WHITE PAPER

How to Apply Network Visibility Within Educational Institutions

Technology Disrupts the Classroom

The education sector is undergoing significant change. National enrollment for higher education has declined 3 percent across the United States since 2015, according to the 2017 National Student Clearinghouse Research Center annual study. This is resulting in increased competition, student demands for more cutting-edge facilities, and shrinking profit margins, even as course fees reach all-time highs.

Across the country, national enrollment for higher education has declined 3 percent since 2015, according to a National Student Clearinghouse Research Center annual study.

To confront this trend, colleges and universities are focusing on a student-centered experience. For example, in addition to traditional classrooms, distance learning and mobile device support are being introduced to attract more millennials and older students. Institutions are also investing in technology improvements so that they retain their most important competitive asset–faculty and staff.

At the same time, existing trends like cyber security and public cloud-based networks continue to dominate Education sector changes. For instance, cyber security risk remains a point of concern as bad actors focus their attention on ransomware and theft of personally identifiable information (PII) from educational institutions. As IT organizations scramble to offer new digital and mobile services, this creates even more cyber security risks. In addition, public cloud networks, including those not endorsed by IT departments, have grown in popularity and can constitute new security risks.

KEYSIGHT TECHNOLOGIES

Therefore, these technology trends are creating the following network and data monitoring challenges for IT:

- Cybersecurity threats continue to represent a clear and present danger
- Blended data center strategies require extensive monitoring solutions
- Enhanced distance learning feeds require improved performance analysis
- Bandwidth monitoring is required due to expanding application usage
- Geographically distributed components are increasing troubleshooting time

Network visibility (monitoring) components and techniques can be used to overcome these challenges. Better visibility eliminates blind spots, decreases troubleshooting and monitoring costs, and improves operational efficiency.

A visibility architecture is a design that provides access to network traffic, intelligently filters the 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.

What is Network Visibility?

Information technology (IT) teams face increasing pressure to optimize the performance and security of IT networks and applications, monitor security defenses, and monitor and enforce compliance mandates. These initiatives require access to comprehensive network data. Complete visibility into the network is required for security and monitoring solutions to perform optimally. Limited visibility can result in extended threat analysis times, increased false positives, inaccurate conclusions, and longer mean times to repair (MTTR).

A visibility architecture will help you access the right network data, filter it, and convert it into actionable information. With actionable data, you can reduce troubleshooting and forensic analysis costs, as well as costs due to missed security threats.

A visibility architecture is a design that provides access to network traffic, intelligently filters the 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 will 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 specialized devices for analysis

Proper visibility starts with proper data access. The first and easiest task is to install taps. Taps are typically passive devices that you install once and never touch 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.

In addition to taps, you will want an NPB to optimize your filtering methodology. An NPB can provide several features that offload 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 (e.g. protocol analyzer, security appliance, loss prevention, etc.) 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.

By filtering data within the NPB, the monitoring tool (e.g. protocol analyzer, security appliance, loss prevention, etc.) 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.

