ARBOR NETWORKS

Issue 1

Modern DDoS Defense Toolkit: Best Practices, Advice from Arbor Networks and Gartner

Featuring research from
Gartner

From Gartner Files:

Master These Eight Steps to Control the Damage From DDoS Attacks

The DDoS landscape has changed considerably since 2012, leaving many organizations unprepared to deal with today's distributed denial of service threats. Establishing key processes in advance will help to mitigate the impact of a DDoS attack.

Key Challenges

- Many organizations lack the technical expertise and the operational experience to respond effectively to DDoS attacks.
- Business leaders and IT leaders often fail to communicate well during the critical early stages of a DDoS attack.
- DDoS toolkits have made it possible for individuals with little technical knowledge to launch attacks.

Recommendations

CIOs and IT leaders:

- Create a "playbook" based on the practices outlined in this research. Review that playbook at least twice a year.
- Test your DDoS mitigation capabilities quarterly.
- Establish ground rules for communications and decision making between business leaders and IT leaders throughout the duration of a DDoS attack.

Introduction

Many organizations lack the expertise and skills to mitigate distributed denial of service (DDoS) attacks effectively and efficiently. The

emergence of DDoS attack toolkits, such as Dirt Jumper and Pandora, has made it easier for "hactivists" and other individuals with minimal technical expertise to launch DDoS attacks. At the other end of the spectrum, 2012 and 2013 saw new advances in DDoS attacks (see Note 1) that challenged even the most experienced DDoS mitigation experts.

The typical IT organization is caught off guard when it experiences its first round of DDoS attacks, regardless of whether the attack is sophisticated or unsophisticated. The next round of DDoS attacks may come months or years later, making it difficult for the security team to build the skills and refine the processes necessary for defending against these attacks. However, by implementing several best practices, organizations can be better prepared to control the damage from DDoS attacks.

"Enterprise Strategies for Mitigating Denial-of-Service Attacks" outlines three approaches, and highlights their trade-offs, for defending against DDoS attacks:

- Scrubbing Center — The role of the scrubbing center is to "scrub" all traffic and send only clean (valid) traffic to their destined addresses. Redirecting traffic from your organization to the scrubbing center presents important technical and operational challenges, as noted in our first best practice.

- Content Delivery Network (CDN) — The distributed nature of a CDN, in which content is hosted on multiple (potentially thousands) servers, mitigates the risk of a successful DDoS attack against websites. With this strategy, DDoS mitigation is "always on," which eliminates the need to temporarily redirect traffic.

- On-premises Equipment — Scrubbing centers and CDNs are cloud-based strategies. By implementing DDoS mitigation equipment on-premises (in enterprise data centers), organizations can defend against application-based DDoS attacks and smaller volumetric attacks (provided the attack has not already consumed all available bandwidth).

These strategies are not mutually exclusive and are increasingly deployed in combinations to defend against advanced DDoS attacks. With the exception of the first best practice, all of the best practices highlighted here apply to all three DDoS mitigation approaches.

Analysis

Appoint a Small Team of IT Leaders to Make the Decision to Redirect Traffic to a Scrubbing Center During the Early Stages of a DDoS Attack

A common problem among enterprises facing their first DDoS attack is that they take too long to make the traffic redirection decision ("pushing the button") to redirect traffic to the closest scrubbing center. (Note: This does not apply to the CDN-only approach.) These enterprises typically convene a large meeting (10 or more people) of IT managers and business executives to gain consensus on the decision to redirect traffic. This consensus-building approach wastes valuable time during a DDoS attack. The best practice is to empower two to three IT leaders with the authority to quickly make traffic redirection decisions. Gartner clients that have adopted this approach report that it enables them to begin DDoS mitigation within several minutes of an attack, instead of the several hours' delay that is often the result of the consensus-building approach.

Deciding who has the authority to push the button is an important consideration. The best candidates are individuals that have the technical expertise to assess the severity of the attack, as well as the business experience to understand the impact and risks to your organization (see Note 2). Typically, these individuals are at the vice president level.

