WHITE PAPER

Important Network Visibility Use Cases for the Financial Industry

According to a joint 2017 Ponemon instiute and Accenture study *(Cost of Cybercrime study: Insights on security investments that make a difference)*, the financial services industry suffers the most loss of any industry due to cybercrime, with an annual loss of **$18.28 billion**.

Digital Disruption Occurring in the Financial Industry

The financial industry is experiencing a massive wave of change. As digital transformation has swept through this industry, cybercrime has risen dramatically. For instance, according to a joint 2017 Ponemon Institute and Accenture study (*Cost of Cybercrime study: Insights on security investments that make a difference*), the financial services industry suffers the most loss of any industry due to cybercrime, with an annual loss of $18.28 billion. One recent example is the ATM Cashout attack that has hit various banks. Many other security intrusions and breaches have also been successful.

Other financial industry segments have been disrupted as well. Some examples include: insurance companies rushing to cloud computing to meet growing demands to support new customer applications and services, credit card companies being hit with web-based attacks and on-line fraud, and financial trading companies moving to acquire instantaneous access to market feeds before stock prices change.

Network visibility components and techniques are valuable tools in this dynamic environment. Visibility eliminates blind spots, decreases troubleshooting and monitoring costs, improves operational efficiency, and enhances compliance data.

KEYSIGHT TECHNOLOGIES

What Is Network Visibility?

IT teams are under ever-increasing pressure to improve various responsibilities, such as optimizing performance and security of IT networks and applications, monitoring security posture, and monitoring and enforcing compliance mandates. These initiatives require access to comprehensive network data. For security and monitoring solutions to perform optimally, they need full visibility into the network. The ramifications of limited visibility include extended threat analysis times, more false positives, inaccurate conclusions, and longer mean times to repair (MTTR). Simply put, more data results in better monitoring, which reduces your troubleshooting and forensic analysis costs, as well as the cost due to missed security threats.

When it comes to data monitoring, ensuring proper access to network data is the most critical thing you can do. After that, data filtering and the conversion of data into actionable information can take place. This is where a visibility architecture is important.

A visibility architecture is a design that provides access to network traffic, intelligently filters the requisite data, sends the groomed data to analysis tools, and then delivers information from the monitoring tools so that IT can make informed decisions about problem resolution and network performance. With the proper visibility architecture in place, you'll be able to see what is (and what is not) happening on your network.

To accomplish these goals, two fundamental components are required:

- Installation of test access ports (taps) to access network data
- Installation of a network packet broker (NPB) to filter and distribute that data to purpose-built devices for analysis

Proper visibility starts with proper data access. The first and easiest task is to install taps. Taps are passive devices that are typically "set and forget" devices. Once deployed, you never have to touch them again. After a one-time disturbance to the network to install the taps, you benefit from always-on visibility, resulting in fewer change board approval meetings to gather troubleshooting, monitoring, and security data. This one step gets you better data to reduce your troubleshooting and forensic analysis costs.

Taps are an alternative to the use of switched port analyzer (SPAN) ports. Taps are superior to SPAN ports, primarily because SPAN ports do not provide a complete copy of all network data, and because taps are more versatile and can be deployed anywhere in the network without performance concerns. SPAN port configuration costs, including change board approvals, far outweigh the simplicity and cost of taps.

A visibility architecture is a design that provides access to network traffic, intelligently filters the requisite data, sends the groomed data to analysis tools, and then delivers information from the monitoring tools so that IT can make informed decisions about problem resolution and network performance.

In addition to taps, you will want a network packet broker (NPB) to optimize your filtering methodology. An NPB can provide several features that off-load compute intensive processing from security and monitoring tools. Powerful NPB features include: packet filtering, load balancing, packet deduplication, packet trimming, and multiprotocol label switching (MPLS) stripping.

By filtering data within the NPB, the monitoring tool is freed to perform the work that it was originally purchased to do, resulting in more useful work being done by the monitoring tool. Since the tools are now as efficient as possible, less devices may be required to accomplish the same goals. In addition, the right choice of an NPB optimizes filter programming costs by removing the manual command line interface (CLI) process used in SPAN ports and some NPB models.

Application intelligence is an enhanced feature of network packet brokers which allows them to deliver true signature-based application identification and packet filtering along with the correlation of metadata information like geolocation, user device type, and user browser type. This gives you much more explicit control over exactly what you want to monitor.