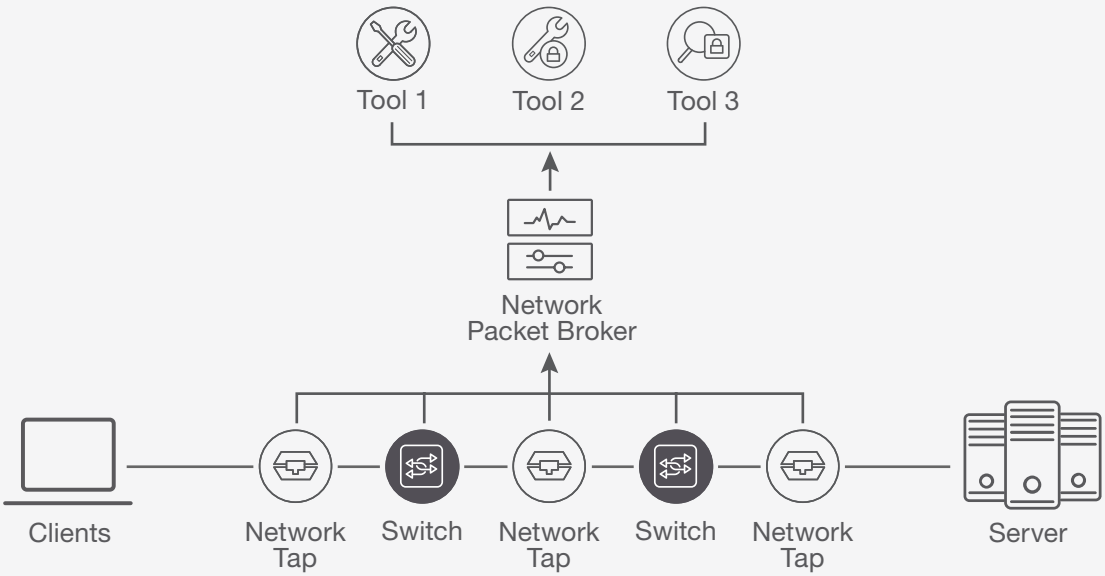

Figure 1. A network packet broker aggregates data from tap and SPAN ports.

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 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.

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 Higher education institutions and K-12 school districts.

Strategies To Control Security Risks

Cyber risk is a critical threat, whether it be a website attack, phishing, advanced persistent attack, or something else. As education institutions take on more federally sponsored research, they will need to safeguard data to conform to government regulations regarding federal contact information and data handling. Another potential source of concern are individual divisions and colleges within universities and K-12 school districts that have begun using cloud solutions without consideration for the security holes that they are creating for the university or district.

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 education network.

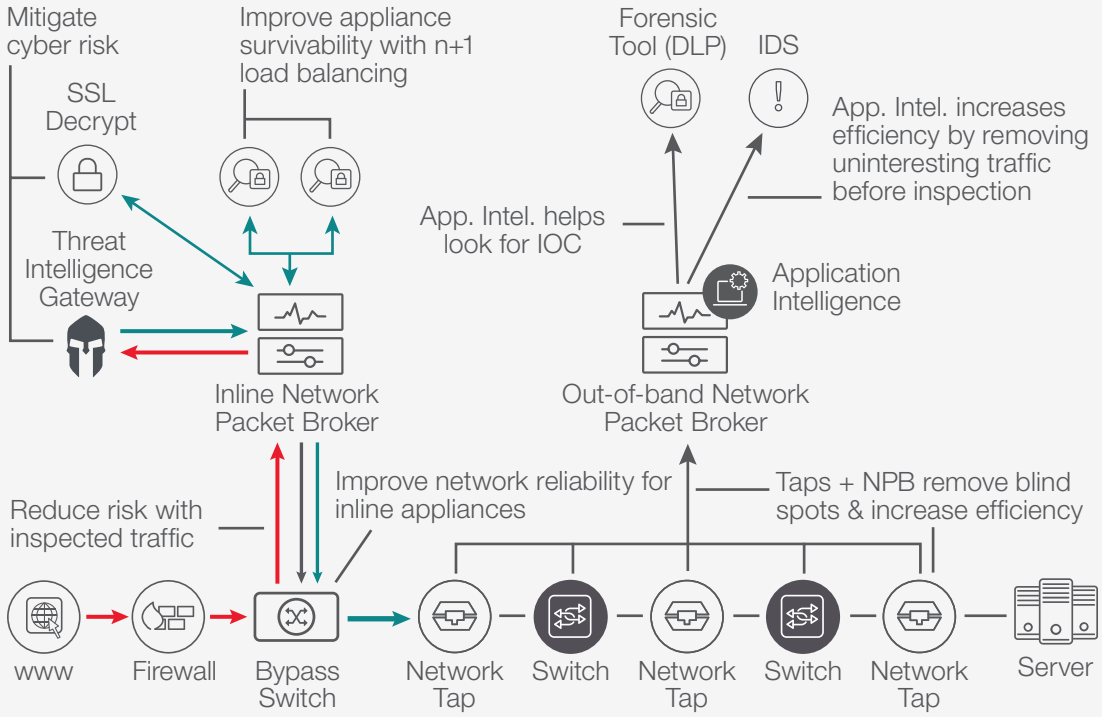

Figure 2. Example of network visibility and security solutions

As education institutions take on more federally sponsored research, they will need to safeguard data to conform to government regulations regarding federal contact information and data handling.

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

- **Mitigate cyber risk**–Threat intelligence gateways, inline security tools, and integrated Secure Sockets Layer (SSL) and Transport Layer Security (TLS) decryption solutions should be added. As an example, threat intelligence gateways remove 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.
- **Optimize data security threat analysis** – IT should add application intelligence to screen out unnecessary data flows (Hulu, Netflix, Pandora) and make security risk analysis faster. This type of application intelligence makes an Intrusion Detection System (IDS) up to 35% more efficient.
- **Reduce cloud security risks** – Individual colleges and other campus groups are spinning up cloud solutions that may introduce security and compliance problems for a large university system. Application intelligence can be used to examine the types of applications being utilized at various points across the network to expose unknown risks due to shadow IT. A subsequent proactive approach can be implemented using a virtual tap at those cloud instances to capture relevant security-related data and forward it to a centralized security analytics platform for analysis.
- **Improve network reliability** – Inline external bypass switches should be added in front of inline appliances to eliminate single points of failure within 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 packet broker which then connects the network performance monitoring appliance to the data it needs.

Individual colleges and other campus groups are spinning up cloud solutions that may introduce security and compliance problems for a large university system. Application intelligence can be used to examine the types of applications being utilized at various points across the network to expose unknown risks due to shadow IT.

Blended Data Center Management

As the education sector adds public cloud solutions to the network, this introduces many complications and may result in a split (hybrid) infrastructure for both public cloud and physical on-premises solutions. As a result, many institutions invest in technology that does not incorporate their security and monitoring tools with the right analytic techniques to create an overarching strategy. This is where network visibility solutions can expose the data that is needed and deliver that data to the proper analytic technology.

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 combined for a blended data center approach.

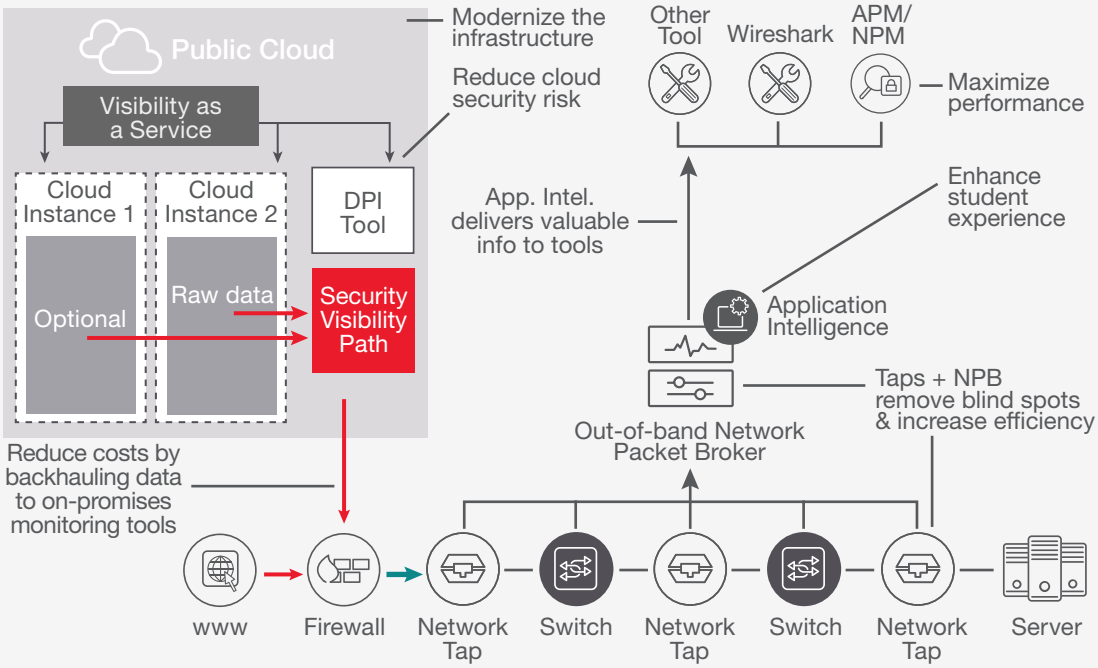

Figure 3. Example of network visibility for blended data centers

As Figure 3 illustrates, there are specific benefits that can be derived from visibility solutions for hybrid data centers:

- **Remove on-premises blind spots** – Install physical taps and packet brokers to get better access to data. This is especially important as K-12 and university networks are often spread out geographically with a substantial amount of distributed service centers. 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** – Public 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 capture packet data in the cloud.
- **Reduce costs** – Another consideration is to implement an 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.
- **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.
- **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.
- **Enhance student 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. This will allow IT to improve user quality of experience for student applications and devices running on the network.
- **Reduce cloud security risk** – A cloud visibility solution can be used to capture full packet data that can be used for deep packet inspection by a threat hunting and detection solution.

Digital assignments and live streaming of education content is now mainstream. According to the 2017 Education infographic by Livestream, 77 percent of colleges offer online courses and 55 percent of college presidents predict that by 2022, all students will take at least some of their classes online.

Ensuring Performance For Remote Distance Learning

Digital assignments and live streaming of education content is now mainstream. According to the 2017 Education infographic by Livestream, 77 percent of colleges offer online courses and 55 percent of college presidents predict that by 2022, all students will take at least some of their classes online. Since live stream and on-demand video feeds are critically important, performance issues cannot be tolerated. This is a prime concern for remote students and affects both university and K-12 institutions.

From a network visibility and security perspective, there are clear actions that can be implemented to address these issues. The following diagram illustrates how these technologies can be inserted into a generic education network.

Lots of new applications added to the network can affect network performance. A proactive monitoring solution can characterize your network, so you can understand performance issues and pinpoint where they occur.

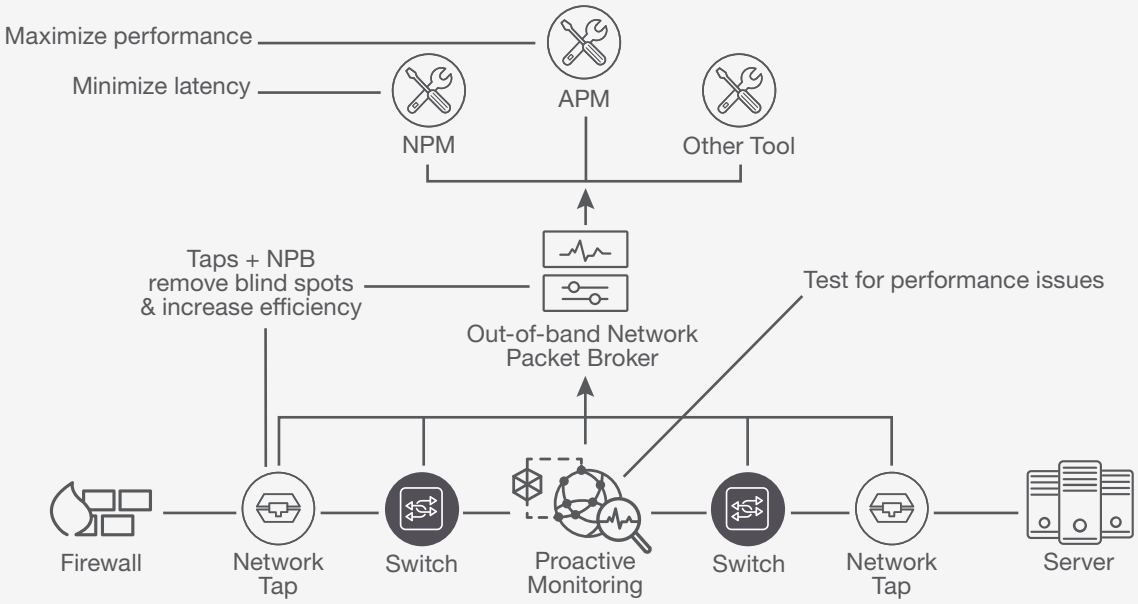

Figure 4. Example of network visibility solutions for performance issues

As Figure 4 illustrates, these are some of the specific benefits that network visibility can provide to optimize network performance:

- **Minimize network latency** – Install taps and NPBs to get network performance monitoring (NPM) data access across the network.
- **Remove on-premises blind spots** – Online education feeds can have issues. Install taps and a packet broker with application performance monitoring (APM) tools to be able to remotely capture data and analyze it to maintain student quality of experience (QOE).

