

Business Brief

Test and Deploy New Cybersecurity Technologies Faster

With new threats emerging every day, IT organizations need to frequently upgrade or introduce new cybersecurity tools and technologies. The problem is that it can be very difficult to set up realistic tests that show how technologies will perform under real-world conditions.

To run a proof of concept on a single tool, security administrators can spend weeks rerouting traffic, changing firewall rules and reconfiguring servers and network devices. If they cut any corners or make any mistakes, it can skew the test results, with potentially disastrous consequences for security and network performance. Organizations can end up with tools that don't scale to meet their needs or that can't deliver intended feature benefits when network traffic spikes.

Even after a new security tool is selected, deploying it can require extensive manual work with very expensive inline interfaces needed to connect the tool to switches, network segments and taps. This is particularly true when networks are complex or highly segmented.

The GigaSECURE® Security Delivery Platform can dramatically reduce the time and effort needed to test and deploy new security technologies and tools. The GigaSECURE Security Delivery Platform is a next-generation network packet broker, purpose-built for security, that acquires network traffic from throughout an enterprise and feeds it as needed to any security tool in the organization.

With the GigaSECURE Security Delivery Platform, you can:

- Strengthen the testing of new security tools by using real data in a production environment without network disruption.
- Test multiple security tools together, comparing them side by side and selecting the ones that best meet your needs.
- Streamline the deployment of security products by moving them instantly from inline to out of band or out of band to inline.
- Reduce the need for expensive inline interfaces.

Strengthen the Testing of New Security Tools

Most enterprises are limited in how many security tools they can test and how thoroughly they can test them. Weeks of work by skilled network engineers and administrators are usually required to capture traffic from the enterprise for a proof of concept. This preparation work is especially time-consuming when it involves "East-West" traffic within data centers and traffic to and from private and public clouds.

With these constraints, organizations are left with no option but to evaluate fewer promising technologies and tools or to test them under unrealistic conditions. Some organizations are afraid to test inline security appliances at all because they fear tests will degrade network and application performance and disrupt business processes.

With the GigaSECURE Security Delivery Platform, you can select the right security tool much faster by running a completely realistic proof of concept, using production data and actual network traffic levels, with no impact on network performance. The GigaSECURE Security Delivery Platform acquires network traffic from throughout your enterprise and uses traffic intelligence to provide the exact traffic needed to each security tool. It can send the same production network traffic that goes to your current security tools, or any subset that you specify, to products you are testing.

You can deploy all security tools out of band during testing – even if they are normally placed inline – and eliminate the risk that testing will affect network performance or slow down applications. The GigaSECURE Security Delivery Platform allows you to compare more tools with less work and with better testing data. This means that you can select the right products and be confident that they will perform as expected.

Test Multiple Security Tools Together

The GigaSECURE Security Delivery Platform makes it easier to test complementary security tools together to ensure that the entire stack performs as expected. Testing is not constrained by a limited number of taps – for example, one traffic stream can be sent in sequence through multiple tools, such as a network access control

(NAC) appliance, an intrusion prevention system (IPS) and a web application firewall (WAF). Moreover, testing may also uncover configuration settings in one tool that impact the performance or effectiveness of others and provide administrators the opportunity to adjust settings before they affect real users and applications.

Streamline the Deployment of Security Products

The deployment of new security products can also require extensive manual work by administrators to reconfigure network and security tools. The GigaSECURE Security Delivery Platform, however, eliminates the need for this manual intervention by interfacing with the tools and enabling new security tools to access all the data they need, from all types of networks – on-premises, virtual and cloud environments.

Tools that need time to observe network traffic to build baselines and learn the difference between normal traffic and anomalies can run out of band as long as needed; when ready, they can instantly be switched to inline mode.

This streamlined process allows organizations to deploy security tools faster and defeat new threats sooner.

Eliminate the Need for Some Expensive Network Cards

Expensive network control cards are another factor that inhibits the deployment of inline security products such as web application firewalls, IPS and access control tools. In high-bandwidth environments, these interfaces can cost tens of thousands of dollars.

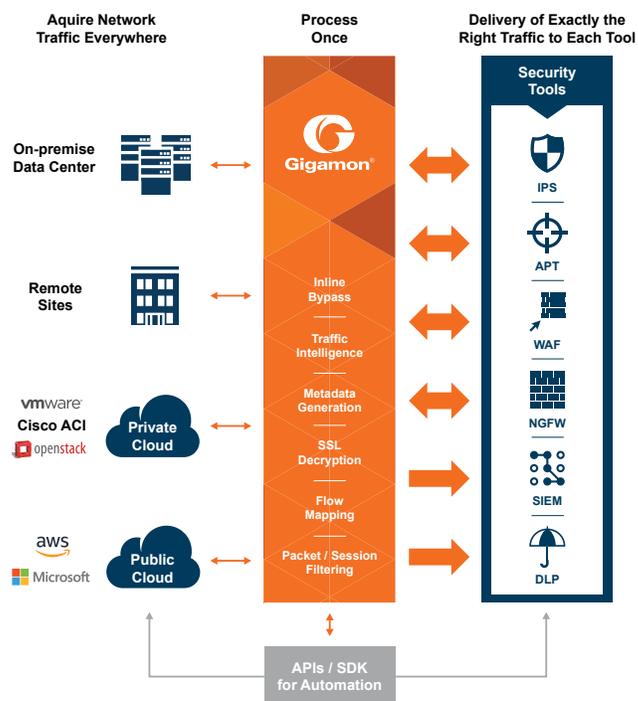
The GigaSECURE Security Delivery Platform enables these tools to receive traffic without an additional costly network card. In some situations, this factor alone can provide almost instant payback on the GigaSECURE Security Delivery Platform investment.

To find out how the GigaSECURE Security Delivery Platform can enable you to test security tools more thoroughly and deploy them faster, visit: www.gigamon.com

The GigaSECURE Security Delivery Platform

As illustrated in the diagram, the GigaSECURE Security Delivery Platform:

- Provides simplified access to network traffic across an enterprise.
- Delivers selected traffic of interest required by individual security tools, both inline and out of band.
- Offloads processor-intensive tasks such as SSL decryption and de-duplication from individual tools.
- Uses traffic intelligence to optimize network traffic or extract metadata from network traffic and deliver to the appropriate security tool.
- Provides a programmatic interface for integration with the security and infrastructure stack, enabling dynamic response to infrastructure changes, events and other early indicators of compromise.



The GigaSECURE Security Delivery Platform is a next-generation network packet broker purpose-built for security tools to work more efficiently across physical, virtual and cloud environments. For inline threat prevention tools, it strengthens security postures, simplifies IT and reduces costs. It also provides pervasive visibility into the activity inside the perimeter of an enterprise so that all security tools can quickly detect, analyze and block cyberattacks. It eliminates partial visibility and blind spots by acquiring network traffic from anywhere in the enterprise and applying traffic intelligence before delivering precise data to specific security tools in and across the organization