JOINT SOLUTION BRIEF

Gigamon-WitFoo Joint Solution Helps Smaller SecOps Teams Punch Above Their Weight

The Challenge

The fundamental challenge in cybersecurity today is the lack of human resources. Every day, organizations have more security events to investigate than is humanly possible to address — and the problem is compounded by the number of tools contributing events and the complexity of each tool. Best practices are out there in the security and law enforcement community, but how can you integrate those practices into your everyday work?

Integrated Solution

WitFoo Precinct has combined time-tested strategies used by criminal investigators and decades of experience leading cyber investigations. Integrated with the Gigamon Security Delivery Platform, WitFoo Precinct brings together human insight with a variety of technological approaches to cybersecurity.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic from physical, virtual and public cloud networks through the Gigamon Security Delivery Platform
- Divides traffic flow across multiple WitFoo Precinct instances
- Delivers full parity with SIEM, SOAR, UEBA and IRP solutions
- Offers an attractive, cost-contained license model with no professional services required

Introduction

If your SecOps team is like most, it's overwhelmed with security data. That's especially true at smaller enterprises. Large organizations have the resources to combine the best approaches in SIEM, IRP, behavioral analytics, orchestration and automation, and big data analytics, while still getting the human touch from cybersecurity experts. This can, however, be beyond the reach of smaller, resource-strapped organizations.

WitFoo Precinct can deliver all these capabilities in a flexible architecture you can instantly deploy and make operational in any environment — without the need for an accompanying professional services contract.

The Gigamon-WitFoo Joint Solution

WitFoo Precinct leverages the Gigamon Visibility Platform to reduce time and labor spent performing security investigations by more than 90 percent. The solution brings full parity with SIEM, SOAR, UEBA and IRP solutions while delivering unparalleled reporting capabilities.

WitFoo is built by veterans of the U.S. military, law enforcement and cybersecurity to deliver a more comprehensive platform for sustaining success in cybersecurity operations. The joint solution with Gigamon leverages human-learned insights and time-tested methodologies from physical law enforcement, delivering that expertise to your security infrastructure.

Key Gigamon Security Delivery Platform features that enhance the value of WitFoo Precinct deployments to secure networks include:

Easy access to traffic from physical, virtual and cloud networks: The Gigamon Security Delivery Platform manages and delivers all network traffic — including east-west data center traffic and private and public cloud workloads — to WitFoo Precinct, efficiently and in the correct format, to help eliminate blind spots and help ensure collective monitoring and analysis of all traffic.

Load balancing to spread traffic across multiple instances: When traffic flows are larger, the Gigamon Security Delivery Platform can split the flow across multiple WitFoo Precinct instances.

Metadata generation: The Gigamon Security Delivery Platform generates and sends unsampled NetFlow records for any traffic flow to WitFoo Precinct. It also sends extended metadata records — for example, HTTP response codes and DNS queries — to provide highly detailed contextual analysis when looking at network events.

For more information on Gigamon and WitFoo solutions,
visit: www.gigamon.com and www.witfoo.com.