Understanding the Needs of Today's Financial Networks

Good Decisions Reduce Risk

The financial industry is at the forefront of network technology. The traditional image of bankers and financial traders is really an anachronism. The reality is that the financial industry, from retail banking to high speed trading, is at the cutting edge of network innovation – for better or for worse. Whether adopting new technologies to allow customers broad-based mobile access, squeezing out the last few nanoseconds of latency, or providing air-tight security, network and IT leaders are always looking for newer and better advantages.

New technology has pitfalls as well. Like the popular image of the banker, the gun-wielding bank robber is equally anachronistic. Bank robbing is now an ultra-sophisticated cybercrime, where highly-organized syndicates leverage their own technology and the ever-growing complexity of networks to their advantage. Sophisticated network equipment and topologies can lead to complex and slow fault-finding processes and times.

Good decisions require good data

These factors place enormous pressure on network and IT groups, who face growing difficulties due to:

- Increasing technical complexity.
- Increasing rates of technology change and adoption
- Increased frequency and sophistication of cyber attacks
- Increased pressure to make the right technology "bets"
- Increased expectations from users (and investors) for access and quality of experience
- Increased instances of performance, stability, and security issues (often found festering in "blind spots")

As any trader will tell you, you can't completely eliminate risk. But you can greatly mitigate it by having the best possible information – better data yields better decisions. With better information you can:

- Legitimize vendor claims so you can make the right technology bets
- Optimize technology roll outs, application performance, and network availability.
- Take the guesswork out of network security performance and resilience.
- Elimtinate blind spots in the network by implementing end-to-end visibility
- Provide operators with actionable insight by maximizing the use of network tools.

The combination of Keysight's network testing and network visibility solutions provides a unique network partner that can ensure your financial network at all stages – from design, to deployment, to production.

Legitimize Vendor Claims

Data sheets can lie

Most vendors are not dishonest, but their goal is to get you buy their solutions rather than those of their competitors. So it's no surprise that they "accentuate the positive" and present the best-case scenario for a product's functionality, performance, and stability.

Most IT departments that are evaluating solutions attempt to mitigate "best-case promises" through live demonstrations and proof-of-concept tests. However, these evaluations are often limited in scope and rarely provide anything approaching a real world assessment. The

fact that they are done in isolation and under vendor control often means they won't accurately emulate the complex interactions with other devices, systems, and users that you find in a "live" network.

Further, these evaluations rarely provide a true "apples to apples" comparison among multiple vendors. It is difficult to get a vendor to give up the necessary control in order to fully test their product – in unpredictable conditions, with unforeseen traffic patterns and types, and while under attack from malicious software.

What all of this means is that the data available for making networking decisions is often suboptimal – a risky proposition for such a high-stakes bet.

A truth serum for data sheets

Keysight Resiliency Score, originally developed by Keysight's BreakingPoint™ team, provides repeatable, comparable measurement of performance, security, and stability of physical network devices.

The resiliency score tests for performance and security with real-world traffic mixes. It gives a numeric grade from 1-100, providing a common basis for comparison between vendors. This enables you to make that comparison based on your network's actual traffic profiles and load (instead of using a contrived and limited mix). The resiliency score also works when comparing physical appliances to virtualized network unctions to help ensure that network functions virtualized (NFV) rollouts are properly resourced and tuned.

Case study: optimized vendor selection

AA major credit card company needed to scale and redesign their access network infrastructure to cope with an ever increasing volume of mobile users. Their goal was understanding if they could replace incumbent IPS devices with next-generation firewalls. The company had firsthand experience with vendors not meeting their scalability claims, providing only best case performance numbers, and/or not providing scalability numbers for the specific application mix and network design that would be deployed.

With the help of Keysight, and an investment in Keysight's BreakingPoint, they were able to validate the new network and security architectures being implemented to support their future strategic initiatives. The company used Keysight to help them:

- Validate various design options
- Compare device features and performance.
- Ensure that security devices were tuned correctly and could properly detect the latest attacks (and DDoS) under a variety of loads.
- Accurately recreate production traffic with real stateful applications and inject adverse conditions

The result was a highly optimized vendor selection process that has all but eliminated insecurity in the selection process. Using Keysight's Resiliency Score, they can now be confident in their network selections.

