The New Business Imperative for DDoS Protection

ARBOR NETWORKS

About Arbor Networks

Arbor Networks Inc., the cyber security division of NETSCOUT, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context—so customers can solve problems faster and reduce the risk to their business.

To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

The modern enterprise is dependent upon connectivity at every level. Every business initiative, whether driven by sales, marketing, manufacturing, finance, R&D or HR, is dependent upon reliable network availability and continuity. Disrupting that continuity is what Distributed Denial of Service (DDoS) attacks are all about.

As an IT manager or security professional, you know that getting executive decision-makers to fully appreciate the material dangers posed by DDoS and prioritize strong DDoS protection can be challenging. In fact, sponsoring strong DDoS protection must be an enterprise-wide commitment—not just an IT problem. Unfortunately it often takes a significant negative event or headline to get attention. Even if you have an advocate in the C-suite, it can be difficult to clearly communicate to all stakeholders the potential business impact and generate a real sense of urgency for prioritizing DDoS defense.

This white paper will walk you through four steps essential to building a business case for better DDoS protection—one that's compelling to your business as a whole.

- **STEP 1:** Communicate clearly to business managers in the language that will help them understand the changing odds and nature of DDoS attacks.
- **STEP 2:** Illustrate the business implications of a target-rich environment in the modern enterprise.
- **STEP 3:** Present more comprehensive ways of evaluating the true value of effective DDoS protection.
- **STEP 4:** Describe the fundamental strengths and weaknesses of current countermeasures.

It is only a matter of time before you will be faced with a significant DDoS event. Protecting the enterprise from such disruptions is increasingly fundamental not only to business continuity, but to strategic success factors like faster innovation and increasing productivity. Enhancing your DDoS security posture requires building awareness and fostering collaboration across business functions.

Arbor Networks' *Worldwide Infrastructure Security Report (WISR)* 2014 found:

50%

Nearly half of respondents saw DDoS attacks during the survey period. And just over half rank DDoS as their number one concern for the coming year.

400 Gbps

The peak attack size this year— 400 Gbps—represents 4,900 percent growth over the 10-years of the Security Report.

42%

Forty-two percent reported attack durations of over 6 hours—some as long as 4 weeks.

STEP 1

Helping Your Business Understand the Changing Odds

DDoS attacks are not old news; they are in fact growing in frequency, size, the extent of targeted organizations and, critically, in sophistication. The natural question within a targeted enterprise is "why me"? The range of attacker motivations have always varied from criminal, financial gain to political agendas to hacktivist annoyance. But for building an effective protection strategy, the reality is motivation doesn't matter. What does matter is the lower "barriers to entry" for those having any motivation at all.

Virtually anyone with an Internet connection can initiate DDoS attacks. It no longer takes an expert, or even basic coding experience. There are a growing number of Do-It-Yourself (DIY) kits available for free online, or for a small fee you can engage a DDoS service (effectively "guns for hire")—all you need to provide is a target IP address. Couple this with ever-increasing public servers (many of which are not following the best security practices) and the conditions are optimal for widespread, significant DDoS attacks. Remember, attackers, like businesses, look at the return on their investments in time and money; the ROI for a DDoS attack is very positive. And there is little downside to the attacker, little risk of being caught or paying any penalty.

The New Normal

Any business is a potential target of DDoS. You don't have to be a governmental body, a retail organization generating ecommerce revenue or a financial services giant to attract unwanted attention. Anyone with Internet-facing applications is susceptible. The increasing reliance on cloud-based services hosted in public clouds, or even passing through service providers with a range of other customers using such services, only increases your exposure. All the potential business benefits of a cloud-based service—productivity, cost advantages, flexibility—go away when users cannot access services when they need them.

DDoS also continues to evolve and now generally consists of three categories: volumetric, state-exhaustion, and application layer attacks.

