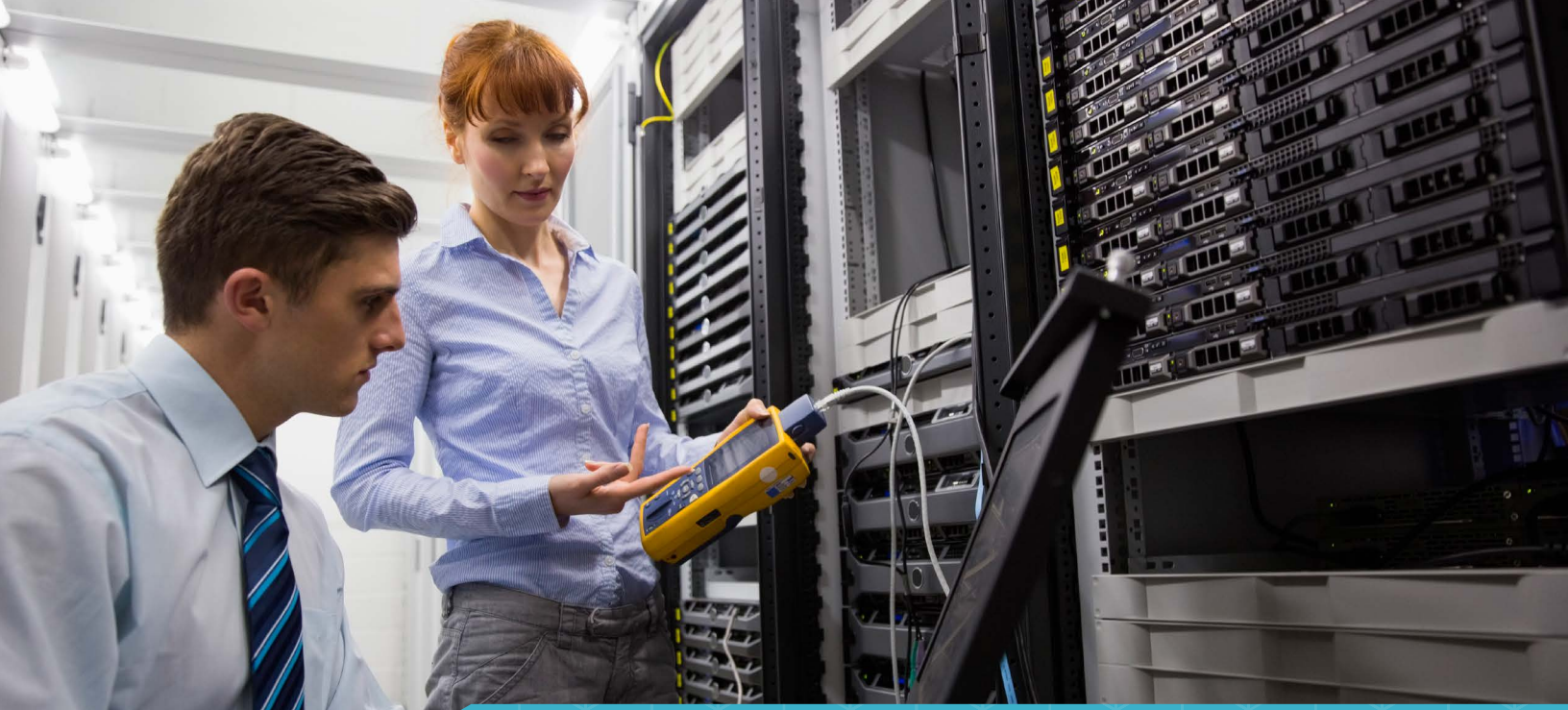


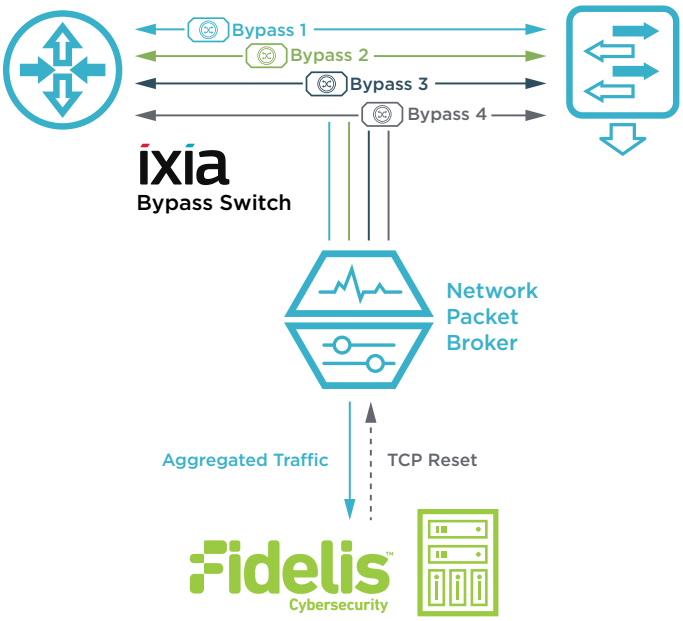
SOLUTION BRIEF

Fidelis Security and Ixia: Scalable Resilient Network Defense

THE JOINT SOLUTION

In today's world of defending against advanced cyber attacks, it is not enough to just identify attacks and alert on them; you must couple your detection strategy with a mitigation strategy. This is where the combined Fidelis and Ixia joint solution comes in.

