Joint Solution Brief

Improve and Accelerate Threat Investigations with Gigamon and WireX Systems

The Challenge

Security investigations are taking too long. At the heart of the problem is a lack of history, context, manpower and even, investigative skills.

Integrated Solution

Combined with the GigaSECURE® Security Delivery Platform, the WireX Systems Integrated Investigation Platform overcomes forensics limitations and complexities by translating raw packets into content and behavior aware intelligence that security professionals can immediately understand.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic from physical, virtual and public cloud networks through the GigaSECURE Security Delivery Platform.
- Filtering and distribution of relevant traffic to the WireX Systems Integrated Investigation Platform accelerates processing throughput.
- Human-readable intelligence that enables security professionals at all skill levels – security managers, Security Operations Center (SOC) operators, analysts and incident responders – to quickly validate threats and handle more complex investigations.
- Cost-effective storage of forensics history, with retention periods up to 25 times longer than traditional solutions.

Introduction

To truly investigate security threats, organizations must capture and analyze all network traffic. Unfortunately, not only does the complexity of sorting through mountains of packets require rare, advanced skill sets, but capturing everything is a storage nightmare. As a result, organizations often only store a few days' worth of packets – not nearly enough to conduct accurate forensics.

To help organizations overcome storage limitations and skill set barriers, the WireX Systems Integrated Investigation gives context to security alerts and eliminates the heavy lifting of data analysis. The solution automatically classifies precise user behaviors within each application, extracts actual content – and not just metadata – in real time and stores it for months. This way, security teams can easily access emails, chats, file transfers, database transactions and remote logins to gain full context of security incidents.

The Gigamon and WireX Systems Joint Solution

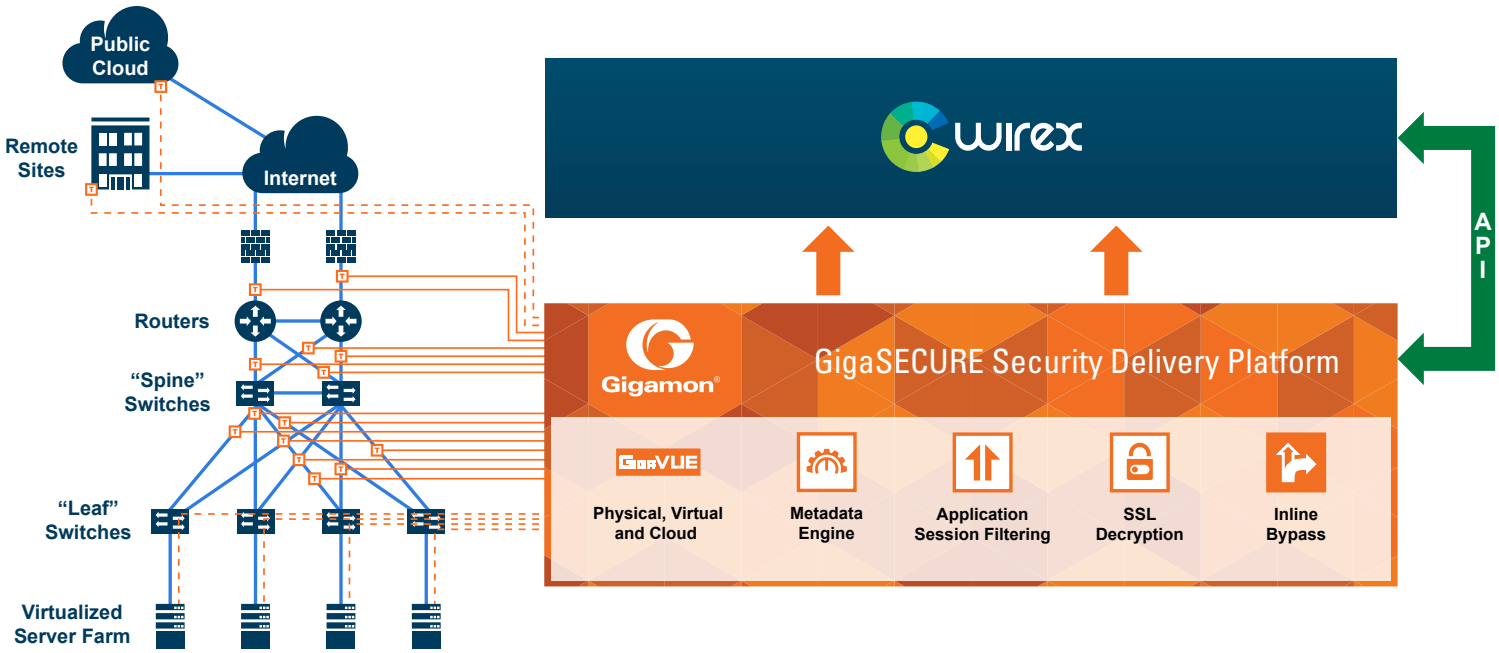
Unlike complex legacy solutions that are slow to parse data, the WireX Systems Integrated Investigation Platform can be used across the entire security organization – SOC, incident response, Security Information and Event Management (SIEM) manager – to quickly validate alerts, handle complex investigations and diminish ticket escalation.

When malicious activity is detected, the WireX Systems Integrated Investigation Platform retrieves related alerts from an organization's SIEM system and searches across all its own analysis sensors to compile clear, comprehensive data for an investigation. While managing and documenting the process, the WireX Systems Integrated Investigation Platform also enriches this data using external tools, such as threat intelligence feeds, to deliver the necessary information to take action.

All analyzed data is efficiently compressed prior to indexing to enable organizations to cost-effectively store months of forensics data within the same budget. In fact, the solution boosts forensics retention periods by up to 25 times longer than those offered by traditional packet-capture solutions.

Integrated with the GigaSECURE Security Delivery Platform, the WireX Systems Integrated Investigation Platform provides easy-to-use forensics context, efficiently delivering months of in-depth visibility to reveal the scope and impact of security incidents. By upleveling skills and creating powerful workflows for knowledge sharing, the integrated solution helps everyone in the SOC become a valuable analyst.

© 2018 Gigamon. All rights reserved.



Key GigaSECURE Security Delivery Platform features that enhance the value of WireX Systems technology deployments include:

Easy access to traffic from physical, virtual and cloud networks: The GigaSECURE Security Delivery Platform manages and delivers all network traffic – including east-west data center traffic and private and public cloud workloads – to the WireX Systems Integrated Investigation Platform to eliminate blind spots and help ensure that all traffic is analyzed together.

Aggregation to minimize tool port use: Where links have low traffic volumes, the GigaSECURE Security Delivery Platform can aggregate these together before sending them to WireX Systems Integrated Investigation Platform to minimize the number of ports needed. By tagging the traffic, the GigaSECURE Security Delivery Platform can also identify the traffic source.

SSL decryption: Real-time SSL decryption increases traffic visibility for the WireX Systems Integrated Investigation Platform, broadening the scope for analysis and inspection of malicious activity.

De-duplication: Pervasive visibility requires tapping or copying traffic from multiple points in the network, which in turn, means tools may see the same packet more than once. To avoid unnecessary packet-processing overhead on WireX Systems devices, the GigaSECURE Security Delivery Platform has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

Learn More

For more information on WireX Systems and Gigamon solutions, contact:

www.wirexsystems.com

www.gigamon.com

© 2018 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

3262-01 04/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com