Scrubbing center providers also offer automated traffic redirection services, thereby bypassing the need for an enterprise to give approval before redirecting traffic. However, because of the inherent risk in traffic redirection, most enterprises prefer to retain control over the decision to push the button.

Develop a Process With Your ISPs to Quickly Block Traffic From Offending IP Addresses

Some volumetric attacks can be easily identified as originating from a specific range of Internet Protocol (IP) addresses. Companies can mitigate these attacks quickly and effectively when their ISPs block traffic from a range of IP addresses that are known to be bad. The list of IP addresses can come from a government agency (for example, the FBI in the U.S.), an industry information-sharing association, or from the enterprise's own troubleshooting efforts.

Enterprises and their ISPs should arrange a process that enables the ISP to quickly block traffic that originates from known bad IP addresses. Enterprises should be able to make proactive blocking requests (in anticipation of DDoS attacks) and reactive blocking requests (while they are under attack) on a 24/7 basis.

Audit the Content on Your Website and Remove Large Files That Are Not Necessary

A common and relatively unsophisticated DDoS attack results when attackers identify a large file on a website and send multiple requests simultaneously (via a botnet) to download this file, thereby resulting in bandwidth saturation. Website administrators should audit the content on their websites to determine if any large files (for example, annual reports to shareholders) can be removed or hosted via a third-party service.

Know the Business Value of Services That May Need to Be Temporarily Disabled

You may need to temporarily disable some functions on your website to recover from an application-based DDoS attack. The goal of an application-based attack is to overtax the CPU and/or memory of a Web server or application server to degrade the performance of the website. Common techniques include using search boxes (for example, store-locator boxes on retail sites, or automated teller machine [ATM] finders on banking sites) to enter malicious commands that execute "search loops" that exhaust server resources. Organizations that anticipate being the target of application-based attacks should instruct their Web developers to prepare a "Plan B" of their websites (without search boxes, or without key applications) to be launched in the event of an attack. IT executives should know the business value of key Web applications and services (for example, online bill payment or other applications linked to revenue) that may need to be temporarily disabled. Knowledge of lost revenue (for example, $X lost per hour of downtime) will help IT executives communicate with business executives during crisis mode.

Establish an Internal Communications Plan

Establish a communications plan that outlines "who speaks to whom" during a DDoS attack. These steps should be part of your incident response and/or disaster recovery plans, and should address:

- Who needs to be informed, and in what order? For example, which business executives need to be alerted about the attack?
- How will they be informed (phone call, SMS text, or email)?
- Who is responsible for internal communications (who does the informing)?
- Where and how can key executives be reached? (Maintain a list of personal mobile phone numbers so key executives can be reached at all times.)

Establish an External Communications Plan

Controlling the message and delivering accurate information are important points in any external communications plan. Decide in advance how your organization will update its customers, business partners and others (including the news media). As noted previously, these steps should be part of any existing incident response and/or disaster recovery plans. Consider the following:

- Use social media (for example, Facebook and Twitter) to deliver updates
- Appoint a spokesperson to address requests from the news media

Perform Quarterly Testing of DDoS Mitigation Capabilities

Whichever approach or combination of approaches (for example, scrubbing center, CDN, or on-premises equipment) that your organization has implemented for DDoS mitigation, it should be tested on a quarterly basis.

- Scrubbing center customers should ensure that pre-established tunnels are functional and are capable of redirecting traffic.
- CDN customers should review and test Web application firewall rule sets.
- Enterprises that have implemented on-premises DDoS mitigation equipment should review the commands and rule sets used to combat DDoS attacks.

The evolving mix of attack vectors demands that mitigation capabilities be tested regularly for effectiveness. (DDoS mitigation providers report seeing an increase in DNS amplification and Network Time Protocol [NTP] amplification attacks since 2013.)