The Network Is the Business

The high price of outages

In September of 2013, U.S. options trading was halted due a problem with a data feed that supplied prices to traders.According to the Wall Street Journal, the outage affected the trading of options based on stocks, exchange-traded funds, currencies, and other asset classes. In addition to prevented trading, a relatively small number of trades were canceled as result of the issue. This brief episode impacted or prevented billions of dollars worth of trades in the space of minutes. In this case, the outage impacted the market equally – for better or for worse. When an individual bank or trading firm suffers a network issue or outage, only their customers suffer – along with the company's reputation and bottom line (not to mention the possible impact on the network and IT teams' job security). With increasing certainty, the network is the business of the financial industry – and Keysight is in the business of network optimization.

Optimizing network performance

Operating and optimizing the network used to be like flying old monoplane, single-engine aircraft. It took some training and specialized skills, but once you had the foundation it was pretty simple. Just adjust the yoke, pedals, rudders, and flaps to control the plane's altitude and direction.

Today's networks, however, are more like jet fighters than traditional aircraft. Not only do they take a team of educated and trained specialists to maintain, but the simple adjustments that control direction

have been replaced by complex, interwoven systems. A myriad of calculations and interactions take place as result of seemingly simple surface changes.

Keysight helps companies tune their networks with a full suite of solutions that can test, emulate, monitor, and optimize modern networks and data centers. This allows them to better manage ultra-complex data centers.

Use Case: Stress Testing Trading Infrastructure

A major global investment bank was concerned with how their trading infrastructure could cope with sudden changes in trading volumes and market data. They were worried that sudden market events might lead to trading infrastructure saturation – resulting in delayed orders

Keysight provided a solution to that allowed the bank to generate test traffic at varying data rates to simulate varying traffic profiles. Keysight's Application and Threat Intelligence (ATI) solution has built-in signatures that support a variety of order entry protocols such as FIX and ITCH, as well as market data feeds. Using the ATI, the bank was able to successfully test the capabilities of key networking and system components without having to deploy expensive and difficult-to-support real trading servers and applications.

The bank is now able to test against changes in market conditions, tools, applications, or global events to ensure that their network is finely tuned to meet the needs of the business regardless of changing external or internal conditions.

Take the Guesswork Out of Network Security

How do you know if your network security is working?

If your CEO asks how you know if the network is secure, how will you answer?

- We have not been breached
- We passed our audit
- We apply the most recent updates and signatures
- We do regular vulnerability scans or assessments
- We perform annual penetration testing
- Our network has not gone down
- I still have my job

If the answers above are the only ones you can give, then unfortunately you are no better off than the several companies who suffered devastating security breaches over the past two years.

Don't guess...know

In today's world of hyper complex systems and everchanging arrays of attacks and defenses, the only way to answer this question in the affirmative is:

Because we tested it

This used to be a daunting task, but now there is an easy, affordable, and highly repeatable method of testing products, solutions, and production networks – with fully loaded application traffic that is customized to your environment. This traffic can be injected with DDoS, malware, and other exploits so that you know for sure how your actual network defenses will respond. Further, these application and attack scripts are updated on a bi-weekly basis to ensure you are always hardened against the latest attacks.

Case study: real world DDoS validation and response

A progressive trading group was particularly concerned about DDoS attacks after observing real service delivery and impact during a volumetric DDoS attack. Since the company was paying a DDoS cloud mitigation service provider $250,000 per month for this service, the level of confidence they had with their effectiveness at stopping DDoS attacks while not denying legitimate user transactions was quickly deteriorating. They needed a real method of understanding the resiliency of their DDoS mitigation service provider.

Keysight's BreakingPoint solution was able to uncover a flaw in the data center workflow of DDoS attack defenses, showing that the DDoS attack mitigation initiated by the DDoS service provider was blocking legitimate user traffic. By simulating a DDoS attack under loaded conditions, the Keysight attack revealed an internal network infrastructure (core router) failure in the service provider network, within the first hour of launching the attack

61% of CIOs and CISOs believe the scope and complexity of IT security make it difficult for their organizations to assess their DDoS mitigation service provider.

