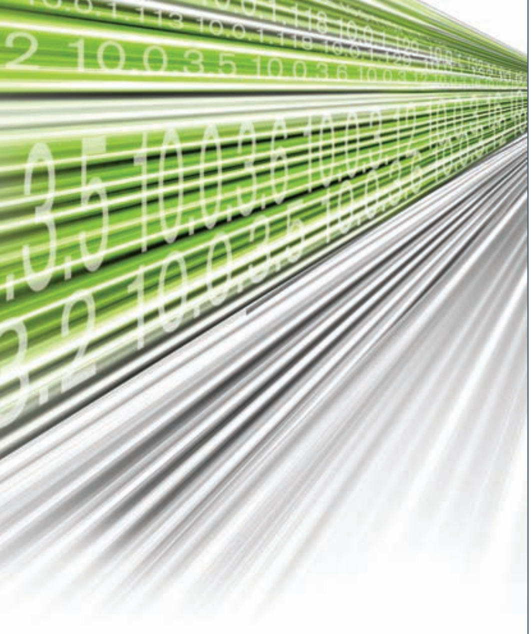

SOLUTION BRIEF

aixit GmbH Uses Arbor Peakflow® SP and TMS for Data Center Protection and Security Services

Customer

aixit GmbH

Industry

Internet Service Provider, Data Center Operator, Hosting Provider

The Challenge

Protect its data center infrastructure and customers from DDoS attacks using a solution that does not require in-line deployment.

The Solution

Rely on the Arbor Peakflow SP solution – consisting of Arbor Peakflow SP Collector Platforms (CP) and Arbor Peakflow SP Threat Management Systems (TMS) – deployed out-of-band for threat detection and surgical mitigation of DDoS attacks.

The Result

aixit now has the ability to detect and surgically mitigate threats using a solution that can be deployed out-of-band, thus eliminating a potential point of failure. In addition, aixit is generating new revenue via managed security services based on the Peakflow SP solution.

Founded in 1996, aixit GmbH was one of Germany's Internet pioneers. Today, aixit continues to be a leader in providing high-quality data center, hosting and Internet access services to customers across Germany and Europe. Its privately owned, trans-European fiber network, together with many peering and IP upstream relationships, enable aixit to cost-effectively deliver high-performance, fault-tolerant Internet access. In 2004, the company started offering hosting services and now has two large data centers located in Frankfurt and Offenbach, Germany. These highly redundant, state-of-the-art data centers enable aixit to deliver scalable and virtualized hosting services to over 250 customers ranging in size from individual consumers to large online gaming and broadcasting companies. As with all customers who outsource a portion of their IT services, aixit's customers rely heavily upon their data center operator and/or hosting provider for the security and availability of their hosted services. To meet these requirements, aixit uses the Arbor Peakflow® SP solution ("Peakflow SP") and Arbor Peakflow SP Threat Management System ("Peakflow SP TMS") to protect its data center infrastructure from distributed denial of service (DDoS) attacks. aixit also uses these Arbor solutions as a platform to deliver managed DDoS protection services to its hosted customers.

The Need to Protect All Customers from DDoS Attacks

One of the main benefits of a semi-private or public data center service is its ability to enable customers to save on IT costs. This is accomplished by leveraging shared data center resources, such as circuits, routers, servers and IT personnel. However, this service also has its drawbacks—especially when it comes to DDoS attacks. A DDoS attack not only impacts the target customer, but it also impacts those customers who share the same data center resources as the attacked customer. Therefore, it's imperative that data center operators or hosting providers such as aixit detect and stop DDoS attacks before they impact one or more customers.

"The frequency of attacks depends upon the customer," explains Holger Grauer, CTO of aixit. "For some customers, it was one to two attacks per month, while others had one to two attacks per week. As a result, we had some customers (such as online gaming and broadcasting companies) asking for DDoS protection services, while others (such as individual consumers) didn't want the services because they weren't the targets."