By filtering data within the NPB, the monitoring tool is freed to perform the work that it is optimized to do. This results in more useful work being done by the monitoring tool. When all tools are operating as efficiently as possible, you may need fewer tools to accomplish the same goals.

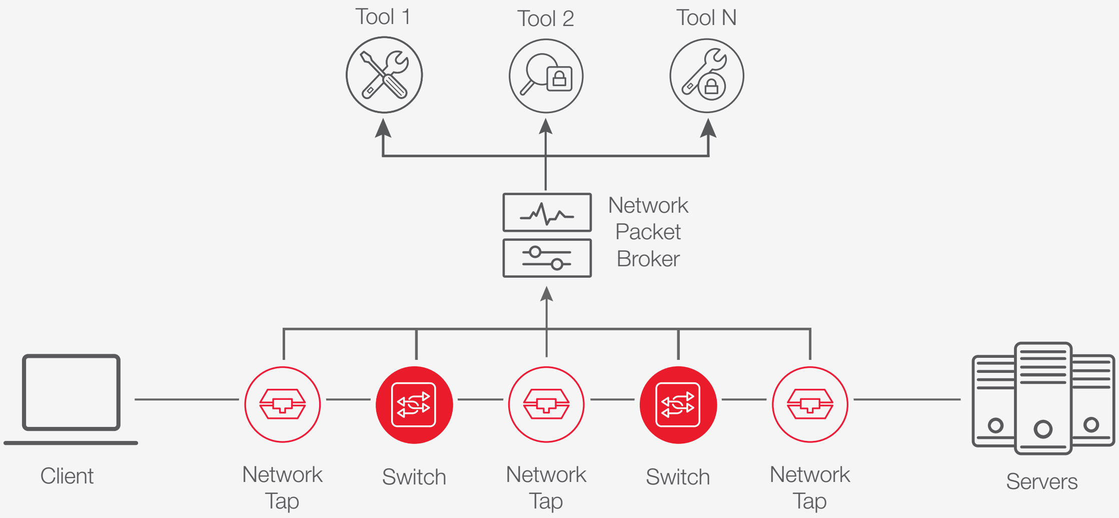


Figure 1. A network packet broker aggregates data from tap and SPAN ports.

If your tools can not consume packet-level data, the packet broker can generate NetFlow metadata and additional detailed contextual information metadata that gives your security and monitoring tools a very optimized set of data to analyze. This means is that your monitoring tools can now be much more intelligent, not just more efficient, and you have access to data and intelligence in a way not possible with other visibility solutions.

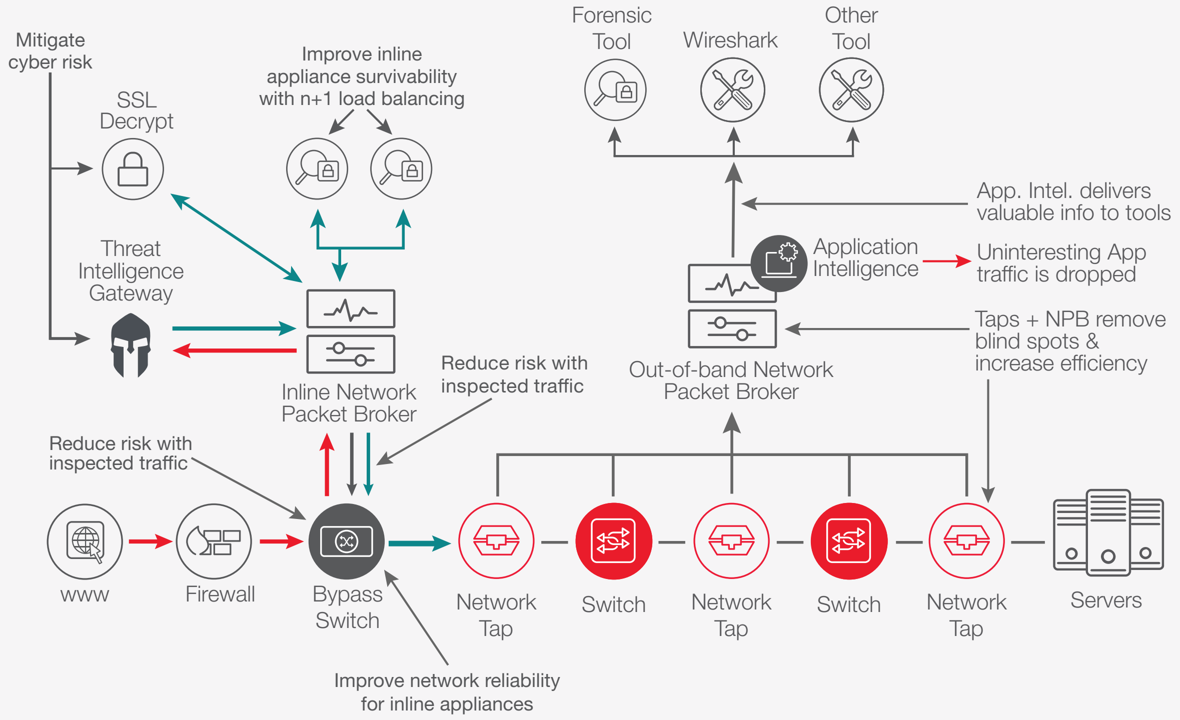
The following sections provide examples of how a network visibility architecture can be integrated into the IT network for several different types of financial industry organizations.

