JOINT SOLUTION BRIEF

IBM QRadar and the Gigamon Visibility Platform: Comprehensive Security Intelligence against Advanced Threats

The Challenge

To detect and defend against today's increasingly sophisticated and targeted cyber-attacks, security teams need to be more effective. More than just monitor logs and network flow data, they need to apply advanced profiling and analytics to reveal the footprints and movements of would-be attackers before they do damage. And that means being able to see all traffic and activities across the network and efficiently sharing information and insights between NetOps and SecOps teams.

The Solution

Together with the Gigamon Visibility Platform, IBM QRadar SIEM delivers network visibility and actionable security intelligence to identify anomalies and defend against advanced targeted threats.

Joint Solution Benefits

- Gain comprehensive, efficient visibility to all data – even encrypted data – across the network
- Detect known and unknown threats, going beyond individual alerts to identify and prioritize potential incidents and applying artificial intelligence (AI) to accelerate investigation processes by 50 percent
- Capture advanced application-specific metadata from the network to provide rich contextual data for incident detection, investigation and response

Introduction

Effectively securing an enterprise requires constant flexibility to adapt to evolving techniques and approaches used by attackers. This is especially true now as adversaries exploit users in social engineering attacks and deploy individually crafted, short-lived malware to establish their initial foothold. Identifying threats quickly and accurately requires having the right threat detection technology in place and giving it complete visibility to all network data.

Successful deployment of anti-threat technologies requires gathering traffic data coming across the entire network. You need to be able to see everything, to ensure you can detect possible security risks. Whether the data is flowing on fiber between routers, on virtual connections in a virtualized datacenter or in your own private segment of a public cloud infrastructure, you need to ensure security analytic tools are given a chance to do their work. And that means seeing into encrypted data too as malware can hide in encrypted traffic as well.

The Gigamon and IBM Security Joint Solution

IBM QRadar is designed to collect logs, events, network flows and user behavior across your entire enterprise. It then correlates that information against threat intelligence and vulnerability data to identify known threats, and also applies advanced analytics to contextual data you provide to signal anomalies that could be "unknown" threats. QRadar uniquely connects the end-to-end chain of activity associated with a single potential incident, and provides prioritized alerts based on severity, helping security teams quickly uncover critical threats while reducing false positives.

Network Data Visibility is Foundational

Getting all the relevant data into the IBM QRadar Security Intelligence Platform is essential to gain full insight and tracking of current and future threats. This is where the Gigamon Visibility Platform comes in:

Packet Data: If you are deploying QRadar components that need full packet data (for example, Network Insights), the Gigamon Visibility Platform can aggregate data from across your network and deliver it efficiently to the target QRadar components. Gigamon optimizes the packet data for efficient processing by the components and also makes the data available for other performance or security tools that need access.

Application Metadata: Gigamon is able to generate rich network metadata for the QRadar platform, providing greater contextual data for threat detection, investigation and remediation. As an integrated, licensable feature of the Gigamon Visibility Platform, NetFlow Layer 3 and 4 metadata can be generated from any traffic flow. In addition, Layer 7 application identification means over 3,000 discrete applications can be identified and advanced metadata records can be generated for each of these providing additional critical insight and granularity to your investigations. Ingesting the metadata into the QRadar platform is simplified using the Gigamon application available for the IBM X-Force Exchange.

Encrypted Data: A significant portion of web traffic is TLS/SSL-encrypted, making it a very attractive vehicle for malware. Gigamon provides a fast and efficient solution to enable inspection of encrypted traffic. By incorporating high-performance, inline decryption/encryption capabilities within the Gigamon Visibility Platform, you can create a decryption zone – sharing decrypted traffic with all tools that need to inspect the contents before re-encrypting the data (assuming inline prevention tools allow it to pass) and sending it on to its destination.