- **Volumetric Attacks** attempt to consume the bandwidth either within the target network or service provider, a/or between the target network or service provider and the rest of the Internet. Their goal is to cause congestion.
- **TCP State-Exhaustion Attacks** attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls, IPS and the application servers themselves.
- **Application-Layer Attacks** target some aspect of an application or service at Layer 7. They are the most sophisticated and stealthy attacks because they can be very effective with as few as one attacking machine generating a low rate of traffic.

Today's DDoS attacks are frequently multi-vector, combining multiple attack techniques concurrently, aimed at the same target, to increase the complexity of mitigation and the attacker's chance of success.

42%

of respondents reported seeing multi-vector DDoS attacks in the past year, and what is just as worrisome is the thirty-six percent who did not know.

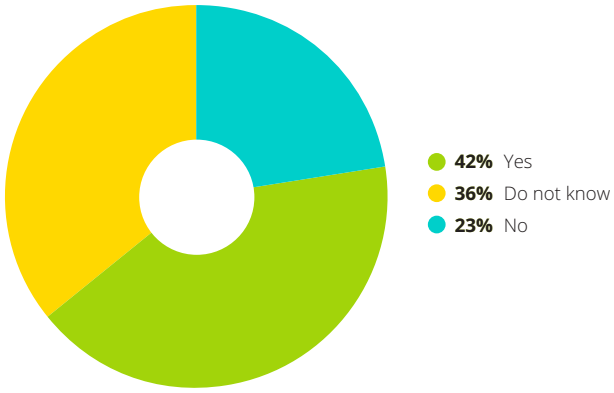
Source: *"Worldwide Infrastructure Security Report, Volume X,"* Arbor Networks, 2015

Multi-vector attack campaigns highlight another new reality of the modern enterprise. Many business applications leverage multiple servers on the back end to provide connected services. While it may appear like a single interface to the end user, back end sub-systems are handling tasks such as web services, database processing, authentication, communications (mail, chat, SMS, etc.) and complete financial transactions, to name a few. Even if you are successful protecting the infrastructure delivering traffic to and from your server, application layer DDoS attacks can bring down the server itself. And a single server failure can have a cascading effect on back end systems with unexpected consequences for multiple business applications.

In retail, a POS system that cannot communicate with the inventory database, or current promotional pricing, could severely impact in-store sales. A customer service self-service application that does not have access to email or chat may not only limit effectiveness but generate negative customer experiences. On-site field resources can be crippled from performing critical service if they cannot access current account information or download the correct patch. A CFO can be delayed closing the books, or preparing a quarterly earnings report, if unable to access current revenue and sales information.

The list of interconnected, web-based applications where performance and availability are critical to different business functions goes on and on. The immediate operational costs to remediate might fall upon IT, but it pays to think far more broadly about the pervasive business costs of DDoS events.

Multi-Vector Attacks



Source: *"Worldwide Infrastructure Security Report, Volume X,"* Arbor Networks, 2015

29%

The proportion of respondents seeing attacks targeting cloud-based services has grown significantly, from 14 percent in 2012,19 percent in 2013 and 29 percent in 2014.

Read the report ›

Source: *"Worldwide Infrastructure Security Report, Volume X,"* Arbor Networks, 2015

STEP 2

Business Implications of a Target Rich, Enterprise Environment

An expanding, target rich environment is coming at the same time as the enterprise is looking to realize cost and productivity benefits from more mobile devices, trends like BYOD, and new business paradigms (SDN, VDI, IaaS, SaaS, etc.) rooted in cloud-based services. These strategies challenge traditional security controls based on visibility into and manageability of endpoints, applications and networks. Not only are there more attack surfaces, but it is harder to monitor what is happening and build in adequate security.

