WHITE PAPER

A Network Architect's Guide to Inline Security - Performance Matters

Security is top of mind today, not only for network architects and IT staff but also in the boardroom. Security is a critical area of executive concern because of its ability to do the following:

- impact revenue
- increase corporate risk
- adversely affect customer satisfaction
- jeopardize regulatory compliance initiatives

How do you translate these goals into a realistic and achievable security architecture? Using inline security solutions is one way. The solution is more than just adding an inline security appliance, such as an intrusion protection system (IPS) or a web application firewall (WAF). It requires complete data visibility, which allows the examination of all data for suspect network traffic.

This white paper does the following:

- summarizes the market drivers for inline security
- shows how an inline architecture solves common security problems
- provides an overview on how to implement inline security

KEYSIGHT TECHNOLOGIES

Inline Security Market Drivers

According to the latest World Economic Forum report on global risks, cyberattacks and data fraud or theft are two of the top five risks that CEOs face[1].This has led to a reprioritization of enterprise objectives and spending. Data from Forrester Research shows that businesses' top security priorities for the next 12 months following January 2019[2].

1. improve advanced threat capabilities
2. improve return on security investments
3. simplify the security environment
4. increase security staff productivity
5. improve operational efficiency

Translating the list above into actionable insights yields the following points:

- Cyberattacks and security incidents are prevalent and costly.
- Security tool failures can cause network and application downtime.
- Successful security monitoring depends on complete visibility.
- Simplicity helps control cost.

Network security has been a hot boardroom topic since at least 2015. To address the risk, businesses are strengthening their security systems and processes.

However, for a business to be truly successful at achieving these goals, it needs to translate them into actionable insights that allow for the rearchitecture of the entire security network. This will not be an easy task. The good news is that technology is available to help businesses create the right security architecture to address these goals, along with unforeseen sources of risk. The next section provides generalized insight to help solve the problem.

1. "The Global Risks Report 2019, 14th Edition." World Economic Forum, 2019. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
2. Complexity In Cybersecurity Report 2019: How Reducing Complexity Leads to Better Security Outcomes. Forrester Consulting and IBM, May 2019. https://www.ibm.com/account/reg/us-en/signup?formid=urx-38409

The need for an inline security solution

Organizations are finding themselves fighting security battles on many fronts: an increase in the velocity and variety of cyberattacks, an increase in the number of alerts they need to investigate, malware camouflaged in encrypted traffic, and breaches that are harder than ever to spot. Each of these threats can have a significant impact on the bottom line.

As security teams struggle to manage a growing volume of alerts, alert fatigue becomes very real. According to the 2020 State of SecOps and Automation Report, 83% of IT security professionals surveyed said they had experienced alert fatigue, which can lead to complacency. Of those surveyed, 70% said the volume of security alerts they receive has more than doubled since 2015[3].

Even if only one in a million alerts is valid, a security breach can be detrimental to a business, causing it to lose revenue and customers while tarnishing its brand reputation. A proactive cyberdefense is necessary to reduce the impact of security threats. However, this does not eliminate the need for a reactive defense. A real-time, proactive defense augments the reactive to reduce the onslaught of attacks and attack vectors against the network. There are four key drivers for the deployment of real-time security measures:

- Cyberattacks and security incidents remain prevalent and costly.
- Business operations cannot tolerate network or application downtime, especially when security attacks or component failures are the cause.
- Successful security monitoring depends on complete data visibility, including encrypted traffic.
- Control of solution costs and complexity depends on the amount of simplicity integrated into the solution.

Rampant and costly cyberattacks

The multitude of security breaches we hear about almost daily shows just how vulnerable organizations are to attack vectors in the wild. Cybersecurity Ventures estimates that in 2021, cybercrime will likely cost the world $6 trillion per year, more than the combined gross domestic product of the UK and France. This has doubled since 2015.

