JOINT SOLUTION BRIEF

Improved Device Monitoring and Security across the enterprise

The Challenge

As the number of devices connecting to your network grows, so does your attack surface. IT and security teams must simultaneously reduce risk without disrupting business operations or innovation.

Integrated Solution

Cubro and Forescout help achieve this goal with 100% visibility via passive methods that ensure no dropped packets and without added latency.

Joint Solution Benefits

Cubro's packet aggregation technology, flow generation, and patented DPI engine integrate into Forescout's device discovery, classification, assessment, contextual insight, and policy enforcement capabilities and combine to equip organizations with the power to streamline risk reduction without impacting business operations.

Cubro and Forescout bring comprehensive visibility to the Enterprise of Things

Introduction

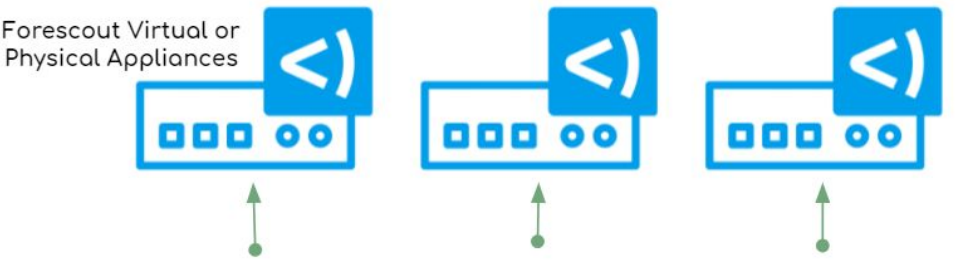
The number of devices being connected to the corporate network is growing at an exponential rate. In addition to traditional technology assets, the Internet of Things has enabled an entirely new class of devices that, historically, were never internet enabled and often these devices lack rigorous security controls. BYOD policies have introduced a multitude of personal devices to the workplace. The rapid move to employees working from home has bridged the divide between home networks and corporate networks faster than comprehensive security policies can be implemented, potentially exposing corporate infrastructure to a litany of IP connected gadgets in environments with little or no security oversight. Additionally, rogue or simply forgotten devices can remain derelict on the network creating opportunities for exploitation. The result is a rapidly expanding attack surface that requires comprehensive and constant oversight.

The Cubro and Forescout Joint Solution

Forescout is the leader in Enterprise of Things security and employs an innovative, agentless methodology to detect, identify, and classify network devices. By combining network traffic analysis with additional data sources (such as flow data) Forescout identifies network devices, and leveraging an internal dataset, classifies the device according to type, ownership, and use. Once the context and device type are understood, Forescout offers centralized controls for network access, segmentation and device compliance policies that define what the device is permitted to access and what its posture should be. Finally, the Forescout solution continually enforces these policies for a proactive risk mitigation and security stance. Fortune 1000 companies and government organizations trust Forescout to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

Cubro Network Visibility compliments Forescout's solution by offering a diverse portfolio of network visibility products that provide full network access and, in addition to raw network traffic, provide valuable data sources that Forescout can utilize in its identification and classification process. Visibility starts with Cubro's fully passive network TAPs. These provide fail-safe access to network traffic by providing an out-of-band copy of everything that crosses the wire, ensuring nothing is overlooked. The copied traffic is then fed from the TAPs to one or more of Cubro's Network Packet Brokers to ensure all tools and appliances have access to the traffic they need.