Mobile Users Do NOT Compromise

There was a time when users who adopted new technologies would accept compromises in quality of experience or performance (and even security) for the added convenience that new technologies (such as online banking or mobility) afforded them. Those days are gone. In the world of credit cards and retail banking, having a resilient and high-performance mobile access product is not just a "nice to have," it's a critical part of a growth strategy. A poorly performing mobile app can lead to customer frustration, dissatisfaction, and loss of market share.

Meeting the needs of mobile clientele

Despite the explosive growth we've seen in mobile data usage over the past five years, the requirements for mobility are increasing. According to a 2014 study from Cisco Systems, "Traffic from wireless and mobile devices will exceed traffic from wired devices by 2016. Business IP traffic will grow at a CAGR of 18% from 2013 to 2018."

This increased usage points out a need to understand how the network will respond to a variety of mobile users, devices, and applications. Network operators must account for the impact of growth in terms of the mobility of applications, servers, and data within and among data centers. Additionally, they must account for the impact of network advancements such as the virtualization of firewalls, load balancers, core routing, and switching.

The importance of user quality and security, and its impact on customer retention, are too important to be left to ad hoc testing and optimization.

Case study: leading global credit card company – mobile access testing

A leading global credit card company takes the rollout of new applications very seriously, and needed to fully test new applications and enhancements before they are launched. Historically their applications were tested in a fairly ad hoc manner, but the increasing importance and wide variety of end user devices meant that this was no longer possible.

A more rigorous approach was necessary. They needed to know exactly how new application rollouts would affect their mobile network, to ensure no negative impact on end users.

Keysight provided a solution based around IxVeriWave™. IxVeriWave allows the credit card company to automate testing processes and ensure that testing is repeatable and consistent. This ensures a smooth rollout of new capabilities and applications that can be accessed over wireless and Wi-Fi networks. As an added benefit, IxVeriWave reduces the test times from months to weeks (or days) – reducing the application or service time-to market. This means the credit card company can offer improved services to its customers regularly, without degrading their quality of experience (QoE).

IxVeriWave helped the credit card company:

- Validate various design options
- Compare device features and performance
- Accurately recreate production traffic with real stateful applications and inject adverse conditions.

Bad Things Happen in Blind Spots

Take a look at the reports on any number of data breaches, network outages, or other major network problems and there is one thing you won't see: someone saying, "We saw this coming." This is, of course, not surprising. If the networking teams had noticed a problem or an emerging threat, they would have dealt with the matter before it became a problem (and public).

Most problems catch teams by surprise because they emerge from "blind spots" – those places you can't see and parts of the network that escape notice. Blind spots are a result of increased network complexity, and it's in these blind spots that problems fester and where cyber criminals ply their trade.

You can't control what you can't see

Keysight helps eliminate blind spots in the network by getting the right information to the right tools at the right time, greatly improving performance, QoE, and security. Our industry-leading Visibility Architecture includes physical and virtual taps, bypass switches, and full-featured network packet brokers. These solve network visibility needs – from single-point solutions to large-scale enterprise and service provider network deployments.

Keysight's Visibility Architecture also extends the life of existing tool investments and maximizes current tool capacity. This is accomplished by filtering and metering out-of-band monitoring traffic, and by delivering intelligent, user-contextual data, rather than raw packets. The Visibility Architecture provides

network visibility that that is scalable in every sense of the word: product, portfolio, design, management, and support.

Case Study: Global Investment Bank Standardizes Monitoring Infrastructure

A major global investment bank needed to monitor its trading infrastructure in over 30 locations around the world. They needed to access order entry and market data at varying points in each location. The bank had major concerns using SPAN ports on switches as the monitoring data source, due to change control issues and the fact that the SPAN ports themselves may be the cause of packet drops – leading to errors in their monitoring tools. A single packet dropped out of millions of packets sent on high-speed data feeds can easily lead to multicast gaps occurring many times per second. The bank was also concerned over using fiber taps. They had multiple fiber types in each location and could not spare the space in the expensive colocation centers necessary for multiple fiber taps. Keysight proposed a solution based on the Keysight Net Optics Flex Tap™.