Banking Industry Example

While banking (which includes retail banking, corporate banking, brokerage and capital markets, wealth management and payment services) is obviously a large category, there are some clear shifts happening within this financial segment. These shifts include: a stronger focus on customer centricity, mitigating cyber risk, technology management, staying competitive with Fintechs, and regulatory recalibration. Consequentially, the shifts have fundamental technology implications that CIOs and IT personnel must address if their business is to stay competitive.

From a network visibility and security perspective, there are some easy actions that can be implemented to alleviate these issues. The following diagram illustrates how these technology components can be inserted into a generic bank network.

Deployment of packet brokers can improve monitoring device efficiency 30%. This reduces both analysis cost and CAPEX, and reduces the amount of monitoring tools needed.



Mitigate cyber risk
SSL Decrypt
Improve inline appliance survivability with n+1 load balancing
Forensic Tool
Wireshark
Other Tool
App. Intel. delivers valuable info to tools
Threat Intelligence Gateway
Application Intelligence
Uninteresting App traffic is dropped
Taps + NPB remove blind spots & increase efficiency
Inline Network Packet Broker
Reduce risk with inspected traffic
Out-of-band Network Packet Broker
Reduce risk with inspected traffic
www
Firewall
Bypass Switch
Network Tap
Switch
Network Tap
Switch
Network Tap
Servers
Improve network reliability for inline appliances

Figure 2. Example of network visibility and security solutions for banking.

As Figure 2 illustrates, these are specific benefits from integrating visibility with your network and security architectures:

- **Remove on-premises blind spots** – Install physical taps and packet brokers to get better access to monitor data. This is especially important as bank corporate networks are often spread out geographically with a substantial amount of customer-facing service centers. A well-planned visibility architecture provides the necessary monitoring data while reducing overlaps of unnecessary data.

- **Increase monitoring efficiency** – NPBs can be deployed to remove duplicate traffic and filter the remaining traffic so that monitoring tools only receive relevant traffic. Deployment of packet brokers can improve monitoring device efficiency 30%. This reduces both analysis cost and CAPEX, and reduces the amount of monitoring tools needed.
- **Mitigate cyber risk** – Threat intelligence gateways, inline security tools, and integrated SSL/TLS decryption solutions should be added. Threat intelligence gateways pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30%, helping reduce security event false positives. In addition, inline security tools provide the ability to stop threats in real-time while SSL decryption allows IT to expose malware hidden by SSL encryption.
- **Improve network reliability** – Inline external bypass switches should be added in front of inline appliances to eliminate single points of failure within the network.
- **Enhance customer experience** – A mobile centric world demands optimization of mobile applications and application delivery. Application intelligence within a packet broker can deliver advanced NetFlow formatted data, including geolocation, user device type, user browser type, etc. to aid better application management, monitoring, and troubleshooting across the network.
- **Maximize inline network performance** – Inline performance tools can be added to better understand network performance issues. This is easily accomplished by deploying an inline packet broker which then connects the network performance monitoring appliance to the data it needs.
- **Enhance compliance activities** – For virtual data centers (VDC), a virtual tap can be added to get access to east-west data and then export key virtual data to your physical tools for a consolidated view of your network.
- **Reduce costs** – IT managers should consider a hybrid cloud/on-premises approach where you backhaul monitoring data from the cloud to on-premises NPBs to get a consolidated view and lower costs (by reusing existing physical security and monitoring tools). This could be particularly effective for operations that do not have strict time dependent requirements.
- **Maximize OOB network performance** – Out-of-band performance tools can be added to better understand network performance issues. This is easily accomplished by deploying an NPB which then connects to a network performance monitoring appliance. Application intelligence can also be used to filter data based upon application to better isolate data and enhance tool performance.

