WHITE PAPER

How To Mitigate Five IT Problems Affecting The Financial Industry

IT Challenges For Financial Services

The financial services industry is no stranger to risks and challenges. With the rise of fintech in a new world of digitization, financial services organizations have been suffering from five major IT challenges in the past several years that include:

- How to minimize security breaches
- Reducing cyber theft
- Using technology to improve overall performance
- Improving compliance to regulatory mandates
- How to use technology to provide a competitive advantage

Constantly changing technology for the financial industry has brought new challenges along with opportunities, exposing organizations to cyberattacks and high-impact security risks.

Technology has always played a key role in the financial sector. Notwithstanding tough competition, recessions, and new regulations, constantly changing technology for the financial industry has brought new challenges along with opportunities, exposing organizations to cyberattacks and high-impact security risks. As an example, the recent cyber theft from Tesco Bank illustrates that traditional approaches to security are not working or that companies are not taking the threat seriously enough. In this case, Tesco Bank halted online banking after 40,000 current accounts were compromised and half of those were hit by fraudulent transactions by hackers during a single weekend. Although the bank

KEYSIGHT TECHNOLOGIES

promised to cover all losses, shares in Tesco dipped 1% amid predictions that the brand could be damaged by the security breach, according to the BBC.[1]

The challenges for IT are not restricted to security alone. Although financial institutions deal with recurring issues every year, they now operate in a new economic, digitized, and transformational environment after the financial crisis. According to a PwC CEO Survey, nearly 60% of industry leaders view the speed of technological change as a threat to their growth prospects.[2] Some of the dynamic technological shifts require financial institutions to quickly adapt to new and next-generation platforms, mobile banking and robust cyber security. Outdated core IT systems are a significant concern for global bankers. These typically translate into lack of proper network integrations and creation of blind spots as disparate corporate data networks trying to communicate with each other do not transmit data correctly. Blind spots are areas where IT does not have complete visibility into what is happening on the network or how applications are behaving.

Failure to invest appropriately in secure, agile systems that can enhance digital and mobile banking can result in significant loss while compounding the risk for cyber attacks.

Failure to invest appropriately in secure, agile systems that can enhance digital and mobile banking can result in significant loss while compounding the risk for cyber attacks. Additionally, banks face serious competition from a host of disruptive innovators who are able to provide customers with seamless and more affordable experiences across a variety of channels.

Success for these institutions are highly dependent on how they take advantage of these technology innovations. This includes visibility into potential network and application problems as a result of the new technology and the ability to improve the performance of the network. Network visibility and testing solutions are available to help overcome these challenges. The secret is to eliminate network blind spots, perform key network assessments, and harness technology. In this white paper, we will explore how a visibility architecture and your network validation solutions can be integrated with your network and security architectures to maximize network defenses and performance.

Minimizing Security Threats

Improving network security is important for all businesses, particularly for the financial industry. If consumers and other businesses cannot trust you with their money, then you are wrestling with serious business setbacks.

There is no doubt that keeping up with technological innovation presents a challenge by itself. Media reports have indicated that America's Financial Industry has been, and continues to be, highly susceptible to data breaches. For instance, according to SecurityScorecard's 2016 Financial Cybersecurity Report[3], 75% of the top 20 U.S. commercial banks (by revenue) are infected with malware.

[1] Tesco Bank theft shows need to take cyber security more seriously

[2] Top Issues Facing the Financial Services Industry

[3] America's Financial Industry Highly Susceptible to Data Breaches

Findings from the report implied that:

- The U.S. Commercial bank with the lowest security posture is one of the top 10 largest financial service organizations in the U.S (by revenue)
- Only one of the top 10 largest banks, Bank of America, received an overall 'A' grade
- 95 percent of the top 20 U.S. commercial banks (by revenue) have a Network Security grade of 'C' or below
- 75 percent of the top 20 U.S. commercial banks (by revenue) are infected with malware and a number of malware families were discovered within these banks, including Ponyloader, and Vertexnet
- Nearly 1 out of 5 financial institutions use an email service provider withsevere security vulnerabilities

To combat such threats, financial networks need to understand they ARE being targeted and need to maximize their security defenses.

To combat such threats, financial networks need to understand they ARE being targeted and need to maximize their security defenses. How, is the question. Combating these security breaches can be tackled through different approaches.