Large enterprises with mature DDoS response teams should trigger simulated attacks with live traffic on an annual basis. DDoS response teams can simulate their own attacks or rely on services from penetration testing companies or specialty services (see Note 3). The one-time charge for a typical test ranges from $8,000 to $20,000

Establish a "Playbook" of the Best Practices Outlined in This Research

The processes outlined in this research should be documented in a playbook and reviewed semiannually to reflect changes to your website and your organization. Modifying the content and/or the applications on a website can alter the risk of attack and your response mechanisms. Organizational changes in IT leadership and business leadership can alter your communications plans. Ensure that your

DDoS mitigation playbook remains up to date at all times. The playbook should be organized as follows:

- Preattack (well in advance) — Example: Establish communications policies
- During an attack — Example: Traffic redirection policies
- Postattack — Example: Postmortem analysis of technical and operational responses

Note 1
Recent Attacks

In August 2012, some of the largest U.S. banks were hit by sophisticated DDoS attacks. The Al Qassam Cyber Fighters, an Iran-based organization, took credit for the attacks. One of the hallmarks of these attacks was that they originated from a botnet of servers, as opposed to the typical botnet of PCs. Because servers have more bandwidth and processing power available to them than does a typical PC, the attackers were able to quickly ramp up the intensity of the attacks. The attackers created the botnet of servers by exploiting vulnerabilities in the popular WordPress blogging application.

DNS amplification attacks became commonplace in 2013, including a very large DNS amplification attack that was launched against email security provider Spamhaus (reports of the attack ranged from 140 Gbps to 300 Gbps). Attacks using NTP have become commonplace in 2014. NTP has an even larger amplification effect (for sending "junk" traffic) than DNS.

Note 2
Risks of Redirecting Traffic to Scrubbing Centers

The scrubbing center model has been widely adopted, but it is not without risk. A common technique for traffic redirection is to establish Generic Routing Encapsulation (GRE) tunnels between the customer's site and the scrubbing center. The Border Gateway Protocol (BGP) is used to redirect traffic through the tunnel to the scrubbing center. Challenges with this approach include traffic loss (due to routing problems), performance issues (related to packet fragmentation — a byproduct of GRE tunnels) and instability (when GRE links become saturated). Testing traffic redirection on a quarterly basis (and after major network changes) will detect problems and give you time to take corrective action.

Note 3
Examples of Tools and Services for DDoS Mitigation Testing

Services that specialize in DDoS mitigation testing:

- RedWolf Security
- NCC Group

Ixia offers products to enable DDoS mitigation testing

Free DDoS attack tools that can be used to simulate attacks include:

- LOIC (Low Orbit Ion Canon)
- XOIC
- DDOSIM — Layer 7 DDOS Simulator

Source: Gartner RAS Core Research Note G00261182, Lawrence Orans, 21 April 2014

Quantifying the Risk of a DDoS Attack

Let's begin with a simple question that more than likely has a very complicated answer. How much would it cost you as an organization if your systems went down due to a distributed denial of service (DDoS) attack? If you are completely shut off from your customers for 30 minutes, an hour, a day, or even a week, what is the overall impact to your business? If you know the answer to this already, you are either extremely prepared or are one of the thousands of risk managers who lose sleep over this every night—or both.

DDoS attacks on data center operations and services have become both highly sophisticated yet easy to perpetrate. As a result, enterprises, hosting providers and cloud service providers are experiencing DDoS attacks on their data centers more frequently and with more severe business consequences than ever before. As its name implies, DDoS attacks are an attack on service availability. The goal is to prevent the data center from functioning—whether that is transacting ecommerce; delivering email, voice, or DNS services; providing Web access; or offering other business-critical services.

Because the goal of an attacker is to create maximum disruption, attacks are more likely to occur at the worst possible times for your business. For example, online retailers are especially vulnerable during the holiday season and on "cyber Monday" in particular. I'm sure everyone reading this can imagine their own personal worst case scenarios as well. If you are in the financial services sector it could be at the opening of the market during earnings season or if you are in the technology sector, it could be on the day of a major product launch and so forth.

The point being that no matter what market you are in, your business stands to suffer a significant financial loss if you are the victim of a DDoS attack. How big of an impact depends largely on how well prepared you are to deal with these attacks. Let's explore some of the key considerations that will help IT security managers set budget priorities by determining the risk and business consequences of DDoS attacks on their operations.