Application intelligence within a packet broker can deliver advanced NetFlow formatted data, including geolocation, user device type, user browser type, etc. to aid better application management, monitoring, and troubleshooting across the network.

Insurance Industry Example

Insurance companies also face increasing regulatory pressure as well as cyber threats to enhance network security. One example comes from New York State, where new regulations went into effect on August 28, 2017. These regulations force insurers to adopt specific security practices. In addition to regulation, insurance companies also need to address challenges related to modernization and automation of their security infrastructure.

From a network visibility and security perspective, there are some easy actions that can be implemented to alleviate several of these issues. The following diagram illustrates how these technology components can be inserted into a generic insurance network.

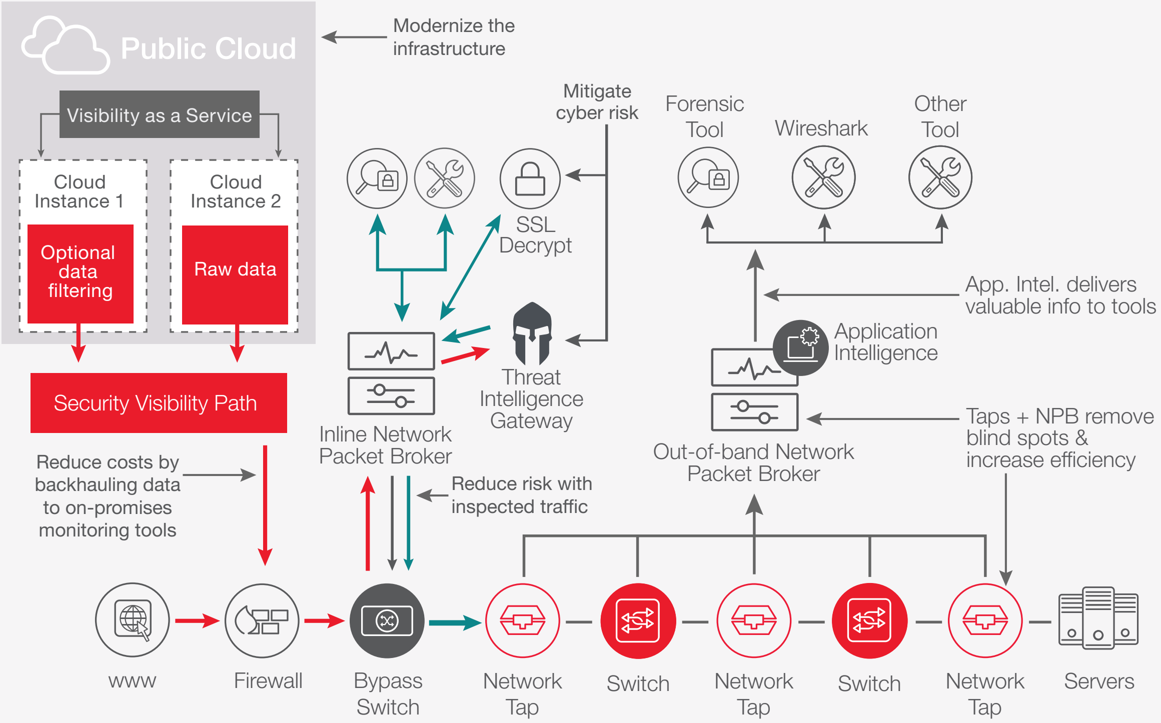

Public Cloud
Modernize the infrastructure
Visibility as a Service
Cloud Instance 1
Optional data filtering
Cloud Instance 2
Raw data
Security Visibility Path
Reduce costs by backhauling data to on-promises monitoring tools
Mitigate cyber risk
SSL Decrypt
Threat Intelligence Gateway
Inline Network Packet Broker
Reduce risk with inspected traffic
Forensic Tool
Wireshark
Other Tool
App. Intel. delivers valuable info to tools
Application Intelligence
Out-of-band Network Packet Broker
Taps + NPB remove blind spots & increase efficiency
www
Firewall
Bypass Switch
Network Tap
Switch
Network Tap
Switch
Network Tap
Servers

Figure 3. Example of network visibility and security solutions for insurance.