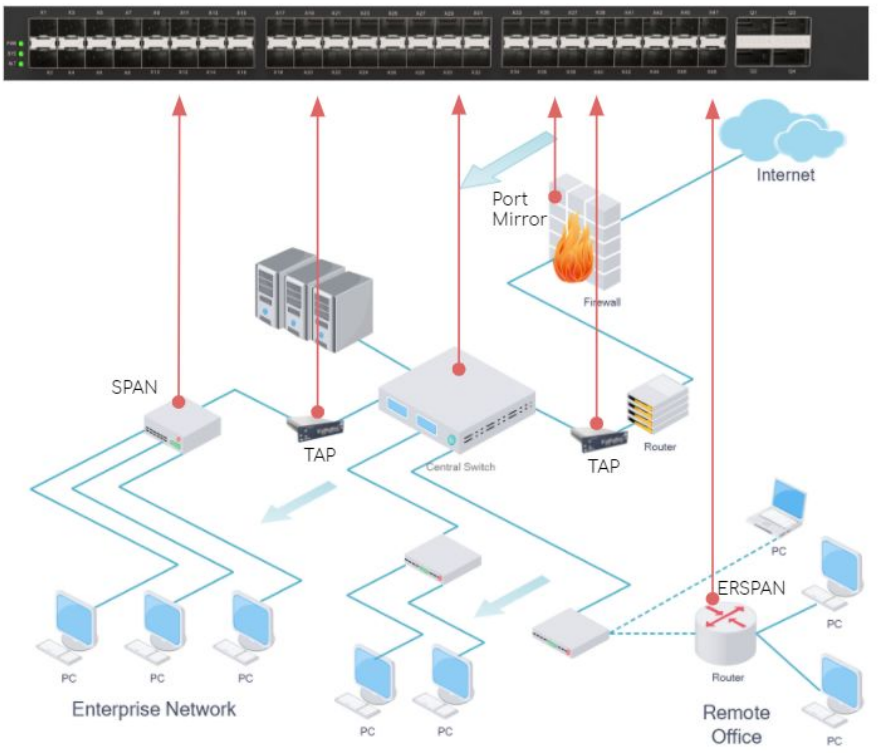
Cubro's diverse line of Packet Brokers provide a solution for all network types, sizes, and speeds, providing a scalable, cost-effective, and efficient solution for organizations of all types. Additionally, granular filtering, load-balancing, and traffic deduplication are just a few of the features that enable tools to handle high-bandwidth environments that would otherwise present issues. Cubro offers unique advanced features that further enhance the Forescout solution. With Cubro's Omnia line of Network Packet Brokers, DPI-enriched NetFlow records can be produced on the fly, providing valuable additional data sources for Forescout to utilize in identification and classification of devices. Omnia provides compliance enforcement as well with the ability to perform data-masking of sensitive information and/or PII, enabling Forescout to inspect traffic that would otherwise be off-limits due to regulatory requirements such as HIPAA.



Use Cases:

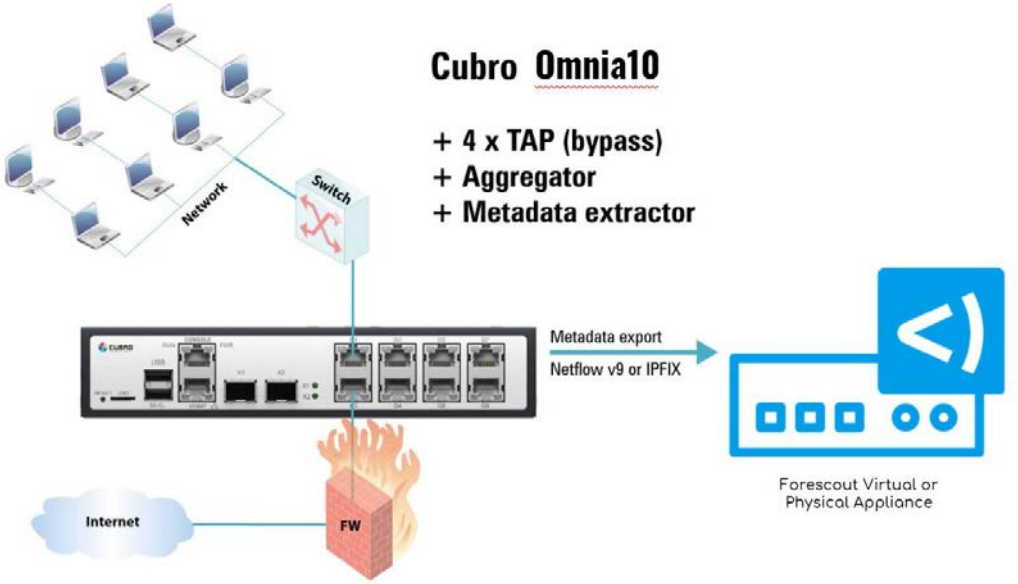
Example 1

Cubro TAPs passively copy traffic from multiple points in the network and feed the traffic to the Omnia120 Advanced Network Packet Broker. The Omnia120 performs aggregation, de-encapsulation, deduplication, and traffic filtering before load-balancing the traffic across multiple Forescout sensors enabling complete visibility into network traffic as well as access to high-bandwidth (multiple 100Gbps) links.