A recent worldwide McKinsey survey[1] of 200 senior business executives and industry experts found that:

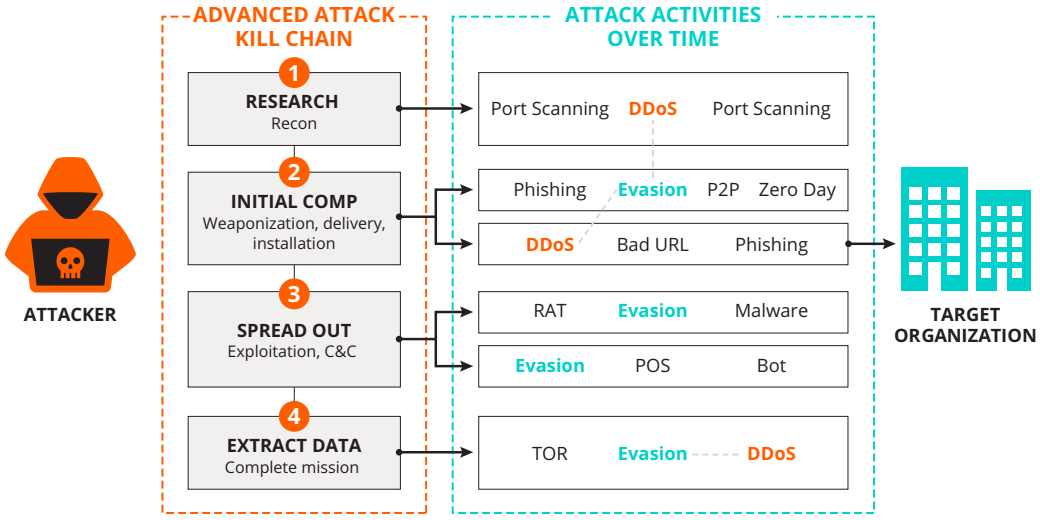
"Some 70 percent of the respondents said that security concerns had delayed the adoption of public cloud computing by a year or more, and 40 percent said such concerns delayed enterprise-mobility capabilities by a year or more. Cybersecurity controls are having a significant impact on frontline productivity, too. About 90 percent of the respondents overall said that controls had at least a moderate impact on it. Half of the high-tech executives cited existing controls as 'a major pain point' that limited the ability of employees to collaborate."

There has always been a dynamic tension between providing adequate security and adopting new technologies and services to make the enterprise more efficient, increase productivity and grow the business. Individual decisions come down to a measure of what is an "acceptable" risk? What is new regarding DDoS is the degree to which the entire range of DDoS risk factors have changed, the rapidity of change, and the increased scope of enterprise business functions that are now or will be at risk.

Yet another wrinkle is that, for whatever reasons, DDoS tends to be considered separately from advanced cyber-attacks. This is an increasingly dangerous assumption. Fifteen years of research into global Internet traffic conducted by the Arbor Security Engineering and Response Team (ASERT) has determined DDoS botnets are in fact closely related to advanced threat malware, RATs, and other components. DDoS attacks can and have been used in several stages of advanced attack campaigns.

Arbor's insight can be shared via ATLAS®, a unique collaborative effort with 330+ network operators across the globe sharing 120 Tbps of traffic information that informs numerous business decisions.

Attack Kill Chain



DDoS is used by advanced attackers during reconnaissance, to assess your general level of security and preparedness and help them make the decision whether to target your organization. (In this case a DDoS event is a potential indicator of advanced attack—and how well you respond can be a powerful defensive tool.) DDoS is also used as part of delivery and weaponization, when dropping malware, to help avoid detection (think of all those alerts you are trying to prioritize). And finally, DDoS is used to divert attention and cover tracks during data extraction, and even after the fact, when it is used to fill forensic product logs, making the search for planted malware much more challenging.

In the end, you need to raise awareness across your organization that the real business costs of DDoS disruption extend far beyond IT, and build consensus that the risks to the smooth operation of different departments and roles has increased such that DDoS protection needs to be a priority.

For a recent presentation on the connection between DDoS and advanced attacks, as well as overview of the changing nature of DDoS, go to: *Why DDoS Makes for Risky Business* and *What You Can Do About It: 5 Misconceptions about DDoS Attacks.*

View the presentation ›

STEP 3

The True Value of Effective DDoS Protection

What's the real business value of protecting your business availability and continuity against the threat of DDoS? The most straight-forward scenario is found in any business with revenue coming directly from e-commerce or financial transactions; top of mind for these organizations is the hourly revenue that is protected from DDoS disruptions to service availability.