As Figure 3 illustrates, there are specific benefits derived from integrating visibility with your network and security architectures:

- **Remove on-premises blind spots** – Install taps and packet brokers to get better access to data. This helps with monitoring, troubleshooting, and compliance efforts. In a virtual data center (VDC), a virtual tap can be added to get access to east-west data which can be exported to your physical tools for a consolidated view of your network.
- **Modernize the infrastructure** – Cloud instances are great for spinning up business critical applications, but there is often limited visibility into cloud data and functionality. IT managers should add a cloud visibility solution to overcome this issue.

- **Reduce costs** – Another consideration is to implement a hybrid cloud/on-premises approach where you backhaul monitoring data from the cloud to on-premises NPBs to get a consolidated view and lower costs by reusing existing physical security and monitoring tools.
- **Mitigate cyber risk** – Add threat intelligence gateways, inline security tools, and integrated SSL/TLS decryption. Threat intelligence gateways pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30%, and to reduce false positives of security breaches. In addition, inline security tools provide the ability to stop threats in real-time, while SSL decryption allows IT to expose malware that is hidden by SSL encryption.
- **Maximize network performance** – Add proactive monitoring to your network to understand performance issues and test cloud software updates before they go live.

Credit Card Industry Example

The credit card ecosystem faces many challenges, including in-store fraud, online fraud, and many forms of cyber-attacks. While a natural response would be to severely tighten online and digital access, the consumer market is demanding even more digital access with electronic wallets and faster 'tap and go' credit card access techniques. This requires technology and architecture improvements to keep the network secure.

From a network visibility and security perspective, there are some easy actions that can be implemented to address these issues. The following diagram illustrates how these technology components can be inserted into a generic credit card network.