Operations: What is the number of IT personnel that will be tied up addressing the attack and what is the hourly cost of that?

Help Desk: If systems are shut down, how many more help desk calls will you receive and what is the cost per call?

Recovery: How much manual work will be required to re-enter transactions?

Lost Worker Output: What is the level of employee output lost to downtime and the costs associated with that?

Lost Business: How much business will you lose for every hour you are down?

Lost Customers: How many existing customers will defect to the competi-tion? What is the lifetime value of these customers?

Penalties: How much will it cost you in terms of service level agreement (SLA) credits or other penalties?

Lost Future Business: How much will your ability to attract new customers be affected? What is the full value of that lost business?

Brand and Reputation Damage: What is the cost to the company in terms of brand value?

So after evaluating these key considerations, what would the financial impact of a DDoS attack be on your organization?

As guidance, Ponemon surveyed 16 different industry segments with 41 business managers reporting on the costs that their operations had incurred due to unplanned data center outages, both full and partial. Business losses as a percentage of total cost ranged from 63 to 99 percent with a mean of 86 percent. The cost of data center downtime is a function of data center size and business type. Hourly cost of downtime per 1000 square feet ranged from $8,500 to $201,000, with a mean of $46,000. The large fluctuation in downtime is mainly due to business type. Companies reliant upon data centers to conduct business such as financial services companies, incur the greatest losses.

Unfortunately, the number of DDoS attacks is trending upwards and repeated attacks causing outages greater than 12 hours are not uncommon. Therefore security managers should take into account the risk and financial impact of annual outage time of 24 hours or more when planning for security budgets. As the key considerations outlined in this article have highlighted, for most enterprises, replacing highly uncertain and risky cost outcomes with the predictable, lower cost of DDoS threat mitigation and attack protection is sound practice from a security perspective as well as a financial perspective.

Source: Arbor Networks

Why Have DDoS Attacks Become so Complicated?

For nearly a decade, DDoS was a basic flood attack that simply tried to overwhelm a connection with traffic with the goal of taking that web property offline. DDoS was a basic attack against availability.

When Arbor Networks first began working with leading web properties fighting DDoS attacks in 2000, "flood" attacks were in the 400Mbps range. Today, they can exceed 300Gbps. The sheer size of the attacks is not all that has changed.

Beginning in 2010, and driven in no small part by groups like Anonymous and the rise of Hacktivism, we've seen a renaissance in DDoS attacks that has led to innovation in the areas of tools, targets and techniques. Today, DDoS is a complex attack against availability.

What's changed?

The barrier to entry has been obliterated by new tools that enable anyone with an Internet connection and a grievance to launch an attack. This is a true game changer in terms of the threat landscape and what businesses should consider themselves a potential target of attack. It used to be certain verticals would be likely targets for DDoS, finance, gaming and e-commerce at the top of the list. Today, any business, for any reason, any real or perceived offense or affiliation, can become a target.

Beyond the democratization of DDoS are the advancements in attack techniques and targets. DDoS today is in fact a series of attacks that target not just connection bandwidth, but multiple devices that make up your existing security infrastructure, such as Firewall/IPS devices, as well wide variety of applications that the business relies on, like HTTP, HTTPS, VoIP, DNS and SMTP.

The hottest trend in DDoS today is the multi-vector attack, combining flood, application and state exhaustion attacks against infrastructure devices all in a single, sustained attack. These attacks are popular because they difficult to defend against and often highly effective.

The new realities of DDoS today require a new approach to DDoS defenses.

We believe that the best defensive posture against the modern DDoS threat is a layered approach that combines on-premise and cloud based protections. Only then will your organization be protected against the full spectrum of DDoS attacks.

Source: Arbor Networks

Arbor Cloud DDoS Protection for Enterprises

DDoS has become the primary threat to the availability of enterprise networks. DDoS was once a basic high volume attack that flooded the pipes of its targets. The modern DDoS threat is a complex series of attacks that target not just connection bandwidth, but multiple devices that make up existing security infrastructure, such as Firewall/IPS devices.