But an effective solution against today's DDoS has value beyond protecting immediate revenue streams. Protection against DDoS means you also avoid incremental costs in specific functional areas due to dissatisfied or lost customers, slowed product launch, disruptions to inventory and supply chain, decreased productivity—and, looking forward, opportunity costs.

Even within IT, a more effective DDoS solution means IT can avoid incremental costs of paying existing staff overtime, or reconfiguring components, adding capacity, or hiring an outside firm for mitigation and forensics. But IT also suffers opportunity costs in terms of diverting resources from current, perhaps revenue generating activities, or more strategic initiatives such as rolling out new productivity applications or building out new datacenters.

This pattern is repeated as we look across the enterprise. More effective protection against application and network availability helps ensure different departments continue to fulfill immediate tasks uninterrupted—and can pursue initiatives that push the business forward. Here are a few examples.

Sales

The inability to close affects current business—and disruption in pursuing leads slows down near-term opportunities. In retail, a POS system that cannot communicate with the inventory database, or the current discount data, could severely impact in-store sales—especially if part of an on-going promotion.

Customer Service

Staff may be prevented from performing on-site service if they cannot access current account information. Unavailability of services such as email or chat may delay responding to unhappy customer today, which may mean losing them to a competitor tomorrow. And how many more help desk calls will be received, or lost?

Marketing

Disrupted promotional campaigns that are tied to major events (think World Cup Soccer, Olympics, and March Madness) may not only fail to meet revenue objectives and recoup sunk costs but leave the brand with a "black eye."

Corporate Communications

Highly visible DDoS attacks require extra cycles and funding for PR campaigns to repair damage to brand.

Manufacturing

An inaccessible back end web property can lead to operational costs in overtime and shipping, and if communication flow with suppliers is disrupted, product delivery time may be delayed.

Legal

The fall-out from DDoS attacks may include legal costs for defense, diversion of legal staff from more strategic initiatives (like M&A), settlements, and penalties in terms of regulatory fines when valuable data is exfiltrated under the cover of DDoS.

Finance

Timing of the attack could have short term impact—such as inability to close the quarter, or delay certain filings. But after the attack, senior management a/or the Board will expect detailed reports of the financial impact of the attack.

It is important to note that targets at risk within an enterprise are influenced by a number of factors that vary according to the nature of a specific business: organizations are different in their type of infrastructure, organizational configuration, business workflows and dependencies, etc. Risk factors differ, for example, according to whether an organization is public or private, or has deployed a cloud-based vs. an on premise ERP system. It's not just that an ecommerce enterprise will have different areas of risk than a healthcare organization; it means one ecommerce or healthcare company will have different risk factors than another.

"With trillions of dollars in play and cyberresiliency affecting a growing range of business issues—business continuity, customer privacy, and the pace of innovation, to name just a few—it's clear that current operating models for combatting attacks aren't up to the task. Often, they are compliance driven and technology centric. Instead, they must be grounded in collaboration across business functions."

The best estimate of the true value of an effective DDoS protection solution means enlisting the help of knowledgeable LOB managers. Working with functional business units not only helps provide a better picture of the risks and true value of a solution, but increases enterprise-wide awareness and build consensus to take action. Each discussion should begin with a specific scenario: What would happen to the LOB if it were under attack for an hour in terms of the types of revenue loss, incremental and opportunity costs.

STEP 4

Fundamental Strengths and Weakness of Current Countermeasures

The increasing frequency of attacks and ease with which virtually anyone can initiate DDoS means the days of "this would never happen to me" are over. A recent study showed that fewer than half of the enterprises, government and educational institutions surveyed feel reasonably or well-prepared for a security incident, and 15 percent indicate they have no plans or resources in place.[2] More common—and perhaps more dangerous—is the "checkbox" mentality: the belief that current on premise perimeter devices such as web-application firewalls (WAFs), load-balancers and intrusion protection systems (IPS) are sufficient defense from DDoS.