3. 2020 State of SecOps and Automation Report. Sumo Logic, n.d. https://www.sumologic.com/brief/state-of-secops/

Malware is the most expensive attack type for the majority of organizations. Cybersecurity Ventures estimated that global ransomware cost $11.5 billion in 2019 and could skyrocket to $20 billion in 2021 — 57 times the 2015 amount. Cybersecurity Ventures also predicts that a business will fall victim to a ransomware attack every 11 seconds in 2021[4].

Just as troublesome is the inability to stop attacks. Ponemon Institute found that 80% of cybersecurity and IT experts anticipate a "catastrophic" data breach at their companies by 2021 as a result of having unsecured Internet of Things (IoT) endpoints. In addition, a Microsoft study found that only 19% of businesses are highly confident in their ability to mitigate and respond to any cyber-event[5].

Fewer than half of IT respondents surveyed by LogRhythm indicated that their teams could detect a major cybersecurity incident within one hour. Most respondents who say it takes longer (more than two hours) to detect an incident are decision-makers. They also report that they do not have a security operations center (61%) or a formal program to protect against ransomware (64%), insider threats (68%), or denial-of-service attacks (71%)[6].

More importantly, Ponemon Institute found that it takes organizations approximately 279 days to identify and contain a breach. This is the data breach life cycle. The 2019 data breach life cycle was 4.9% longer than the 266-day average in 2018. The longer a breach's life cycle, the greater the total cost[7].

An important number to know is the median length of time between intrusion and detection for incidents, which was 206 days in 2018, according to the Ponemon study[8]. The other 73 days in the 279-day life cycle is the average time to contain the breach.

It's hard to imagine an intruder going undetected in your home for more than six months before you realize someone is there, then spending another 2½ months to get rid of that intruder. However, that is precisely what happens in many security breaches. The magnitude of potential damage and harm to an enterprise is staggering.

4. Morgan, Steve. 2019 Official Annual Cybercrime Report. Cybersecurity Ventures and Herjavec Group, n.d. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
5. Ponemon, Larry. "Ponemon Institute Announces the Release of the 2018 Megatrends Study." Ponemon Institute. Last modified March 15, 2018. https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf
6. 2018 Cybersecurity Perceptions & Practices. LogRhythm. https://logrhythm.com/cybersecurity-perceptions-practices-survey-white-paper
7. 2019 Cost of a Data Breach Report. Ponemon Institute and IBM, 2019. https://www.ibm.com/security/data-breach
8. 2019 Cost of a Data Breach Report. Ponemon Institute and IBM, 2019. https://www.ibm.com/security/data-breach

Another unfortunate fact is that most companies find out about a security breach from someone else (law enforcement, partners, customers) — as they often do not detect the intrusion themselves. In our example, that would be like having an intruder in your home for half the year, only to hear about the person's presence from your neighbor or the police department.

Network and application downtime

Incident response is fraught with manual processes and bottlenecks. A 2019 report from Viavi Networks indicates that 83% of network teams were involved in resolving security issues. Of those, 74% said they spent up to 10 hours per week, with another 17% saying they spent significantly more time[9].

Adding to the ordeal is that IT often deploys security tools directly inline. This tactic creates a solid line of defense, but these tools also introduce points of failure in the network. Deployment of any tool on the live network carries the risk of becoming a single point of failure. Should the inline tool go down, it can take the network link it's on down with it.

While some security tools include a bypass switch, that feature does not protect the network if IT takes the tool offline for maintenance or upgrades, which many organizations must do. This approach usually happens overnight or on weekends, and the work must be completed within a specified window, adding to the frustration and stress.

Network visibility and decryption

IT security and analytics tools are only as good as the data they see. IT has more traffic to monitor, coming from more sources, and carrying more threats than ever before. Globalization, the IoT, cloud, virtualization, and mobile devices are forcing companies to extend their network edge — often into places where they cannot easily gain visibility.

This situation causes vulnerable blind spots, which, like a dark alley, provide a place for attacks to go unnoticed. These blind spots have become a serious security issue for enterprises and service providers, especially when victimized companies don't discover the security breaches until it's too late to stop or contain the damage.