- **Remove cloud blind spots** – Just as with the on-premises blind spot situation, cloud-based online education feeds can have issues as well. In this situation, a cloud visibility solution can be installed to collect packet-based data for those cloud apps and then the data can be passed on to an APM tool for analysis and QOE optimization.
- **Maximize network performance** – Lots of new applications added to the network can affect network performance. A proactive monitoring solution can characterize your network, so you can understand performance issues and pinpoint where they occur. A built-in synthetic traffic generator allows you to respond to complaints about application or network slowness to actively test different segments within your network and isolate and remediate problems faster. It can also be used to test software updates before they go live.

Prevent unexpected network outages due to application explosions

New network applications (especially multi-user games, online gaming, and movies) can consume a lot of network bandwidth. They also create volatile spikes in bandwidth usage. Application intelligence and the use of geolocation can be used to understand the applications running on your network, where bandwidth bottlenecks are located, and how to prevent outages should certain apps (like a multi-user scavenger hunt game or other interactive game) pop up out of the blue.

The following diagram illustrates how network visibility technology components can be inserted into a generic network to capture this kind of information and address it before a bandwidth explosion results in an outage.

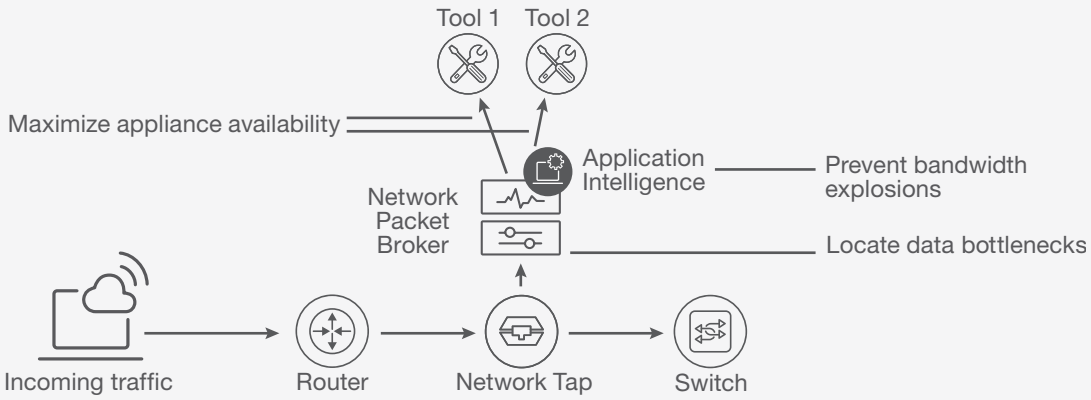

Figure 5. Example of network visibility and the usage of application intelligence

As Figure 5 illustrates, these are some of the specific benefits that result from integrating visibility and application intelligence into your network architecture:

- **Locate data bottlenecks** – Use application intelligence with geolocation to understand what apps are running on your network, where bandwidth bottlenecks are located, and prevent outages should certain apps (like multi-user scavenger hunt games) appear from nowhere. This can affect both wired and Wi-Fi IP networks.
- **Prevent bandwidth explosions from taking down the network** – Application intelligence can identify the specific applications running on your network so that you can monitor the amount of bandwidth they each consume. If severe usage spikes occur, you can visually see that information and respond accordingly. This includes notifying the application users or by terminating the application process on the network before it causes network disruptions.
- **Maximize appliance availability** – An NPB deployed can be used to load balance data across multiple tools. This provides 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.

