| SOLUTION BRIEF |

NETSCOUT and Arbor Networks: Reduce Time to Threat Identification

The security threat landscape has fundamentally changed. It is no longer advanced malware, which traditional defenses can miss, that represents the greatest risk to your organization. As individual bad actors give way to organized crime syndicates and state sponsored cyberterrorism, sophisticated, multi-stage attacks have become the main worry for network and security teams.

The majority of successful advanced threat attacks in the past two years never exploited a critical vulnerability, and many did not use malware to bypass the target's defenses. The attacks' effectiveness now lies in their ability to remain undetected; most organizations take months (!) to detect a breach. To counteract these threats, enterprises must dramatically reduce detection times.

NETSCOUT Packet Flow Switches and and Arbor Networks Advanced Threat Platform

NETSCOUT and Arbor Networks deliver a joint solution that allows security teams to surface and then to detect, investigate and prove threats within your network.

See attack campaigns in real-time across your entire network: Arbor's global threat intelligence coming from its service provider network will be cross referenced to an organization's internal traffic patterns to detect the most dangerous threats.

Search and surface anything within the network: unlike the current security forensics models, the solution provides complete visibility into all past and present network activity, at a fraction of the cost.

Prove threats on your network faster: real-time workflows and analytics empower and scale security teams to investigate threats 10 times faster than existing solutions.

The NETSCOUT packet flow switches enable you to easily and rapidly deploy, scale and optimize the Arbor Networks Spectrum™ environments where the need for enterprise-wide data access and visibility is essential. Arbor Spectrum gets a complete view of all activity on the network for real-time flow and packet analysis.

Packet flow switches create a logical separation between physical network and security capabilities via network aggregation, enabling the security teams to easily expand their threat protection as the traffic grows. The NETSCOUT vMesh™, a fabric-based architecture, allows the PFS devices in the network to communicate with each other, enabling a unified packet delivery strategy for service assurance and security across the entire network.

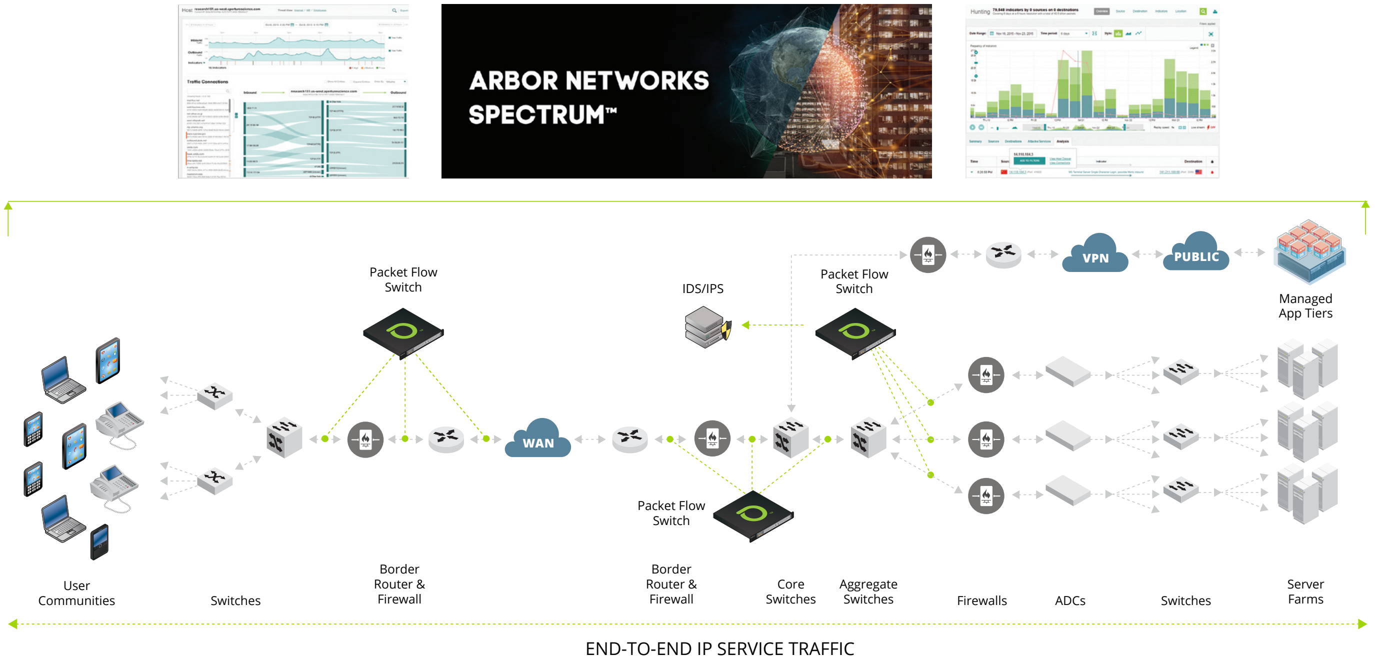

Diagram 1. See and search across the entire network — connecting awareness of global attacks with activity on the internal network.