In fact, firewalls, load-balancers and IPS were not designed to protect availability, and may inadvertently abet DDoS attacks. Setting aside the potential challenges represented by the staggering volumes generated by new reflection techniques, these devices are vulnerable to TCP state exhaustion attacks. Firewalls, load-balancers and IPS can become an Achilles heel in the infrastructure. In the study previously referenced, nearly half of the participants indicated that they have seen attacks targeting infrastructure such as routers, load balancers, firewalls and overall network bandwidth.[3]

On premise solutions alone are simply no longer enough for defense against today's DDoS. By the same token, counting solely on your ISP or MSSP is a risky strategy. Upstream protection is appropriate for volumetric attacks (providing that the lines of communication about attacks are fast and procedures clear), but a cloud-based defense is not optimal for the low and slow application-centric attacks. To effectively detect and mitigate this type of attack in real time, it is necessary to deploy an on premise, in-line or other packet-based component to your DDoS defense.

Because modern day DDoS attacks use a dynamic combination of volumetric, TCP state exhaustion and application-layer attack vectors, industry best practices recommend that organizations take a layered approach to DDoS protection.

That is, the best place to stop large flooding attacks is upstream in a service provider's cloud before they overwhelm local internet connectivity or on premise DDoS protection systems. And the best place to stop stealthy application-layer attacks is on the customer premises, closer to where key applications or services reside.

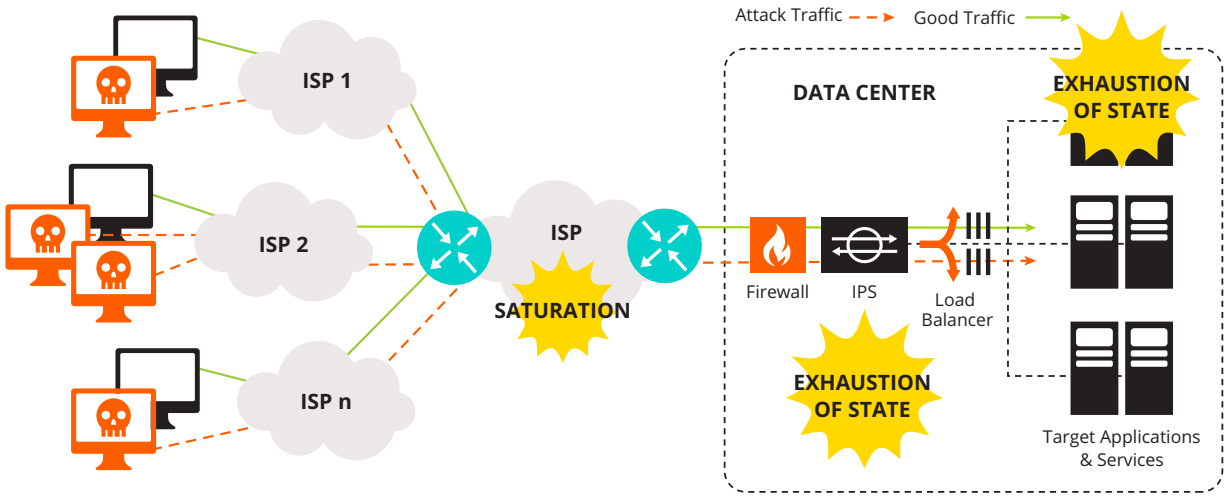
To be most effective you must have rapid, intelligent communication between these two layers; this includes automated signaling where practicable and pre-established, well-defined response procedures.

Best Practicies: Layered DDoS Defense

- Maximize visibility into, and control over, your traffic—whether it's coming from the cloud or on premise, so that you lower the risk of a DDoS attack ever effectively penetrating the data center.
- Implement a streamlined mitigation process—an integrated solution connecting the on premise and the cloud visibility, detection, and mitigation processes.
- Minimize downtimes associated with initiation of third party mitigation efforts.

