions that clarify where other’s stand and what concerns them, you build trust and confidence. You are then well positioned to present a powerful new approach. Then, you could make the transition, by asking something like, “If we had a way to dramatically reduce risks associated with DDoS attacks while maximizing network uptime and availability, would you be interested in learning more?”

4. Look for Anecdotes, Cases, and Industry Data that Bolster Your Case
   Seek insights, cases and examples that are relevant to your industry and circumstances. You want to demonstrate that your proposed DDoS solution has produced results for your peers in companies you respect.

5. Be Prepared to Take Action
   Ensure you have a plan, support and resources to back you up if your team decides to proceed. You want to ensure you have next steps, timeframes, and required resources lined up to ensure your team’s decision and rollout are well executed.
Let Arbor Help You Make the Case

The potential for DDoS attacks has increased dramatically in size, frequency and complexity. It’s critical now you have an advanced DDoS attack protection solution that is matched to your circumstance. You know the “resistance strength” of the solution you put in years ago is no longer ahead of the “threat capability” of a modern-day attack.

With Arbor as your partner, you can develop a quantifiable business case. You can go beyond reducing risk exposure to clarifying the cost of that exposure and the returns associated with its reduction. You’ll know how much your organization must invest in protection to reduce the risk and ultimate loss. You can compare the cost of added control strength (i.e., different Arbor solutions) to risk reduction benefit. You’ll use the simple formula of:

\[
\text{Return on Investment (ROI)} = \frac{\text{Reduction in Risk} - \text{Cost of Arbor Protection}}{\text{Cost of Arbor Protection}}
\]
Example of Quantitative Risk Analysis

<table>
<thead>
<tr>
<th>RISK COMPARISONS (MOST LIKELY)</th>
<th>RESISTANCE STRENGTH</th>
<th>LOSS EVENTS</th>
<th>LOSS: PRODUCTIVITY</th>
<th>LOSS: RESPONSE</th>
<th>LOSS: REPUTATION</th>
<th>TOTAL LOSS EXPOSURE</th>
<th>LOSS REDUCTION (FROM AS-IS)</th>
<th>% REDUCTION</th>
<th>ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td>As-Is: Firewall Only</td>
<td>10%</td>
<td>8</td>
<td>$648,000</td>
<td>$14,000</td>
<td>$38,000</td>
<td>$700,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To-Be #1a: Arbor APS</td>
<td>60%</td>
<td>4</td>
<td>$382,000</td>
<td>$8,000</td>
<td>$34,000</td>
<td>$424,000</td>
<td>$276,000</td>
<td>39%</td>
<td>503%</td>
</tr>
<tr>
<td>To-Be #1b: Arbor Cloud</td>
<td>40%</td>
<td>5</td>
<td>$431,000</td>
<td>$5,000</td>
<td>$27,000</td>
<td>$463,000</td>
<td>$237,000</td>
<td>34%</td>
<td>88%</td>
</tr>
<tr>
<td>To-Be #1c: Arbor APS + Arbor Cloud</td>
<td>90%</td>
<td>1</td>
<td>$212,000</td>
<td>$439</td>
<td>$14,000</td>
<td>$226,439</td>
<td>£473,561</td>
<td>68%</td>
<td>146%</td>
</tr>
</tbody>
</table>

You’ll be able to compare “as is” and “to be” scenarios in your effort to clarify the value of reducing risk exposure by different levels to achieve different ROI outcomes. You’ll be able to make the case in business and financial terms to your fellow stakeholders.

Figure 2: Risk analysis and Return on Investment (ROI) of Arbor DDoS attack protection.

For more details of this analysis download the “How to Reduce and Analyze the Risk of DDoS Attacks" paper.
Success Stories You Can Share

Here are two success stories that vividly illustrate how other companies have capitalized on the integrated, layered and fully managed solutions provider Arbor. By incorporating stories like these into your discussions with stakeholders, you provide context for understanding the impact and value of these solutions.

A Large Multi-National Retailer Thwarts DDoS Attacks

This Fortune 500 company manufactures products and provides engineering services for a wide range of industrial, commercial, and consumer markets. It has over 115,000 employees and 220 manufacturing locations worldwide.

It was challenged when its customers and partners experienced the impact of application-layer DDoS attacks on its web site. Recognizing that ISPs couldn’t offer the comprehensive protection that was required, the company sought a solution that could be rolled out quickly.

Ultimately, it implemented Arbor’s full portfolio of DDoS protection products and services. The Result? The fully integrated, fully managed, intelligently automated combination of in-cloud and on-premises solution provided comprehensive protection from modern-day DDoS attacks with extremely limited demands on its understaffed IT security team. To optimize the solution, the customer chose to outsource management of the entire solution to Arbor’s Security Operations Center which provides 24x7 coverage.

A Major Investment Banking Firm Protects Data Centers

This Wall Street investment banking firm manages trillions in assets and provides an array of investment and trading services through 30 offices worldwide. The success of the business depends on reliable and secure online infrastructure.

Like other financial institutions, it had increasingly become the target of coordinated, multi-stage attack campaigns and were well aware of the threat posed by DDoS attacks.

Recognizing the magnitude of the threat, network security and operations executives took action – seeking increased DDoS and attack protection for their Internet-facing data centers. They sought more rapid and flexible countermeasures than a cloud-based service provider could offer.

Given the growing complexity of their infrastructure and the sheer volume of network traffic, automation was vital. They did not want to add staff to identify threats. And they needed an approach that was easy to use and could be rapidly implemented.

The executives ultimately landed on Arbor as a firm that could provide always-on, in-line protection from network and application-layer attacks as well as other advanced threats. They obtained the insight, analysis and real-time control they needed to better protect data center operations. They particularly liked solution’s ‘force-multiplier’ effect in relation to existing staff. Providing an easy to use interface to configurable threat alerts and intelligently automated countermeasures.

With the investment bank’s reputation at stake every time its network and applications were attacked, it chose an advanced solution provider with a solid reputation of its own. That is the key reason the network executives were guided by their peers to Arbor in the first place: Its deep experience and impressive performance in the financial sector.
WHAT’S NEXT?
COLLABORATING WITH YOU

You are the advocate for the Arbor solutions you champion. You need to be clear and confident when you get behind a solution – and a solution provider. You want to ensure you are presenting your case as effectively as you possibly can when you are engaging your fellow stakeholders.

But you don’t have to engage in this effort alone. Rely on Arbor to support you in the development of this case and its presentation to your team. Reach out to your account representative and ask how Arbor can support you and collaborate with you to achieve a successful outcome in the eyes of your executive leaders and fellow team members.

LEARN MORE
For more information please contact your Arbor account team.