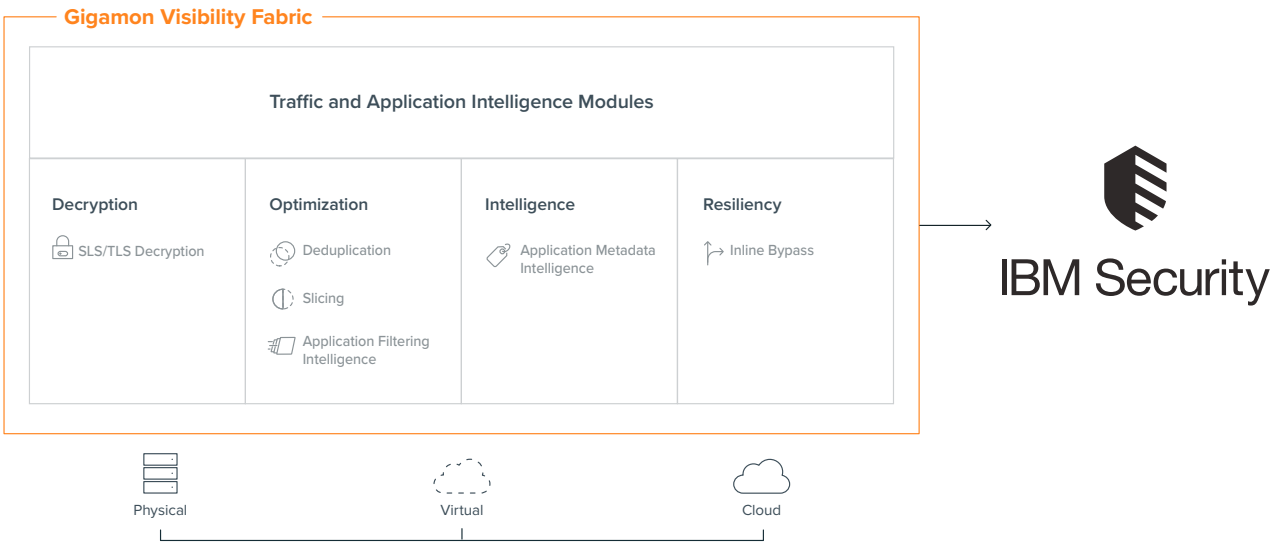

Figure 1: The Gigamon Visibility Platform gathers and delivers the network data IBM QRadar needs to secure your environment

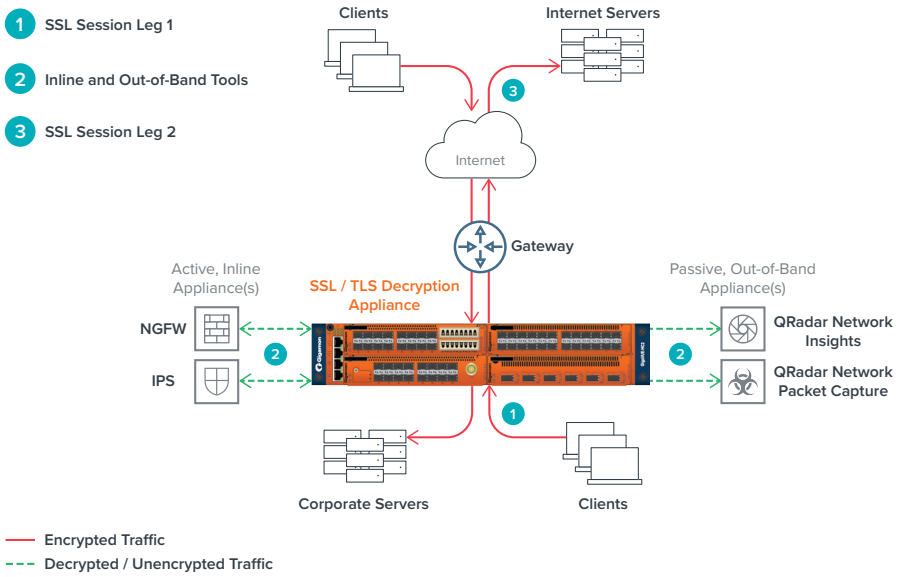

Figure 2: The Gigamon Visibility Platform centrally decrypts SSL/TLS traffic and easily shares decrypted traffic with the QRadar tools

For more information on Gigamon and IBM Security, visit:
www.gigamon.com and www.ibm.com

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