Read Arbor Network's The Business Case for Best Practices DDoS Defense ›

DDoS Attacks Are A Multi-Vector, Diverse Threat



Of course best practices include other operational and organizational components. Clearly a more mature overall security posture will improve your response to the newer DDoS attacks. Components of a more "mature" DDoS security posture include:

- **Staffing & Accountability:** Coordination or a hybrid of network and security operations teams who have the expertise and capabilities to respond quickly, for example are able to coordinate across organizational boundaries to mitigate a DDoS attack.
- **Operational Readiness:** Have a virtual team identified, and empower that team with DDoS detection capabilities, training, documented processes, and conduct mock simulated attacks on a regular basis to refine process as needed.
- **Risk Focus:** Conduct a continual risk assessment of threats faced by your organization (including DDoS) by likelihood of the threat occurring and the impact of each threat.
- **Awareness of DDoS as an Advanced Threat:** Leverage products to protect and have visibility into advanced threats (including security analytics and security intelligence feeds). Maintain all advanced threat operations even in the face of DDoS attacks.

And let's not forget the increasing value of timely threat intelligence. A more mature security posture includes a higher level of shared threat intelligence:

"Organisations need to look at the benefits that can come from sharing threat intelligence; sometimes organisations are too concerned about 'helping the competition'—but the key thing to remember is that sharing intelligence is usually a reciprocal arrangement, and the right information could prevent a hugely embarrassing and costly breach for all parties. Government initiatives such as CiSP, which is part of CERT-UK, help facilitate sharing by providing a safe and secure environment between organisations."[4]

The sharing of threat intelligence is becoming more critical for effective DDoS defense. Just as with advanced attacks, the more you know of specific and current threat activity the faster and more confidently you can identify a truly threatening DDoS event. But there is a trick to making the best use of intelligence:

"Given the influx of threats coming at you from every possible angle, entry-point and vector, what is really needed to stay ahead of attackers? Context. That context can help you gauge risk, prioritize your security operations team's time, and move on to the next threat (among many) at hand."[5]

Context, like what other organizations have been attacked, what methods were used, where are these attacks sourced from, what were the motivations behind these attacks, what was their attribution, was it multi-vector, etc. is just as relevant for defense against DDoS as against advanced attacks.

Looking Ahead

Communicating more clearly to business managers and senior executives the transformed threat represented by DDoS—what DDoS attacks mean in terms of their achieving their business goals—will help your organization as a whole appreciate the new business imperative for effective DDoS protection.

The new DDoS attack must be viewed more like an advanced attack campaign, of which it may very well be a component. You can better protect strategic initiatives across the enterprise with a defense in depth DDoS security posture that combines the advantages of cloud services and on premise protection. Best practices include leveraging timely threat intelligence to speed mitigation and minimize downtime.

The next step to moving forward is to examine the strengths and weaknesses of your current DDoS countermeasures and assess the overall maturity of your security posture.

Resources

[1] Bailey, Tucker et. al., Andrea Del Miglio, and Wolf Richter, "The Rising Strategic Risks of Cyberattacks," McKinsey Quarterly, May, 2014.

[2] "Worldwide Infrastructure Security Report, Volume X," Arbor Networks, 2015.

[3] "Worldwide Infrastructure Security Report, Volume X," Arbor Networks, 2015.

[4] Pudwell, Sam, "Interview: Arbor Networks Gives Us the Lowdown on DDoS Attacks," IT Pro Portal, August 23, 2015.

[5] Holden, Dan, "The Great Threat Intelligence Debate," CIO Review, 2015.

CORPORATE HEADQUARTERS
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

NORTH AMERICA SALES
Toll Free +1 855 773 9200

EUROPE
T +44 207 127 8147

ASIA PACIFIC
T +65 68096226

www.arbornetworks.com

WP/NEWBUSINESSIMP/EN/0915-LETTER