Fidelis and Ixia have partnered to deliver solutions that enable scalable, flexible, and actionable security defense for your network. Ixia's Network Visibility Solution (NVS) uses its bypass switches and Vision ONE™ network packet broker (NPB) to aggregate traffic from all parts of your infrastructure and deliver it to Fidelis for security inspection and prevention. Ixia's Vision ONE can deliver traffic to Fidelis Network™ for advanced threat detection at every stage of the attack lifecycle, while at the same time it can be used as a mechanism to send Transmission Control Protocol (TCP) resets to a specific host for attack mitigation. For added flexibility, Ixia's NPBs can deliver traffic to other specialized tools, such as Web application firewalls (WAF) or application performance monitoring (APM) tools, protecting



915-8131-01 Rev A

the customer's legacy tool investment—and filtering can be used to send only relevant traffic (e.g. HTTP/HTTPS) to specialized tools in order to maximize useful utilization and return on investment for those tools. For inline resiliency, Ixia bypass switches and NPBs use automatic heartbeat health checks to ensure desired network connectivity is maintained, even when network monitoring services may be down. The modular aspect of the individual bypass switches and the standalone NPB provides customers the flexibility to design the architecture with the desired number of data inputs and outputs. It also overcomes common infrastructure blinds spots by delivering distributed network traffic to Fidelis for analysis.

BENEFITS

- Efficient data collection for out-of-band breach detection, as well as inline active mitigation
- Automatically maintains continuous connectivity, in case of tool maintenance or other outage
- Scales security solution capacity through inline and out-of-band load balancing
- Filters only relevant traffic to each tool, maximizing utility and return on investment
- Enables adding Fidelis best-of-breed security, while protecting investment in legacy tools

FIDELIS: NETWORK DEFENSE

Fidelis Network can detect attacks that other solutions miss. In addition to advanced malware, exploits, and command-and-control activity, Fidelis identifies attacker behavior, including lateral movement and the staging of data for exfiltration and halts data theft before it begins. And with the ability to correlate and validate alerts from unrelated events, it can conduct monitoring of reconstructed sessions for an advanced level of analysis and accuracy of attack defense.

IXIA: NETWORK VISIBILITY SOLUTION

Ixia's NVS provides complete network visibility into physical and virtual networks, improves network security, and optimizes monitoring tool performance. Ixia's NVS ensures that each monitoring tool gets exactly the right data needed for analysis. This improves the way you manage your data centers and maximizes return on investment. Ixia NVS sits between access points that require monitoring in the physical and virtual infrastructure and tools that need to analyze and protect data. Ixia's NVS simultaneously aggregates traffic from multiple Switched Port Analyzers (SPANs), taps, virtual taps, and bypass switches in the network and directs filtered relevant traffic to tools for analysis. Ixia's NVS also allows traffic sharing with multiple monitoring tools, eliminating the SPAN/tap shortages

that occur when another tool is attached to a needed access point. Moreover, NVS maintains network resilience with features such as automatic heartbeat health check, and it has an intuitive graphical user interface (GUI).

ABOUT FIDELIS CYBERSECURITY

Fidelis Cybersecurity is creating a world where attackers have no place left to hide. We reduce the time it takes to detect attacks and resolve security incidents. Our Fidelis Network and Fidelis Endpoint™ products look deep inside your traffic and content where attackers hide their exploits. Then, we pursue them out to your endpoints where your critical data lives. With Fidelis, you will know when you are being attacked; you can retrace attackers' footprints and prevent data theft at every stage of the attack lifecycle. To learn more about Fidelis Cybersecurity products and incident response services, visit www.fidelissecurity.com and follow us on Twitter @FidelisCyber.

ABOUT IXIA

Ixia (Nasdaq: XXIA) provides testing, visibility, and security solutions, strengthening applications across physical and virtual networks for enterprises, service providers, and network equipment manufacturers. Ixia offers companies trusted environments in which to develop, deploy, and operate. Customers worldwide rely on Ixia to verify their designs, optimize their performance, and ensure protection of their networks to make their applications stronger. Learn more at www.ixiacom.com.

WORLDWIDE HEADQUARTERS

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(FAX) 1.818.871.1805

www.ixiacom.com

EUROPEAN HEADQUARTERS

Ixia Technologies Europe LTD
Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

ASIA PACIFIC HEADQUARTERS

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127