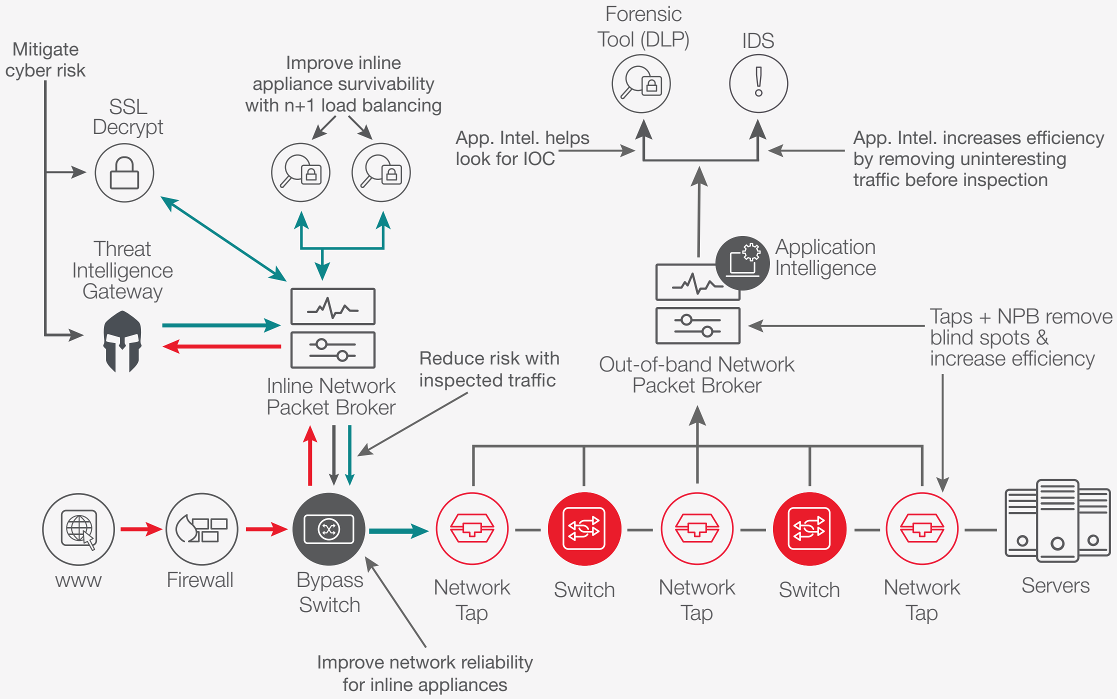

Mitigate cyber risk
SSL Decrypt
Improve inline appliance survivability with n+1 load balancing
Forensic Tool (DLP)
IDS
App. Intel. helps look for IOC
App. Intel. increases efficiency by removing uninteresting traffic before inspection
Threat Intelligence Gateway
Application Intelligence
Taps + NPB remove blind spots & increase efficiency
Reduce risk with inspected traffic
Inline Network Packet Broker
Out-of-band Network Packet Broker
WWW
Firewall
Bypass Switch
Network Tap
Switch
Network Tap
Switch
Network Tap
Servers
Improve network reliability for inline appliances

Figure 4. Example of network visibility and security solutions for credit cards.

As Figure 4 illustrates, these are some of the specific benefits from integrating visibility with your network and security architectures:

- **Remove on-premises blind spots** – Install taps and packet brokers to get better access to transaction data. This helps with troubleshooting and compliance efforts. For a VDC, a virtual tap can be added to get access to east-west data and export key virtual data to your physical tools for a consolidated view of your network.
- **Strengthen network security** – Add application intelligence to your secure area as a warning system for indicators of compromise (IOC). For instance, secure credit card transaction processing areas only have a few applications running. Have application signatures created for those trusted applications. Then run continuous monitoring with the NPB, using application intelligence within that zone to monitor for any unknown application signatures. If unknown signatures appear at any time in the future, there is a high probability this is an IOC.
- **Improve network reliability** – Add inline external bypass switches to eliminate single points of failure within the network.
- **Mitigate cyber risk** – Add threat intelligence gateways, inline security tools, and integrated SSL/TLS decryption. Threat intelligence gateways pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30%, and help reduce false positives from security events. In addition, inline security tools provide the ability to stop threats in real-time while SSL decryption allows IT to expose malware that is hidden by SSL encryption. SSL decrypted data can be fed to an intrusion prevention system (IPS), web application firewall (WAF), or data loss prevention (DLP) tool for inspection.
- **Maximize security appliance availability** – An NPB deployed inline can be used to load balance data across multiple tools. This provide n+1 survivability (all the way up to full redundancy) for inline security tools. Fail-over and fail-back processes are automated for maximum survivability. An n+1 approach can be a very cost-effective alternative to full redundancy.

Threat intelligence gateways pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30%, and help reduce false positives from security events. In addition, inline security tools provide the ability to stop threats in real-time.

Financial Trading Services Example

Financial trading services companies are extremely sensitive to technology changes and need to constantly re-evaluate their use of new capabilities. Just one millisecond of unnecessary delay can cost the company, and their clients, millions of dollars. Deploying proven, cutting-edge technology lets the company maximize financial trading performance, deliver better services to their clientele, and maintain a strong security posture.

The following diagram illustrates how network visibility technology components can be inserted into a generic financial trading network to address the unique challenges of high speed trading organizations.