Attackers also target a wide variety of applications that the business relies on, like HTTP, HTTPS, VoIP, DNS and SMTP. These infrastructure and application-layer attacks are low volume and they are designed to evade traditional perimeter defenses, and often target them.

Arbor Cloud is DDoS best-practices defense in action—a unique, integrated combination of on-premise and cloud-based mitigation for protection from the full spectrum of modern DDoS attacks. Powered by the world's most widely deployed DDoS protection technology,

Arbor Cloud provides the most comprehensive DDoS protection available today. Arbor's technology, products and ATLAS research infrastructure power Arbor Cloud, supported by a 24x7 Security Operations Center staffed by Arbor DDoS and security experts. Arbor Cloud brings the availability of your network, services and applications back under your control.

Pravail® Availability Protection System

The on-premise Pravail® Availability Protection System is designed to detect and stop DDoS attacks immediately, without upfront configuration or any user interaction. It delivers DDoS attack identification and mitigation capabilities that can be deployed rapidly, even during an attack.

Pravail empowers you to define parameters and keep track of what's "normal" in the terms of processing capacity, memory usage or buffers. Pravail helps detect and alert early on anomalies created by such application-layer attacks as malformed HTTP, LOIC, slowloris, HTTP GET/post floods and DNS cache poisoning.

What makes Arbor's Pravail such an important product for the enterprise is that it not only helps protect against application-layer threats, it provides additional investment protection to existing security infrastructure. For example, firewalls and IPS are designed for important security problems other than DDoS. They were built to stop unauthorized access to critical resources, enforce corporate security policies and prevent data loss. These all remain critical security problems. What's changed is that availability itself is now under assault and it requires a solution designed specifically for today's complex DDoS problem.

Key Benefits of Pravail On-Premise Protection

- Easy to install, configure and use
- Gain real-time visibility into availability threats, attacks and blocked hosts. Automated threat updates.
- Advanced DDoS countermeasures that have proven effective in the world's largest and most complex network environments.
- A single Pravail appliance can mitigate attacks up to 10Gbps, leaving the enterprise in control of most attacks.
- In-depth, real-time attack reports that are easy to understand along with forensics detailing blocked hosts, origin countries of attacks and historic trends.

Arbor Cloud: Delivering Global Threat Protection

The Arbor Peakflow® platform powers many of the world's leading cloud-based DDoS managed security services. Arbor Cloud leverages this technology for threat detection and mitigation. Arbor Cloud provides additional protections for the enterprise, including botnets and malware, via the ATLAS® Intelligence Feed.

The ATLAS Intelligence Feed delivers deep DDoS signatures in real-time to keep networks protected against hundreds of botnet-fueled DDoS attack toolsets and their variants. This unique feed includes geo-location data and automates the identification of attacks against infrastructure and services from known botnets while ensuring that updates for new threats are automatically delivered without software upgrades. The ATLAS Intelligence Feed enables Arbor Cloud customers to directly benefit from the depth and breadth of Arbor's research team.

The Arbor Security Engineering & Response Team (ASERT) is a recognized industry expert when it comes to Internet threat analysis. ASERT's primary focus is on botnets, malware and DDoS, which account for a majority of the attacks on the Internet today. ASERT has unique visibility into botnets, malware and DDoS because of its ATLAS infrastructure, which combines a darknet sensor network with traffic data from more than 300 service provider customers around the world. This enormous dataset, measuring 90Tbps, enables ASERT to develop a unique, globally-scoped view of malicious traffic traversing backbone networks that form the Internet's core. This insight is critical, as threats are constantly changing and updating to thwart detection.

Cloud Signaling: How it works

Cloud Signaling is an efficient and integrated way of bridging the enterprise data center to the service provider cloud. The real power of an integrated solution combining on-premise with cloud-based protection is the communication between the two. When an enterprise or data center operator discovers that he is under a service-disrupting DDoS attack, they can choose to mitigate the attack in the cloud through the Cloud Signaling system, simply by clicking on a drop down menu and triggering an alert to the Cloud. The Cloud Signal can also be pre-set to occur at certain levels, say when the connection is at 85% capacity. The proactive approach enables the business to stay in control and maintain expertise in command of the event. When an attack begins to saturate connection bandwidth, Arbor's on-premise Pravail appliance sends a signal to Arbor's cloud-based Peakflow equipment, and mitigation begins. A volumetric DDoS attack congesting the upstream links diminishes, or disappears altogether from the data center's access links, and service availability is protected.