The IT department within financial organizations can improve their security solutions by deploying bypass switches and inline network packet brokers (NPBs) with heartbeat technology. Inline refers to the fact that the device is directly in the flow of traffic rather than receiving a copy of the traffic, which is called out-of-band. The inline NPB is used with inline tools like intrusion prevention system (IPS), firewalls, threat prevention systems, SSL decryption/encryption techniques, etc. Together, this solution gives you the maximum availability of the tools so they can process suspicious data.

It is also important to implement High Availability and load balancing for your security tools. These two features can dramatically improve network availability. High Availability (n + n) provides maximum resilience against failure by having a completely duplicate set of NPBs and tools to process traffic, should one set fail. For many customers, failover is required as uptime is a key driver. Load balancing across tools provides a similar but much more cost-effective version of this as you do not have to have a fully redundant set of equipment. In this case you can have one or more tools that are over-dimensioned to share the load. Should one device go down, the rest can handle the load. This type of system is dimensioned as n + 1 all the way to n + n, depending upon the total number of tools and NPBs deployed. A load balancing configuration can be very useful if your intrusion protection system (IPS) does not support clustering and exchange state information.

Data retention is another one of the main challenges within forensic security projects. This is due to the relatively high cost incurred by the financial institution to allocate a huge storage capacity for the captured network traffic. An out-of-band NPB has demonstrated a tremendous reduction on the solution's overall cost by filtering out unimportant traffic before sending it to the forensic probes like data loss prevention (DLP) tools for processing and storage. The filtering process results in a remarkable reduction of the storage requirement for data retention.

Another capability is the deployment of threat prevention systems that screen traffic based upon IP address. They can be used for both black listing and white listing architectures. Threat prevention systems (with automated updates for known bad IP addresses) can help protect against various security threats (malware, ransomware, DDOS, etc.) by preventing inbound and outbound communications to and from those bad IP addresses. The automated updates help keep systems as up to date as possible, since bad actors change IP addresses frequently so they can launch new threats. The alternative is to use firewalls with access lists but the updates to those access lists are usually a manual process, which can have significant delays between updates. This translates to more vulnerability and risk.

An often overlooked action is to thoroughly test your security architecture before you rollout new updates. This is not as difficult as it sounds. All a security architect needs to do is to create a lab environment that mimics the security architecture. After that, a test solution (like the Keysight BreakingPoint product) is installed into the lab. The test solution can then run automated test scripts with a combination of application load and malicious traffic to see how the solution performs against various threats (malware, DDOS, etc.) and configuration errors before general roll out. The last thing you want is self-inflicted injuries from network and security architecture changes.

Uninspected emails could be carrying links to malware like ransomware.

For high security environments, application intelligence can be used to create a "safe zone". In this safe zone, the number and types of applications are limited. Signatures can be created for the approved applications. Once this is done, application intelligence can be used to constantly monitor the environment to make sure that there are no unauthorized applications, which would probably be security threats, running in those environments. An example would be a credit card load approval process that has maybe five different applications running in the protected environment. If any other application traffic is discovered, it can be quickly analyzed to determine location and source.

Application intelligence can also be used to identify applications running on the general network that should not be there. This could be important if web-based email applications are being used to circumvent your stated email security policies, like the general anti-virus, anti-malware inspections of the normal email system. These uninspected emails could be carrying links to malware like ransomware.

Solution Options

- Use an NPB to improve the availability of inline security tools to prevent breaches
- Implement High Availability and load balancing for security tools with an NPB
- Use an NPB to improve data retention policies for suspect data analysis and low storage costs
- Test security solutions to prevent self-inflicted injuries from network and security architecture changes

Reducing Cyber Theft

Even though bank revenues have increased over the last several years, cyber theft is top concern for banks and other financial institutions. Your customers envision banks as a fortress that protects their money. If that myth is shattered, then the need for a bank quickly unravels in their minds. This is one of the reasons that cyber theft from banks is severely underreported, as evidenced by data gathered the City of London Police.[4] Speaking at a TechUK conference Adrian Leppard, commissione of City of London Police, said cyber criminals are stealing more money online—but banks are not reporting the full extent of the theft. He said only one in five cyber crimes is reported. Of those, only another one in five provoke a proper response from law enforcement agencies. 2014 saw a 48% rise in the amount of money stolen from UK online bankers[5] as criminals pilfered more than £60m through a total of 53,192 incidents.

Cyber theft is a top concern for banks and other financial institutions.

Since financial data is one of the most appealing targets for hackers, institutions need to remain extra vigilant about cybersecurity and watch for indicators of cyber theft and ransomware.

An NPB can help aggregate data from various taps and SPANs and direct the right data to out-of-band (IDS, SIEM, DLP) security tools. Out-of-band tools can be especially useful in looking for transaction trends that are indicative of fraud.

[4] Banks hide cyber crime losses, says City of London police
[5] UK online banking fraud sees big increase

NPBs can also be used to assist in data storage, should a backup of data be needed. The NPB can make a copy of select data types, or all data types, and pass that data to a recording tool for long term storage of data.

Solution Options

- Use an NPB to capture data and send that data to out-of-band security tools for inspection
- Use NPBs to replicate data and send it to a SAN for storage

Using Technology to Improve Overall Performance

For financial trading organizations, delays in trades will cost your customers, and you, money. These types of transaction are ultra time-dependent. How can you really minimize this trading latency though? It comes down to your network and visibility architecture. To enable new technology benefits, the network has to be working at peak performance. Undetected issues result in internal and external customer complaints. And unfortunately for IT, the MTTR clock starts ticking whether they know there is an issue or not. The hardest part of the process is determining what the issue is. According to Zeus Kerravala, Principal Analyst at ZK Research asserts that, “Problem identification is IT’s biggest challenge.” He explains that 85% of mean time to repair (MTTR) is the time taken to identify there is in fact, an issue.[6] This is where deploying the right visibility architecture will help.

> Problem identification is IT’s biggest challenge. 85% of mean time to repair (MTTR) is the time taken to identify there is in fact, an issue.
>
> —Zeus Kerravala

As a best practice, IT engineers usually start with deploying taps to capture data at key points within the network. This allows you to test incoming delay as well as internal (roundtrip) delay for trades. A useful integration at this point is the NPB which can aggregate the data and deliver it to network impairment analysis tools. A specially configured NPB (like the Keysight TradeVision solution) can deliver superior data filtering and traffic statistics resolution down to 0.1 millisecond for up to 300 market feeds. A full featured NPB can also detect multicast sequence gaps and microbursts.

Some financial institutions need to monitor their financial trading applications for performance details. While some current solutions can monitor latency down to a level of milliseconds, this usually is not good enough. Microsecond and nanosecond level latency details are needed to offer a superior solution. This necessitates the need for timestamping. In addition, timestamping solutions of up to 40 GB line rates are often required now.

[6] IxVision - Eliminating Visibility and Security Blind Spots

Network impairment analysis tools (often deployed inline with a bypass) can be used to test the effects of delay on applications, especially in redundant component solution. By testing the applications, you can ensure the same latency experience across the network, regardless of the specific datacenter. For example, some banks use the network emulators in their datacenter to test the effects of fixed and variable latency on their applications where they test the application with and without latency to observe the behavior.

Proactive performance monitoring solutions are another performance validation capability. A proactive solution allows you to generate synthetic traffic and send it across the network whenever you want. This allows you to capture mean opinion score (for voice), network delay, jitter, packet loss, and packet loss bursts. The results are displayed in a real-time dashboard. Now you know what is really happening at that point in time and lets you start to troubleshoot network problems (if there are any) faster whether you are using physical, virtual, or cloud networks.

Solution Options

- Improve data captures with taps for the right data from the right places
- Implement rapid detection of degradation in the quality of real-time market data feeds
- Use timestamping to get an accurate, objective analysis of packet propagation times
- Actively test network delay to understand network performance

Improving Compliance to Regulatory Mandates

Financial institutions have many regulatory compliance challenges. Existing requirements such as Graham Leach Bliley (GLBA) and PCI-DSS are fairly well known. The implication of newer requirements like the general data protection regulations (GDPR) and country specific financial laws (like the Turkish Rule 5651) are still fairly new. A visibility architecture is needed to accommodate current and future changes while providing validation of regulatory compliance.

An NPB is the right solution to satisfy financial data logging requirements, like the Turkish compliance mandate. The NPB is used to replicate a copy of all financial data and divert it to a data recorder so that it can be analyzed later by financial regulation personnel.

Protection of personally identifiable information (PII) customer data (per PCI and GDPR) is of considerable importance to any financial institution. NPBs can also be used to filter out unwanted. For instance, the GDPR will impact organizations in two ways as it relates to security and visibility. First, companies that are based in the EU, or, if outside the EU, are doing business with EU residents, will need to ensure that their handling of EU residents' personal data, at-rest or in-motion, complies with the GDPR. They must also ensure that no personal data is transported to countries outside of the EU that are deemed to have lower standards, except by design.

Any visibility architecture must ensure that a company knows which countries their data is going to, and if the data is not encrypted, must make doubly sure that it is protected.