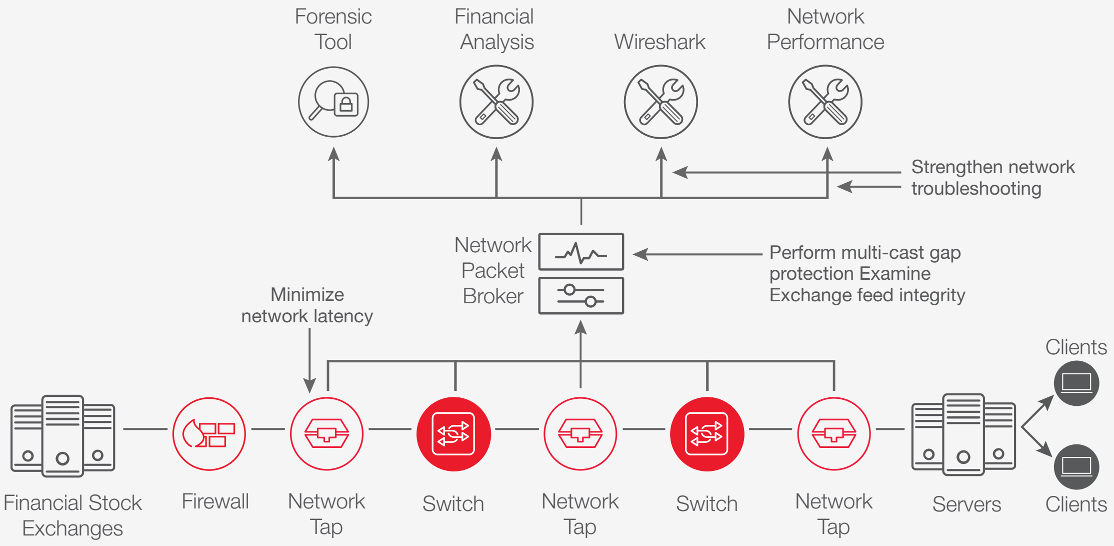


Figure 5. Example of network visibility and security solutions for trading.

As Figure 5 illustrates, these are some of the specific benefits from integrating visibility with your network and security architectures:

- **Minimize network latency** – Install taps where you need monitoring data access (ingress, correct, trading floor) to validate the service level agreement (SLA) for transmission time from trading exchanges. This allows you to monitor and optimize the financial trade speed and latency.
- **Reduce trade latency times** – Install purpose-built NPBs that offer multicast gap protection to improve problem identification and determine if the company is trading behind the market (which could be costing the business money and upset its customers). This is used to determine if there is lost or out of sequence data. The NPB can look into the packet stream, perform deep packet inspection to look at sequence numbers (inserted by the trading exchange) and identify if packets are coming out of order. If so, the receiver company can ask the exchange to rebroadcast that missing data. Purpose-built financial monitoring tools can perform this as well but that is akin to driving a Rolls Royce car to perform simple errand like grocery shopping. Those tools add more value performing data analytics versus performing DPI for out-of-sequence packets.

- **Improve exchange feed reliability and integrity** – Install purpose-built NPBs to get better access to monitoring data to quickly discover traffic feed health. The solution provides a traffic indicator so that you can see if the link is up or down and if the data within the feed is correct. For instance, an exchange (like NASDAQ) sends out heartbeat messages but this is only useful to determine if the link is up or down, not if the data within the feed is being correctly transmitted. An NPB can look at both types of data.
- **Strengthen network troubleshooting** – A purpose-built NPB delivers detailed traffic statistics by feed. Typical traffic statistics and NetFlow data do not include specific data on every feed from an exchange. This solution provides the detailed information with link ID (e.g. link A, B, and E are working but link C and D are not) and the statistics data. This data can then be used natively within the NPB or exported to an external monitoring tool. Threshold alerts can also be set to get an early warning of problems.
- **Mitigate cyber risk** – Add threat intelligence gateways, inline security tools, and integrated SSL/TLS decryption. Threat intelligence gateways pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30%, and reduce false positives from security events. In addition, inline security tools provide the ability to stop threats in real-time while SSL decryption allows IT to expose malware that is hidden by SSL encryption. SSL decrypted data can be fed to an intrusion prevention system (IPS), web application firewall (WAF), or data loss prevention (DLP) tool for inspection.

The NPB can look into the packet stream, perform deep packet inspection to look at sequence numbers (inserted by the trading exchange) and identify if packets are coming out of order. If so, the receiver company can ask the exchange to rebroadcast that missing data.

Conclusion

The financial industry is experiencing a massive wave of digital disruption. To stay competitive, these companies will have to innovate to stay ahead. On the security front, they can address the changing landscape by deploying new and adjusting existing technologies. One such area ripe for improvement is network visibility and monitoring technology.

Organizations can maximize the usable data they gather through the following:

- Deploy taps and NPBs to collect the proper monitoring data and to refine that data so that it can be processed into information as fast as possible
- Deploy threat intelligence gateways to immediately eliminate traffic from known bad sites
- Deploy inline bypass switches to increase network reliability
- Deploy inline NPBs, decryption and security tools to respond to cyber threats and minimize both risk and cost
- Use application intelligence to filter data for security and monitoring tools more efficiently
- Use application intelligence to proactively look for indicators of compromise
- Deploy NPBs to reduce costs by using load balancing, deduplication
- Capture cloud data and back-haul it to on-premises equipment and tools to reduce cost and improve compliance

Ixia network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. For more information on network monitoring solutions, visit www.ixiacom.com/solutions/network-visibility.

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