Conclusion

No vendor has been studying, and mitigating, DDoS attacks longer than Arbor Networks.

Arbor Cloud combines our knowledge and experience in everything from global threat detection right down to the technology, people and processes required to mitigate distributed, multi-layer, multi-vector attacks. Integrated on-premise and cloud-based protection is a must for organizations who have to maintain availability of networks, services and applications. Arbor Cloud reduces the time to mitigation and increases the effectiveness of the response against DDoS threats, thus saving major operational expenses while helping to preserve the brand and reputation. Arbor Cloud represents the most comprehensive DDoS protection solution available today.

Source: Arbor Networks

Video

Arbor Cloud Illustrated

Multi-layered DDoS Protection – From the enterprise network to the Cloud.

Arbor Cloud is powered by the world's leading experts in DDoS, together with the most widely deployed DDoS protection technology. Whether your enterprise needs to maximize the availability of its network, services and applications—or you're a service provider seeking to launch or expand your managed DDoS protection service—Arbor offers a solution for you.

When Preparation Meets Opportunity: A Q&A on Best Practices with Arbor's Director of Cloud Security Services

Kate Stafford is Arbor Networks' Director of Cloud Security Services where she is responsible for the Arbor Cloud Security Operations Center, and all mitigation activities for Arbor Cloud customers. Kate brings 15 years of security leadership experience to her role at the company. Previous experience includes security operations, incident response, security assessment, data protection, and compliance.

Can you describe how planning and preparation help speed time to mitigation?

It's impossible to ensure rapid mitigation without the right game plan. Each enterprise is unique with its own network infrastructure, business imperatives, security policies and traffic visibility. Each enterprise also has unique mitigation capabilities, depending upon its on-premise tools and expertise. The right preparation requires asking the right questions: How much volume can we handle before it becomes an issue? What are the most likely threat scenarios? At what thresholds should we engage additional mitigation support?

To help you answer these questions and develop the plan that's right for your organization, we work with you to make sure you understand your specific tolerance thresholds in light of your unique requirements and capabilities. We help you define your tolerance thresholds both in traffic volume and in time spent dealing with threats such as a low and slow attack. It is when these thresholds are passed that you escalate the issue and redirect the traffic.

We've also learned the importance of defining roles and responsibilities during the planning process to ensure rapid mitigation. We will help you clearly identify those roles and responsibilities—making sure the right people are in a position to make the necessary calls. With the right thresholds, roles, and responsibilities defined in advance, you can respond faster with the added capacity you need to shut down the attack. And of course, you need to know who your business owners and stakeholders are before you are in the midst of a serious DDoS event. What's more, you need to recognize that the universe of stakeholders has greatly expanded due to the growth of e-commerce, online customer service, extended partnerships and supply chains—not to mention internal networks that now go far beyond email and support financial operations, VoIP, audio/video collaboration, scheduling and much more.

It's critical to know all these stakeholders to better understand the impact of your mitigation decisions, and to recognize whether all your systems are acting as they should when you get back online. Making sure that the mitigation process doesn't impact key functions of the organization is almost like acceptance testing. It calls for fine tuning processes in order to let the "right" traffic through. Understanding the needs of your stakeholders upfront will help you make this determination.

In your experience, what are the characteristics of a successful mitigation?

Here's one recent example. This was a customer heavily reliant on Internet traffic and very familiar with DNS protocols. We had worked with it previously to make sure there was a clear DDoS mitigation playbook, and this preparation paid off. The organization came under attack via a DNS attack. It was able to quickly anticipate the attack passing its thresholds and had the right people on the bridge to make the call. It also knew how to coordinate internal stakeholders and what to expect back from us. Throughout the attack mitigation process, it had the right people on the phone. We were able to identify what DNS traffic was part of the attack and what DNS traffic the enterprise relied on for its daily operations.

