BEST PRACTICES
FOR APPLYING VISIBILITY TECHNOLOGY TO INLINE AND OUT-OF-BAND SECURITY

AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) WHITE PAPER
PREPARED FOR GARLAND TECHNOLOGY
BY SHAMUS MCGILLICUDDY
MARCH 2020

IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

Table of Contents

EXECUTIVE SUMMARY

Network visibility solutions are essential to security technologies that analyze network traffic. These solutions, including terminal access points (TAPs), bypass switches, and network packet brokers (NPBs), are foundational to ensuring that security solutions can reliably protect the enterprise without impacting service availability and performance. Typically, enterprises require two kinds of visibility technologies for security: one for inline appliance connectivity and other for mirroring traffic data to passive analysis tools.

This paper explores how enterprises use network visibility technologies for both inline and out-of-band security use cases to support security solutions.

BYPASS DEVICES FOR INLINE SECURITY

The Importance of External Bypass Devices

Today's enterprises have a variety of inline security solutions in place. Enterprise Management Associates (EMA) research found that three-quarters of companies have intrusion prevention and web application firewalls installed. Seventy percent have a distributed denial of service (DDoS) protection solution, and 65% have an inline data loss prevention tool. Nearly 60% have a next-generation firewall.[1]

All of these solutions are bumps in the wire. They inspect production traffic and decide whether to block or allow that traffic to pass through. If an inline security appliance performs poorly, network health and performance will also degrade. If the device fails, it can cause network downtime.

Due to these risks, bypass functionality is essential to inline security deployments. Many inline security appliances have internal bypass functionality that triggers if a device fails. However, these onboard bypass functions are less reliable than specialized external bypass devices, like bypass TAPs, bypass switches, and inline NPBs. External bypass devices can also report on security device health and performance, and they may offer packet manipulation features that can make security appliances more efficient and effective.

EMA's research found that extensive use of external bypass devices is a best practice. As **Figures 1** and **2** indicate, enterprises that are successful with their use of inline security appliances are more likely to apply external bypass devices to all their deployed appliances, in both the data center and the enterprise network.

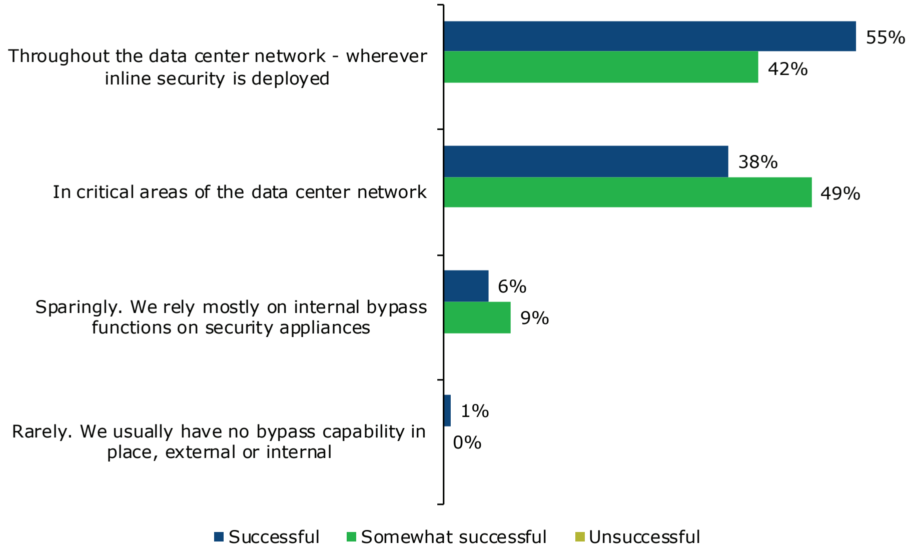

Figure 1. In the data center, successful organizations rely more on external bypass devices for inline security

[1] All data in this research was originally published in the EMA research report, "Visibility Infrastructure Strategies for Inline and Out-of-Band Security," in February 2020.

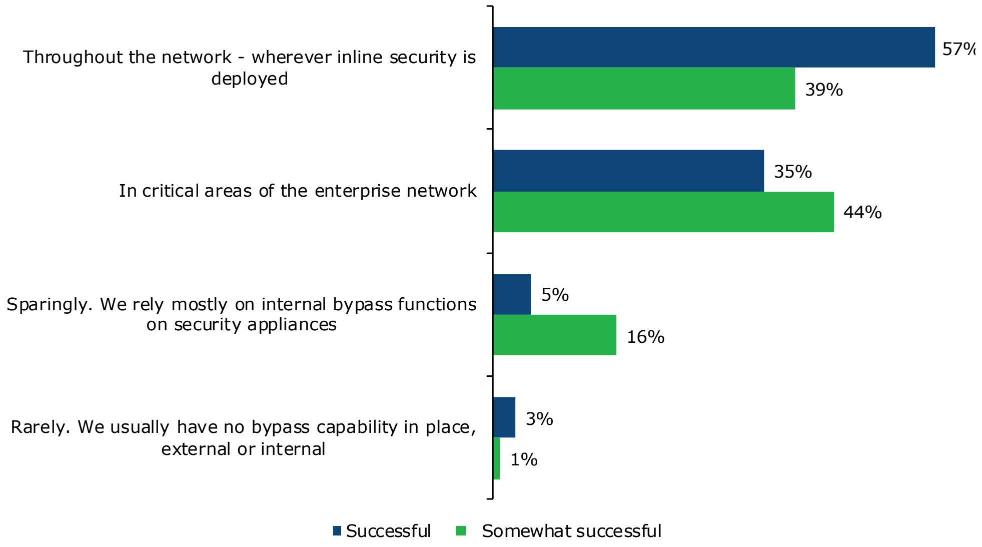

Figure 2. In the enterprise network, successful organizations rely more on external bypass devices for inline security

Bypass Device Requirements

Enterprises typically deploy a defense-in-depth approach to network security, with multiple types of security controls at the edge of the network. Thus, enterprises often need a bypass device that can support the connectivity requirements of two or more appliances at once. EMA's research found that 63% of enterprises require their bypass devices to serve multiple appliances. This will reduce the risk of a breach when a security appliance fails. The bypass device will engage to maintain uptime, but it will still send traffic through the other security controls at the edge of the network for inspection.

Bypass devices also present an opportunity to measure and monitor the performance of security appliances. Some bypass devices can deduce inline security appliance performance by monitoring egress and ingress traffic. By analyzing traffic as it is forwarded to and received from a security appliance, the device can measure how much latency was added to the network and detect whether there were any packet drops or errors. Nineteen percent of enterprises say this is their preferred method of monitoring inline security performance. This monitoring approach is particularly interesting to enterprises that give administrative control of bypass devices to data center operations teams (30%).

Bypass Device Benefits

Bypass devices tend to prove their value once deployed. For instance, 92% of enterprises had a bypass device engage itself in the past year to prevent downtime, and 81% reported multiple engagements within the last year.

Downtime prevention is obviously beneficial, but enterprises see other kinds of value in bypass devices, too. EMA asked enterprises to identify the single most important benefit they recognize from their use of bypass devices. **Figure 3** details their responses.

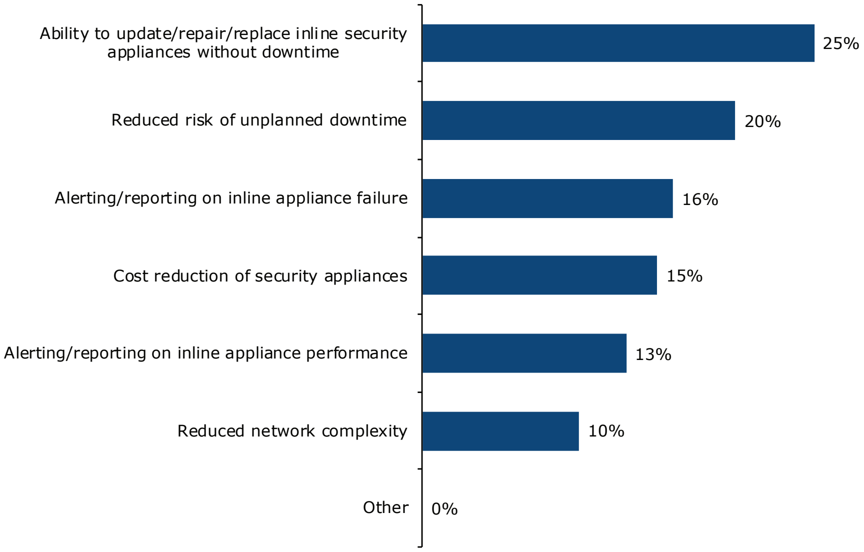

Figure 3. Most important benefit of using a bypass device to connect inline security appliance to the network

The ability to update, repair, or replace security appliances without downtime is the biggest opportunity. With bypass devices, enterprises can conduct these operations without creating a window for planned downtime. This benefit is more prized in enterprises that give the security team primary administrative control over bypass devices.

Preventing unplanned downtime is the other big opportunity. Alerting and reporting on appliance failures and cost reduction of security appliances are secondary benefits. Successful organizations told EMA that cost reduction was a low priority.

OUT-OF-BAND SECURITY

Inline security can't block everything, and breaches will happen. Passive, out-of-band security analysis tools are the next line of defense, and they require access to traffic, too. In fact, 92% of enterprises have detected attacks with passive monitoring tools over the last year.

Unlike inline appliances, out-of-band security tools are not bumps on the wire. They consume mirrored traffic, which means enterprises must deploy visibility solutions to deliver mirrored traffic to these analysis tools.

Enterprises typically have a variety of passive security solutions installed. EMA's research found that 55% of enterprises have passive data loss prevention tools connected to mirrored traffic today. Forty-six percent have SIEMs connected, 46% have DDoS detection, and 44% have intrusion detection, and 43% have network detection and response solutions.

Out-of-Band Visibility Architecture

Passive security begins with mirroring traffic from the network. Enterprises have two basic options: a TAP device or a span port analyzer (SPAN) feature on a switch or router. SPANs can add overhead on a network device, and that SPAN port will often drop mirrored packets if the device gets too busy. Therefore, TAPs are a better option. Due to resource constraints, most enterprises will use a mix of TAPs and SPANs. However, EMA found that 45% of companies rely on a majority of TAPs, while only 21% use a majority of SPAN ports. The rest (29%) claim to have a 50/50 split between the two options.

From the mirrored port to the analysis tool, enterprises have two basic options. They can connect analysis tools directly to the mirrored port, or they can use an NPB or similar device to aggregate traffic, process it, and load balance it across analysis tools. Aggregation devices like an NPB allow tools to analyze different parts of the network simultaneously. Enterprises are roughly split on their primary architectural approach; 51% primarily rely on NPBs rather than a direct connection to a mirrored port.

Out-of-Band Network Packet Broker Requirements

NPBs can add a lot of value to out-of-band security through traffic manipulation features, which can reduce the amount of packet processing required of analysis tools. **Figure 4** looks at the NPB features enterprises find most valuable for passive security use cases.

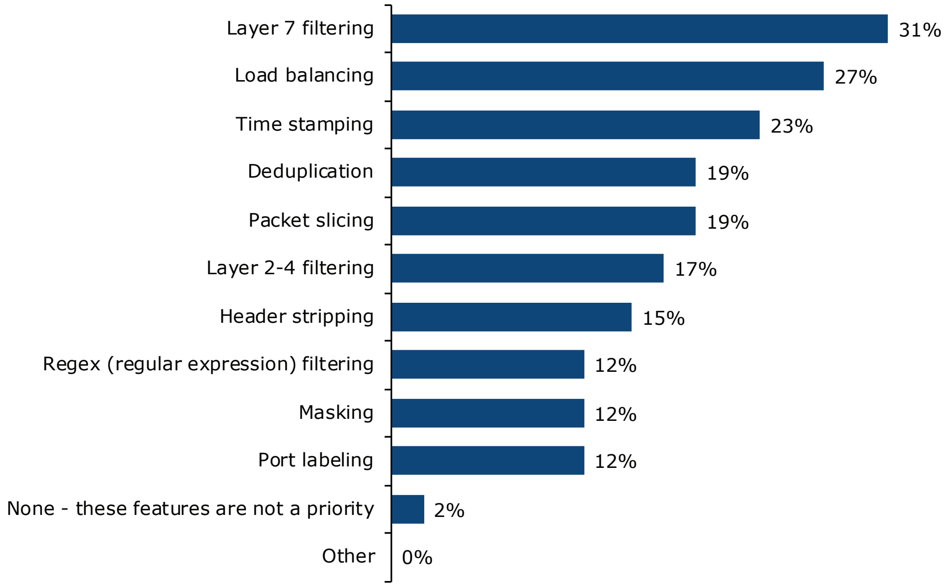

Figure 4. Most important traffic manipulation features for visibility technologies that deliver traffic data to out-of-band security

Layer 7 filtering is much more valuable than Layer 2 though Layer 4 filtering. Load balancing across tools is also a big priority, followed by time stamping, although successful organizations are less interested in the latter feature. Deduplication and packet slicing round out the five most popular features.

EMA PERSPECTIVE

Good security requires visibility. EMA research reveals that enterprises need to invest in TAPs, bypass devices, and NPBs to optimize their security controls and analysis tools. These solutions must be scalable, reliable, and feature rich.

This paper presented some insight into peer-driven best practices for applying visibility solutions to security technologies. Every network is unique, however. EMA recommends that security and network teams do their homework to determine which visibility strategy will work best for their security requirements.

ABOUT GARLAND TECHNOLOGY

Garland Technology is an industry leader delivering network products and solutions for enterprise, service providers, and government agencies worldwide. Since 2011, Garland Technology developed the industry's most reliable test access points (TAPs), network packet brokers (NPB), and cloud solutions, enabling data centers to address IT challenges and gain complete network visibility.

Securing and monitoring your network is the ultimate goal. Garland's TAP to Tool™ philosophy empowers the solution by architecting to the tool, not competing with them. Garland Technology provides the scalability and flexibility to deploy what you need, when you need it, so you can focus on what's important – network visibility.

Garland Technology ensures complete 360° network visibility by delivering a full platform of network access products, including breakout TAPs, aggregator and regeneration TAPs, advanced all-in-1 filtering TAPs, inline edge security bypass TAPs, cloud solutions, as well as purpose-built network packet brokers.

For help identifying the right visibility solution for projects large and small, or to learn more about the inventor of the first bypass TAP, visit GarlandTechnology.com or @GarlandTech.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates® (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3940.02202020