But aixit knew that DDoS attacks impact all customers—making it imperative to put a solution in place to protect and maintain its entire data center infrastructure. aixit looked for a solution that would give it the flexibility to detect and stop DDoS attacks on a per customer basis. In addition, the solution could not be deployed in-line as this could potentially be another source of failure in its network. aixit chose the combination of Peakflow SP and Peakflow SP TMS to fulfill its needs. "When our customers' Internet-facing services are down, this not only impacts their ability to generate revenue, but also ours," says Grauer. "We're glad to have found a company like Arbor to help us solve this problem."

ARBOR®
NETWORKS

Out-of-Band, Surgical DDoS Attack Mitigation

aixit proudly boasts the quality and benefits of its exceptional customer service. Maintaining the integrity of its network, data center and IP-based services is critical to the success of its business. "We looked at different security companies and products, but there wasn't anything like Arbor's Peakflow SP TMS," explains Grauer. "One of the main reasons we chose the Peakflow SP and TMS solution was because of its ability to be used out-of-band and not be a potential source of failure in our network during a DDoS attack."

aixit uses the combination of Arbor Peakflow SP Collector Platforms (CP) and Peakflow SP TMS devices, which can be configured for either in-line or out-of-band deployment. The Peakflow SP CP devices gather IP flow data from their network's routers, analyze this information to provide pervasive network visibility, and detect network anomalies sometimes caused by DDoS attacks. Once a DDoS attack is detected both the legitimate and attack traffic are off-ramped using Border Gateway Protocol (BGP) routing to Peakflow SP TMS devices which then conduct surgical mitigation of only the attack traffic while allowing legitimate traffic to continue to flow. Providers such as aixit can optimize their threat management by choosing from multiple models of Peakflow SP TMS devices that allow them to conduct surgical mitigation of attack traffic from 1 Gbps to 40 Gbps. aixit uses the combination of TMS 2500 (2.5 Gbps) and TMS 3050 (5 Gbps) to protect dedicated customers and its overall data center from DDoS attacks.

> "When our customer's Internet-facing services are down, this not only impacts their ability to generate revenue, but also ours. We're glad to have found a company like Arbor to help us solve this problem."
>
> Holger Grauer
> CTO
> aixit GmbH

New Services Equate to Stronger Customer Relationships

As the competition increases and prices drop for services such as dedicated Internet access or hosting, service providers scramble to find new services that can generate additional revenue, increase profits and retain customers. aixit uses the Peakflow SP and TMS solution to not only protect its data center from DDoS attacks, but also simultaneously deliver additional DDoS protection services to its existing customers. "We have a managed DDoS protection service called 'Look & Protect' that is based upon the Arbor Peakflow SP and TMS products," explains Grauer. "Customers have a portal where they can look at their own network traffic and alerts." Furthermore, the customization features in the Arbor products allow aixit to easily offer multiple levels of its DDoS protection service (e.g., Bronze, Silver, Gold and Platinum). "Not only is this service an important tool for our customers, but we have found that managed services such as these strengthen the relationships we have with our customers—which in turn allow us to retain them and generate additional revenue."

The bottom line: The integrated Peakflow SP and TMS solution has enabled aixit to protect its data center from DDoS attacks using an out-of-band solution while generating new revenue by providing valuable managed security services to its customers.

Highlighted Products & Information

Arbor Peakflow SP
Arbor Peakflow SP Collector Platform (CP)
Arbor Peakflow SP Threat Management System (TMS)

About Arbor Networks

Arbor Networks is a leading provider of secure service control solutions for global business networks. Its customers include over 70 percent of the world's ISPs and many large enterprises. Arbor solutions deliver best-in-class network security and visibility, along with the power to improve profitability by deploying differentiated, revenue-generating services. By employing flow-based and deep packet inspection (DPI) technologies, Arbor solutions measure and protect the entire network—from the network core to the broadband edge. Arbor also maintains the world's first globally scoped threat analysis network—ATLAS—which uses technology embedded in the world's largest ISP networks to sense and report on comprehensive worldwide threat intelligence.

ARBOR® NETWORKS

Corporate Headquarters
6 Omni Way
Chelmsford, Massachusetts 01824
Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe
T +44 208 622 3108

Asia Pacific
T +65 6327 7152

www.arbornetworks.com