The GDPR will have a major impact on the types of personal data that may be collected and recorded, as well as where this data can go. Any visibility architecture must ensure that a company knows which countries their data is going to, and if the data is not encrypted, must make doubly sure that it is protected. Protection standards outlined in the GDPR include pseudonymization or encryption, where possible, to reduce privacy risks.

Full featured NPBs can also provide data masking and packet trimming features that can ensure compliance to regulatory mandates. Data masking is the hiding of portions, or all, of the data collected with generic symbols. This preserves privacy of important customer data. Packet trimming is the permanent removal of the payload for the monitoring data. This if for monitoring data only and does not the affect the actual data in the network. Whether data masking or packet slicing is used depends upon the customer's need, as the two methods are similar but different.

Full featured NPBs also have the ability to provide granular, role-based access to data filters. This feature shows diligence towards network security and ensures further compliance to regulatory mandates. The capability is often more important to a business that has a multi-group environment that wants to use an NPB-based solution but it can be used by any organization.

Solution Options

- Logging of all financial data passing across the network
- Filter out any unwanted traffic to keep networks safer
- Packet slicing/trimming to remove the packet payload (including personal data) that is contained within monitoring data packet captures
- Granular role-based access control within an NPB as it diligently secures monitoring data and monitoring/security tools

Using Technology to Provide a Competitive Advantage

While competitive advantages are often fleeting, the IT network is a critical focal point for financial institutions and banks to capitalize upon. Two key ingredients for success often revolve around reducing downtime and controlling costs. Downtime is especially important. According to a 2016 Ponemon Institute study, an average minute of downtime for an enterprise can cost $8,851. Controlling costs is also important as precious capital can be redeployed to support other business objectives to create a competitive advantage due to new features and new products.

Reducing downtime is paramount. There are two quick things that can be done to benefit IT teams in this area. The first is to deploy an NPB. Once the NPB is in place, you can typically connect up security and monitoring tools up to it at will because there is no disruption of traffic, i.e. once the NPB is in place—it is in place. This has the fundamental benefit of limiting the amount of Change Board approvals needed for troubleshooting activities and usually means that you can start capturing data right away to help diagnose problems and locations of problems. This can dramatically decrease the mean time to repair (MTTR). Keysight customers have seen up to an 80% reduction in MTTR once they deploy an NPB.

The NPB will also allow you intelligently filter and feed only traffic of interest to your monitoring, security, and probe tools. Screening out extraneous data allows your tools to perform their analysis faster, as they have less data to process, and helps you reduce the time required for troubleshooting network issues. Filters can be defined and added to a library to make troubleshooting efforts as fast as possible, and repeatable (i.e. no filter definition mistakes).

An NPB can help you with data aggregation of multiple links to one or two security tools. This allows you to centralize tools to increase the load utilization on each tool. An NPB can also be used for load balancing data across multiple tools. This prevents tool overloads and provides a very acceptable level of survivability, as noted earlier. Load balancing also has the benefit of reducing costs for unnecessary tool purchases as the load can be spread evenly across multiple tools.

Solution Options

- Add an NPB to reduce the number of Change Board approvals and decrease MTTR
- Use data filtering and filter libraries to quickly gather diagnostic information reducing MTTR
- Use an NPB for load balancing to contain security and monitoring tool costs

Summary

The financial industry IT departments have significant challenges to face when trying to protect and update their networks. At the same time, there are solutions available to mitigate these challenges. These solutions involve eliminating network blind spots, performing key network assessments, and harnessing technology to replace outdated, manual processes.

Here are some specific recommendations:

- Deploy physical taps, virtual taps and bypass switches to get better access to data
- Deploy network packet brokers at the entrance to the network to optimize the flow of data between security analysis tools
- Deploy network packet brokers elsewhere in your network to make the flow of monitoring data to your monitoring and security tools more efficient
- Deploy Application Intelligence capabilities within your network to augment APM and NPM tools
- Perform security assessments against new security architecture changes before rollout to the production network
- Conduct proactive network performance monitoring to get objective performance data
- Deploy threat intelligence gateways to block traffic to and from known bad IP addresses

For more information on how to eliminate problems in your banking and financial network, refer to these Keysight solutions:

- Keysight taps and bypass switches (e.g. Flex Tap, iBypass 40)
- Keysight network packet brokers (e.g. Vision One)
- Keysight Network Emulator
- AppStack
- BreakingPoint
- CloudLens Private
- Hawkeye
- IxLoad
- ThreatARMOR

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