9. "Wire Data Is Now the #1 Network Data Source for Security Incidents: Twelfth Annual 'State of the Network' Survey from VIAVI." Last modified July 2019. https://comms.viavisolutions.com/State-of-the-Network-2019-vi56109

Threats obfuscated by encryption can bypass many security controls. Fifty-nine percent of businesses surveyed by Forrester Consulting report that getting visibility into security-related data and insights from across the organization is a top challenge[10]. The sudden and rapid expansion of a new or previously unknown application can enable threats to go undetected until they jeopardize the network's availability and health.

The use of encryption for legitimate traffic and malicious cyberattacks alike continues to grow. "More than 70% of malware campaigns in 2020 used some type of encryption to conceal malware delivery, command-and-control activity, or data exfiltration. And 60% of organizations fail to decrypt HTTPS efficiently, missing critical encrypted threats," Cisco Systems reported[11].

Security architecture complexity

Security environments are increasingly complex. In fact, the following data from a Forrester Consulting report shows that 91% of organizations are concerned about complexity in IT networks. Security professionals tend to operate in siloed teams, so it is rare — if not impossible — to get a full picture of data and processes across the entire security discipline. As an example, 72% believe simplification would have a "moderate" or "significant" improvement in operational efficiency, security staff productivity (68%), and security investment return (58%) — addressing their highest priorities[12].

A study by Jon Oltsik, senior principal analyst at Enterprise Strategy Group and founder of the firm's cybersecurity service, uncovered similar findings. According to his research, "83% of respondents believe network security has become more complicated over the last two years." His research also showed that this complexity is a direct cause of security incidents in 29% of organizations[13].

10. Complexity in Cybersecurity Report 2019: How Reducing Complexity Leads to Better Security Outcomes. Forrester Consulting and IBM, May 2019.
11. "Cisco Encrypted Traffic Analytics." Cisco, 2019. https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf
12. Complexity in Cybersecurity Report 2019: How Reducing Complexity Leads to Better Security Outcomes. Forrester Consulting and IBM, May 2019.
13. Oltsik, Jon. Navigating Network Security Complexity. Enterprise Strategy Group, June 2019. https://www.cisco.com/c/dam/en/us/products/collateral/security/defense-orchestrator/esg-research-insights-report.pdf

Organizations are spending more but not necessarily getting more security for their money. Increases in security budgets and organizational pressure to avoid a damaging data breach have led them to adopt a plethora of disconnected point solutions. On average, organizations have added 52% more security products and 77% more vendors over the last two years, according to Forrester Consulting. In addition, they are managing an average of 25 security products or services from 13 vendors[14].

Oltsik sums up the problem this way: "What's killing security is not technology; it is operations. Companies are looking for ways to reduce their overall operations requirements and need easy-to-use, high-performance solutions to help them do that."

Solving the problem with inline security

Effective security monitoring depends on having visibility into traffic across all links in your network, including virtual and encrypted traffic, without the danger of dropped packets. The larger and more complex your network, the greater the probability of network blind spots and the risk of threats going undetected. That is why a strong visibility architecture should be the foundation of your security architecture. The tremendous amount of data that traverses your network needs quick inspection to identify packets that require further analysis.

One way to address the risks mentioned above is to create an inline security architecture. This allows you to immediately inspect and stop bad traffic before it ever enters your production network.

While an inline security architecture will not create a foolproof defense against all threats, it provides the crucial data access security that engineers need. Data is the lifeblood of any security architecture. The wrong data can result in false positives, or, even worse, missing data can result in false negatives, leaving you feeling safe when, in fact, you are not.

Combining inline visibility with inline security appliances creates a formidable defense. For instance, extensive use of encryption, data loss prevention (DLP), threat intelligence sharing, and the integration of security into the software development process are all associated with lower-than-average data breach costs. Among these, encryption had the greatest impact, reducing breach costs by an average of $360,000, according to Ponemon Institute[15].