What are the best practices for incident response (IR) that all enterprises should be following today?

They all revolve around creating a clear incident response playbook. Do not wait until you are under duress! Create scenarios where you actually have to reroute traffic. Identify your stakeholders now, and those individuals who have the authority to make changes. Define your process for communication and escalation. Once you've created your IR playbook, update and test it regularly. Your organization is not static. People and roles change. Infrastructure changes. Vendors change. And remember, with today's extended supply chains and business channels, it's critical to ask your vendors and partners to be part of your IR playbook. And like many things, practice is key: practice, practice, practice. You do not want to be testing your mitigation capabilities when you are under attack.

Source: Arbor Networks

The Arbor Advantage

We See Things Others Can't

Unmatched traffic intelligence, across the Internet, and your network

Arbor has leveraged our unique customer footprint and experience working with the world's most demanding network operators to develop a more enduring solution for the threats of today and tomorrow. Arbor does this not by focusing on specific threats or points in the network but on networks themselves.

ATLAS is a collaborative project with more than 300+ ISP customers who have agreed to share anonymous traffic data totaling an amazing 90Tbps. From this unique vantage point, Arbor is ideally positioned to deliver intelligence about DDoS, malware and botnets that threaten Internet infrastructure and network availability.

Arbor customers enjoy a considerable competitive advantage by giving them both a micro view of their own network, through our suite of products, combined with a macro view of global Internet traffic, through ATLAS. This is a powerful combination of network security intelligence that is unrivaled today.

Proven Technology, Highly Scalable Solutions

Arbor products can scale to meet the needs of any size network operator. Our technology is proven and tested in the world's largest, most distributed network environments. Our products are backed by ASERT, our security research team that is respected around the world. We're fanatical about customer support, especially when you need it most, during an attack.

Cable & Wireless

"The ATLAS Initiative is a world first – but more importantly, it gives us the most comprehensive threat intelligence on the market today and provides a nice cherry on top of our managed security services offering."

Harvard University Berkman Center for Internet & Society's Ethan Zuckerman

"Arbor Networks' research is utterly indispensable for anyone who wants to understand the network security landscape, how it is evolving and what the implications may be."

Hostopia

"Within weeks, our selection was validated when Arbor's Threat Management System helped block a major denial of service attack, eliminating the attack traffic while keeping legitimate traffic moving to and from our customers."

Rostelecom

"Due to the collaboration we have with Arbor, we were able to deliver continuous services to all of our customers during the Sochi Olympic Games."

Savvis

"The Peakflow platform continues to evolve and deliver real value for Savvis' global network."

Wired.com

"Arbor Networks knows more about the Internet's workings than possibly anyone outside the National Security Agency. Their monitoring equipment sits in nearly all Tier 1 internet providers — and if you want data on what the Internet looks like and what the top threats are, they've got it through their ATLAS service."

Yahoo!

"The global deployment of Arbor products within the service provider community and the relationships they have leveraged to develop innovative and unique solutions like ATLAS and ATF, were key factors in their favor. Peakflow SP not only provides network-wide visibility and protection against attacks, it provides the analysis and reporting we need to communicate with executive management about the threats facing our network."

Did you know? The Communications Security, Reliability and Interoperability Council (CSRIC) has adapted Arbor Networks DDoS incident response best practices as part of their *Remediation of Server Based DDoS Attacks* final report to the FCC?

Did you know? Arbor was named one of the 10 Brilliant DARPA Inventions?

Did you know? When the European Union was investigating how to protect Europe from large scale cyber-attacks, they called upon two companies, the world's largest security vendor, and Arbor Networks.

Did you know: ? U.S. Department of Homeland Security's Doug Maughan, Director, Cyber Security Division, praised Arbor Networks as the best example of DDOS protection?

Source: Arbor Networks

About Arbor Networks

About Arbor Networks Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor's advanced threat solutions deliver comprehensive 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," mak ing 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 help 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.