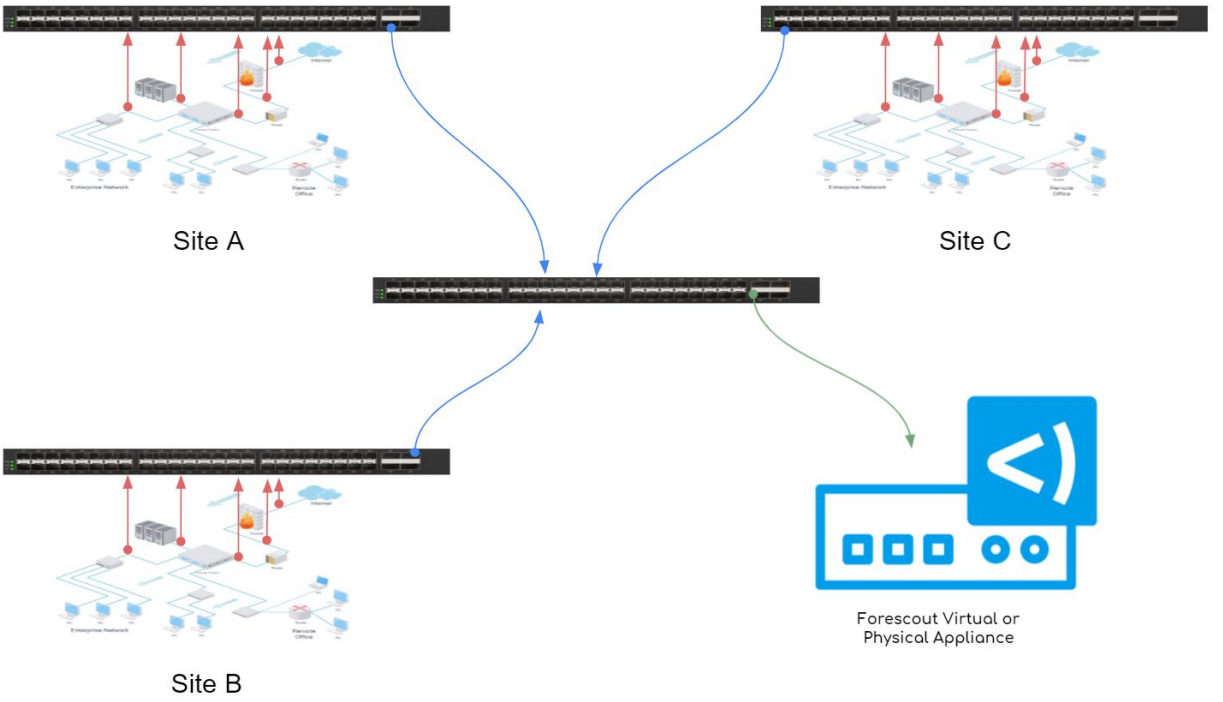
Example 2

Omnia10 passively taps network traffic, aggregates, and forwards a copy to Forescout's sensors. Additionally, the Omnia10 can perform network analytics, such as NetFlow and IPFIX, to provide Forescout with more data points for device identification and classification.



Example 3

Cubro TAPs and Network Packet Brokers are deployed at remote sites for comprehensive visibility and access to network traffic. The Network Packet Broker further encapsulates a copy of the aggregated traffic for backhaul to a centralized location where the tunnel is terminated on an Omnia120 and the remote traffic is forwarded to the Forescout solution.



For more information please visit www.cubro.com and www.forescout.com.

Cubro Network Visibility
EMEA USA APAC Japan
support@cubro.com