14. Complexity in Cybersecurity Report 2019: How Reducing Complexity Leads to Better Security Outcomes. Forrester Consulting and IBM, May 2019.
15. Rathod, Lakshna. "Cost of a Data Breach: Ponemon Institute Report." Diligent, August 13, 2019. https://diligent.com/en-gb/blog/cost-of-a-data-breach-ponemon-institute-report

The following chart summarizes four security-related problems and the inline solution that companies can deploy to mitigate, if not remedy, the issue.

Table 1. Potential solutions for the four most common security problems

Key specifications	Options
Cyberattack prevalence and increasing costs	Reduce number and cost of breaches • Deploy inline tools to inspect data • Add an NPB to make data distribution easy
Network and application downtime	Increase network and application availability • Insert external bypass switches to support business continuity fail-overs • Use NPB for n+1 tool survivability • Deploy NPB in high-availability model
Lack of data visibility, including encrypted traffic	Insert a visibility architecture • Deploy an NPB to regenerate data to multiple tools for analysis • Deploy an NPB with internal SSL decryption • Deploy an external appliance to perform SSL decryption
Increasing amount of complexity	Replace complexity with simplicity • Use an NPB for remote access to tools • Use an NPB for simplified programming with a graphical user interface • Use an NPB for serial tool chaining • Use an NPB for aggregation and filtering of data • Use an NPB for deduplication (if needed) to remove extraneous data

The Inline Visibility Architecture

Inline means that a component or tool is deployed directly in the path of network data flow. This includes both security tools and network visibility equipment. In the case of visibility equipment, this would be a bypass switch, packet broker, and security appliances. One drawback to this approach is that if any system in the data path fails, the link goes down. Fortunately, solutions that provide fail-over and redundancy eliminate the failure concern.

External bypass switch

The purpose of a bypass switch is to route traffic around tools that have gone down, either because of some fault or power issue or because they need software updates, patches, or subsequent reboots.

You can set a bypass switch to fail open or fail closed. Fail open means that traffic continues to flow between network devices if you remove a security monitoring device from the network or the bypass switch loses power. This mechanism is also known as "fail to wire" to clarify that this failure scenario supports business continuity. In the fail-closed scenario, the bypass switch's failure results in no traffic passing, the safest option.

The bypass switch generally uses a heartbeat packet to detect application, link, or power failure on the attached monitoring device. If the heartbeat packet gets disrupted, the bypass switch removes this point of failure by automatically shunting traffic around the security tool whenever the tool is incapable of passing traffic.

While directly deploying inline security tools can create a line of defense, these tools can also result in single points of failure. Even a strong mix of security and analytics tools can lead to network reliability risks as regular rebooting, maintenance, and upgrades of those tools increase the chances of a costly network outage. If an inline tool becomes unavailable, it can bring down the network link, compromising network uptime and disrupting business continuity. This can be a big problem for the almost 20% of IT organizations that directly deploy inline security tools and the 40% that deploy internal bypass solutions instead of external solutions[16].

An external bypass switch allows fail-safe deployments of inline security and monitoring tools to ensure high availability and maximum uptime. The standalone (external) bypass offers superior protection compared with a security tool with an integrated bypass option.

16. McGillicuddy, Shamus. "On-Demand Webinar: Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics." Enterprise Management Associates. Accessed September 12, 2019.

Some external bypass switches have a mean time between failure (MTBF) of approximately 450,000 hours. This reliability can be up to five times better than various security tools like combined firewall and IPS solutions with a MTBF of 80,000 to 100,000 hours. Adding internal bypass capability further reduces the MTBF and reliability for those types of solutions[17]. When you replace various security tools, you may have to remove the integrated bypass. An external bypass eliminates this issue.