This industry-changing design allows up to 24 fiber taps in a single rack mount unit and gives the option for the bank to "mix and match" a wide variety of fiber taps (split ratios, fiber types, and speeds) to meet the specific needs of the local data center and trading infrastructure. The bank adopted the Flex Tap as their standard way of accessing critical markets on a global basis due to the tap's flexibility and small form factor. Their network visibility was further enhanced with the Net Tool Optimizer™ (NTO) solution, which provides a scalable, easy-to-configure and manage solution for global network visibility. Not only does the solution eliminate blind spots, but it ensures that networking tools get optimized.

The Need for Speed

Seconds don't count. Nanoseconds do. The race to deliver low latency trading and banking transactions continues. Financial organizations are vying for unrivaled speed, accuracy, and security within the network. Understanding network performance and how trading applications react under real-world conditions provides an edge over competitors. Dropped packets lead to increased latencies and incorrect trades – or even compliance issues.

Worldwide, those responsible for trading network infrastructure in financial organizations are adopting comprehensive strategies for measuring and minimizing latency and infrastructure quality "door-to-door" before, during and after deployment. They're turning to Keysight for the broadest, most accurate array of testing products and services needed in vendor selection, design, and deployment of ultra-low-latency LANs, WANs, WLANs, and virtualized web- and cloud-based services.

The company must minimize latency and packet losses, from quote reception and order entry to the completion and settlement of trades. To achieve this, trade plant engineering and operations must understand how the performance of networks, links, devices, and applications affects users. This means modeling and measuring performance using simulated and real traffic – in both live environments and stressful test lab scenario.

Data feeds

Rapidly detecting degradation in the quality of data feeds is a considerable challenge for any market participants who use or transport real time market feeds. Market data transport technology is primarily

based around the use of multicast, which does not have any error correcting mechanisms at the network layer. This means that any packets containing key trade data that have been lost cannot be detected until they are passed through a feed handler system at the end user site. This has a number of issues:

Application teams may be aware of the problem, but the tools they use may not be available to the network operations teams who are responsible for diagnosing and resolving the issue.

Many feed handlers use feed arbitration (between A and B feeds) to autocorrect message drops, so application teams may neither be aware of problems nor able to quickly passon details to their network operations teams.

Detecting a problem at the feed handler does not tell you where the problem occurred. Was it a problem with the Exchange or market data vendor's ticker plant? Was it a problem in their internal network? Was there a problem in the third-party network carrier or extranet provider used to transfer the market data? Was there a problem in a firewall? Was the problem in the end user's internal network?

All these questions lead to slow decision-making and long fault repair times that can be measured in days and not minutes.

Much of the technology used to monitor this infrastructure today is either not up to the task or involves expensive data capture, storage, and analytic technologies that have remained more or less the same for twenty years. These technologies are expensive, and consume valuable power and real estate within expensive data centers.

Case study: global hedge fund – monitoring of inbound market data feeds around the world

A global trading company with operations in Asia, North America, and Europe has trading infrastructure in 10 colocation hosting facilities around the world. With its sophisticated trading algorithms, it is a leading player on many of the equities and derivatives Exchanges worldwide. Having access to low latency market data is key to their trading – any faults in inbound market data must be rapidly identified and fixed.

Although in-house tools had been deployed to monitor feed performance, the number of locations and trading venues around the world meant that an undue amount of technical time was being spent on maintaining these tools rather than on deploying new and more effective trading infrastructure. They needed a tool that could monitor their inbound market data feeds and support their wide variety of active Exchanges (without major involvement from the Exchanges).