SIMPLIFIED SECURITY

- Security service assurance
- Speed and media conversion
- Layer 2 to Layer 7 traffic grooming
- Security-in-series with security tool chaining
- Thresholds, alerts and auto triggers
- Fault tolerance for security systems and networks
- Test and deploy security systems without network disruption
- Actionable XML/API integration

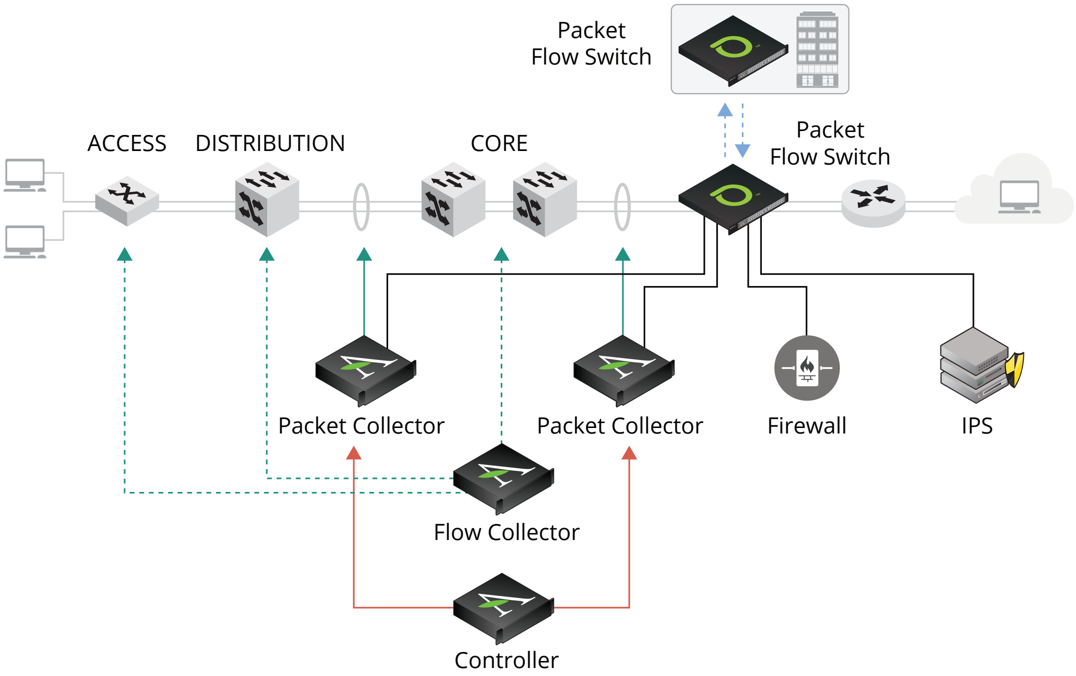

Diagram 2. NETSCOUT packet flow switches delivering to Arbor Networks packet collectors.

Unified and Pervasive Visibility

The vMesh architecture aggregates traffic from all data center locations within the enterprise to a central point where Arbor Spectrum can perform its discovery and forensic analysis. The packet flow switches deliver the entirety of the traffic to the Arbor Packet Collectors for real-time flow and packet analysis, giving the Spectrum platform a complete view of all activity on the network.

The NETSCOUT nGenius packet flow switches enable you to connect your inline active security infrastructure, in addition to one or more Arbor Spectrum appliances. The PFS tool chaining capability allows network security teams to aggregate the traffic and direct it to inline and passive security systems for filtering and inspection in a central location. This reduces not only the security team's workload but improves the organization's security posture.

This combination of packet flow switches, active inspection from third-party tools and Arbor Spectrum discovery and investigation provides a sophisticated infrastructure that offers unmatched visibility spanning the entire network. The combined Arbor Networks and NETSCOUT solution accelerates time to identify a threat and allows you to secure your digital assets, protecting your brand.

Summary

Together, Arbor Networks and NETSCOUT address the increasingly sophisticated and targeted network threats. The NETSCOUT nGenius packet flow switches optimize the efficiency of Arbor Spectrum by providing an unprecedented level of visibility that dramatically speeds threat discovery, investigation and response.

This joint solution delivers:

- End-to-end visibility for threat identification, investigation, and resolution
- Security service chaining to achieve a combined active and passive security posture
- More time spent in research and resolution and less time administering security infrastructure

About NETSCOUT nGenius Packet Flow Switches

NETSCOUT nGenius packet flow switches maximize the efficiency of security and network analysis infrastructure by logically separating the network layer from the tool layer. Backed by a unified packet plane, security systems can be physically anywhere and logically everywhere. Packet flow switches provide critical visibility to combinations of solutions like active inline network analysis and passive, out-of-band forensic appliances. With the NETSCOUT approach, security visibility capabilities are included at no additional cost.

About Arbor Networks

Arbor Networks, the 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 Networks Spectrum™ advanced threat platform empowers organizations to find and stop stealthy attack campaigns - in minutes not hours - with unique threat indicators uncovered in global Internet traffic integrated into intuitive, real-time workflows that surface attacker activity on the enterprise network. 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 risks to their business.

NETSCOUT.

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000