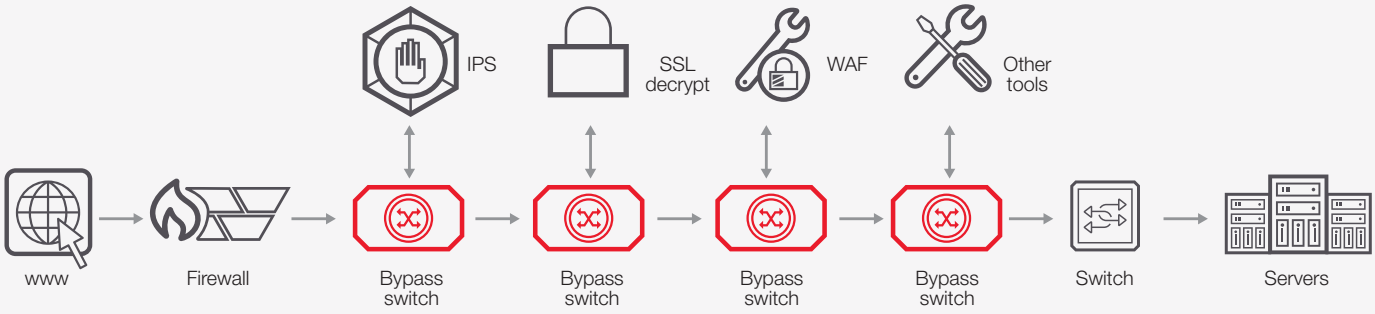

Figure 1. Inline security solution with a bypass switch connected to all components

Another key benefit of the external bypass switch is fail-over capability during upgrades. Certain inline security tools include an internal bypass switch. This becomes a problem when you want to replace the security tool or, in some cases, simply update and maintain that tool. Software upgrades or security patches may require a reboot, with obvious negative implications for architectures using internal bypass switching.

The simple solution is to use an external bypass. Then you do not have to worry about future upgrades.

An external bypass offers the following benefits:

- It eliminates single points of failure for inline tool deployments with a bypass switch.
- The MTBF of an external bypass switch can be up to five times better than an integrated bypass.
- It provides more flexibility to add or remove inline security tools without network impacts.
- An external bypass switch eliminates downtime from tool upgrades and removal.

17. Keysight-conducted research.

Inline network packet broker

The main purpose of the network packet broker (NPB) is to optimize the flow of data going to security tools. Sitting between bypass switches and inline security appliances, packet brokers add another layer of data visibility to your security architecture. By providing the ability to aggregate, filter, deduplicate, load balance, and decrypt Secure Sockets Layer (SSL)/Transport Layer Security traffic, packet brokers provide serialized data to a chain of security tools for deep data analysis. With an NPB acting as a go-between, all security appliances can connect seamlessly and safely to ensure that they don't cause network failures.

Inline versions of NPBs also contain heartbeat and fail-over capabilities to properly handle data continuity and high availability. This works similarly to the bypass switch, except that it is two-sided. There is communication between the bypass and the NPB to make sure the NPB is working. If not, the bypass switch will either divert the flow into the network or stop traffic transmission. The exact action depends on the options selected for the bypass.

Another set of communications sits between the NPB and security appliances. This provides continuity and survivability for the data analysis process. Should a security appliance fail, the NPB will divert traffic to other available security appliances. If all security appliances are out of operational state, you can set the NPB configuration to operate in one of two ways.

First, it could signal an error state to the bypass. The bypass switch will interpret this as a failure and follow its preprogrammed fail-open or fail-closed scenario. Once the security tools are operational again, the NPB replies to the bypass switch heartbeat message, and data flows from the bypass to the NPB again.

The second tool failure option is for the NPB not to declare an error and simply shunt the traffic back to the bypass. While this means that no security inspection occurs, the network remains up until one or more of the security tools becomes available again. Then the NPB will forward incoming traffic to the security tool(s).

The NPB supports load balancing, ensuring that your tools actively process traffic but not at full capacity. If one or more tools fail, the NPB will redirect to surviving tools. This is an excellent and cost-effective way of using n+1 survivability to create tool redundancy, assuming the tools are over-dimensioned by at least one device acting as a spare ready to take over. Utilizing load balancing on a packet broker allows your n+1 spare to be used for load balancing during regular operation, so it isn't just a backup tool sitting idle most of the time.