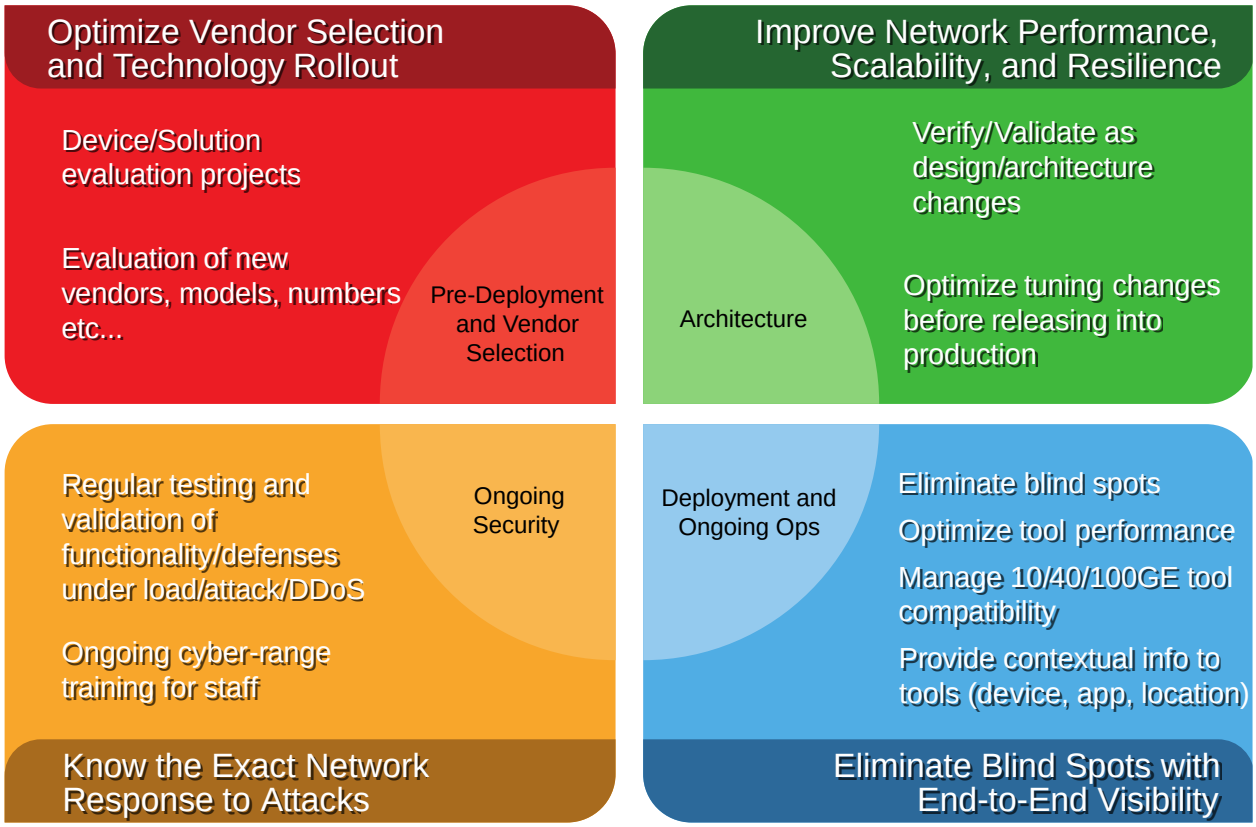
The solution was TradeView™. Keysight's TradeView product allows them to cost-effectively monitor their inbound market data feeds for micro-bursts and multicast gaps, and allows them to reallocate engineering resources to more profit-generating activities.

Keysight Reduces Risk and Optimizes Your Business

Keysight is a leader in assessing, validating, monitoring, and securing today's financial networks. With Keysight solutions, you can be confident that your network technologies, deployments, and security are working at their highest efficiency. Keysight delivers the actionable insights into what you need to do and how you can react in order maximize your network's potential.

Keysight has worked with most major global investment banks, 11 out of the top 15 tock exchanges around the world, and eight of the world's top high frequency traders.

Keysight is a world leader in infrastructure testing, and our flagship IxNetwork and IxLoad products are used worldwide. Our BreakingPoint security products are recognized throughout the industry as a leading, goto technology. With Keysight's Visibility Architecture, which includes the Net Tool Optimizer (NTO) and Keysight Net Optics tap products, our network monitoring solutions give you actionable insights, allowing your monitoring tools to provide the best and most useful data about what is happening in your network.



Our revolutionary TradeView feed monitoring product gives a unique insight into the quality of trading critical, real-time market data feeds.

Keysight's testing solutions, security assessments, and Visibility Architecture work together to help network and IT groups reduce risk in your network and optimize your applications and services so that your customers will receive the highest quality of experience.

The combination of Keysight's network testing and network visibility solutions provides a unique network partner that can ensure your financial network at all stages – from design, to deployment, to production.

With Keysight, you can:

- Improve network performance, scalability, and resiliency
- Legitimize vendors' claims and optimize your network planning
- Secure your network by knowing exactly how it responds to malicious attacks
- Eliminate blind spots with end-to-end visibility

Visit Keysight at www.keysightcom.com to learn more about our financial market networking solutions.

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