Optimize Troubleshooting For Remote Sites

Troubleshooting optimization is important to both university and K-12 school systems. The reason is simple, longer mean times to repair affect the ability of staff, faculty, and students to do their job or complete course work on time. The longer the network service disruption continues, a less favorable attitude is created toward the institution. Faculty and students are expecting a fully functional, modern, and efficient experience whether on or off campus.

The following diagram illustrates how network visibility technology components can be inserted into a generic network to capture this kind of information and address it before a bandwidth explosion results in an outage.

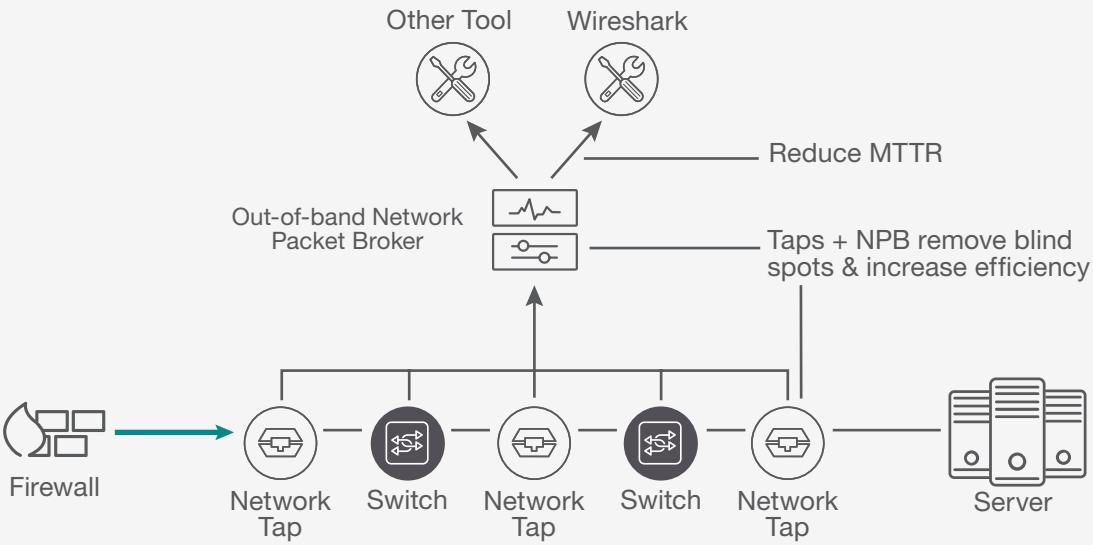

Figure 6. Example of optimizing troubleshooting for remote sites

Application intelligence can identify the specific applications running on your network so that you can monitor the amount of bandwidth they each consume. If severe usage spikes occur, you can visually see that information and respond accordingly. This includes notifying the application users or by terminating the application process on the network before it causes network disruptions.

As Figure 6 illustrates, these are some of the specific benefits that result from integrating visibility into your network troubleshooting processes:

- **Remove on-premises blind spots** – Install physical taps and packet brokers to get better access to monitor data. Taps placed at appropriate locations allow you to localize issues across the datacenter and the network (e.g. particular buildings, campus-wide, etc.).
- **Reduce MTTR** – K-12 school districts can take advantage of existing taps and packet brokers to make remote monitoring and troubleshooting faster and easier. This is because troubleshooting can be conducted from a centralized network operations center (NOC) to collect the requisite information from multiple buildings within the school district. This technology limits the need for on-site troubleshooting visits.

Conclusion

The education industry is experiencing an inflection point. Cyber security risk, human capital transformation, the shift to student centered institutions, and a growing abundance of data analytics is driving the change. To stay competitive, education providers will have to innovate their existing processes and curriculums.

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 inline bypass switches to increase network reliability
- Deploy 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 and proactively look for indicators of compromise
- Capture cloud data and backhaul it to on-premises equipment and tools to reduce cost and improve compliance

The education industry is experiencing an inflection point. Cyber security risk, human capital transformation, the shift to student centered institutions, and a growing abundance of data analytics is driving the change. To stay competitive, education providers will have to innovate their existing processes and curriculums.

Keysight 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 https://www.keysight.com/us/en/cmp/2020/network-visibility-network-test.html.

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