Another benefit of a packet broker is that you can automate the data inspection process. Tool chaining is a powerful way to automate this movement of data packets between security monitoring solutions. Suspect data gets passed back and forth between an NPB and multiple security tools, including IPS, DLP, SSL, WAF, and next-generation firewalls, allowing for deeper analysis of indeterminate data. For example, if your IPS flags data as being suspicious but can't make a concrete determination, it can send the data to a WAF and then a DLP for further screening. Security tool chaining provides the interoperability needed to make network security protection mechanisms successful.

Preset toolchains ensure that data passes sequentially from one tool to another so that actions occur in sequence and are not overlooked. You can link security and monitoring tools by using software provisioning in the NPB to control the flow of data through the selected services. Depending on the situation, the required data inspection can occur in parallel or series.

The primary way Keysight addresses tool chaining is to use a grouping of ports. To accomplish the proper flow of data, at least one tool gets assigned to a port or port group on the NPB. Multiple port groups require chaining together to accomplish the desired data flow.

NPBs provide many benefits that help tools run at top speed with minimal latency. These include the following:

- Improved uptime
- Real-time decision-making
- Extensive fail-over options
- Cost savings resulting from load balancing across multiple tools
- Built-in recovery options
- Reduced complexity
- Fewer upgrades needed, lowering total cost of ownership and maximizing investment
- Diversion of bad traffic to a honeypot

Not all NPBs are the same. Many rely on onboard software-based CPU processing. Keysight uses advanced hardware acceleration that has shown to be far superior in side-by-side performance tests with competitive products that rely on CPU processing. CPU-based NPBs often can't use all their features simultaneously because of limited CPU power, which significantly slows down application detection and reporting. Keysight's NPBs, which use dedicated hardware-based processing, do not have these limitations.

Complete visibility architecture diagram

The following diagram shows the proper way to integrate a bypass and an inline NPB into an inline security architecture.

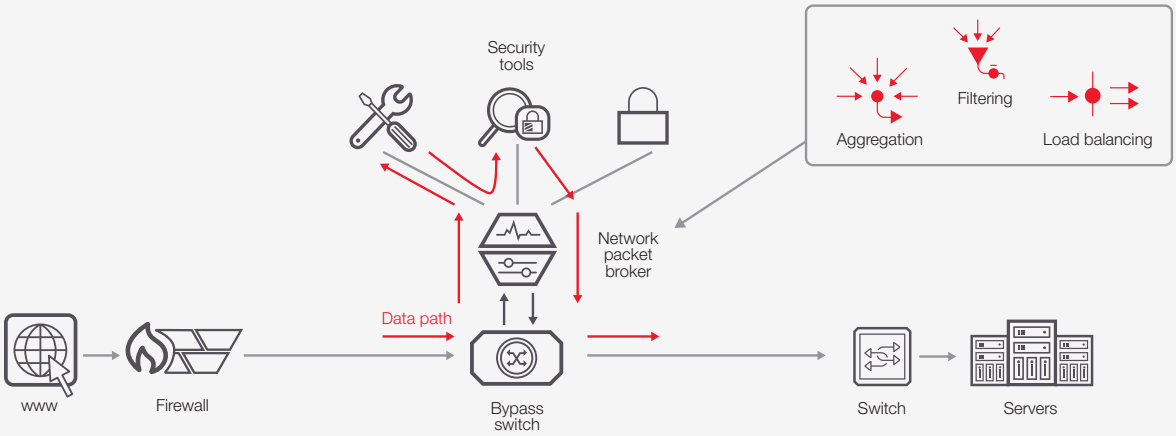

Figure 2. Inline security solution showing a typical traffic data path

Conclusion

Inline security solutions are a requirement for today's security architectures. Organizations cannot afford to ignore this type of solution anymore. The volume of security attacks, increasing network complexity, and the rapid growth of breach costs and risk necessitate a change.

An inline solution starts with an external bypass switch and an NPB. Such a solution enables security teams to do the following:

- Increase network reliability with better fail-over
- Improve security appliance survivability
- Perform SSL decryption to expose hidden security threats
- Reduce security architectural complexity
- Better capture indicators of compromise

Keysight can help you enhance your inline security deployments with a wide range of bypass switches and NPBs.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES