RESEARCH
Influence and insight
through social media

August 2019

How to Build a Solid Business Case for the Purchase of a

# NEXT-GENERATION NETWORK PACKET BROKER

**WHITE PAPER**

Prepared by
**Zeus Kerravala**

**ZK Research**
A Division of
Kerravala Consulting

## INTRODUCTION

While it's easy for a network or security architect to grasp the need for network packet brokers (NPBs), that's not always the case for the people in charge of budgets—company executives and the finance department. This white paper is designed to help you communicate the value of next-generation network packet brokers (NGNPBs).

## SECTION I: NEXT-GENERATION NETWORK PACKET BROKERS DEFINED

Network packet brokers are monitoring infrastructure devices that sit between network infrastructure and the management and security tools layer. Each infrastructure component, such as a router or a switch, provides a copy of traffic and/or data from a switch port analyzer (SPAN) port that tools analyze as part of a data set. To enable access to all traffic, not just a sample, network terminal access point (TAP) devices can also be used as part of the network infrastructure to access the traffic from the network. Without an NPB, each infrastructure component would need to be plugged into every tool. This is unrealistic, as the number of ports required, even in a small network, makes the deployment so overwhelmingly complex that it would be unmanageable, if not impossible.

When NPBs are used, each infrastructure device is connected to the NPB via a single connection, as is each security and monitoring tool, which is significantly simpler than when everything is directly connected (Exhibit 1). The term "broker" is appropriate because the NPB receives all traffic from every device and then sends the appropriate data to the individual tools. When an NPB is not being used, every connected tool receives all traffic, which puts the filtering burden on the tools and creates unnecessary overhead—in addition to their network interface card (NIC) needing to match the network link speeds, and each tool being unable to collectively see across multiple network links to cover asymmetrical routing and link aggregation groups (LAGs).

NPBs started out as out-of-band aggregation TAPs and provided the most basic of functions to ingest packets, aggregate (interlace) the packets and then pass them along to each tool connected to the aggregation TAP. These then evolved through the addition of some basic intelligence, where the NPB would selectively apply filtering and load-distribution capabilities to the copied traffic before sending it to the management and security tools. The next evolution added more advanced features such as de-duplication, header stripping, tunnel de-encapsulation and packet slicing to ensure only appropriate packets and data content were being directed to certain tools as opposed to all packet copies and all data content being sent to all tools. All NPBs available to buyers today contain some level of intelligence, whether it is only basic or more advanced.

In a parallel evolution, some NPBs had specific security capabilities added, such as data masking (to hide private or sensitive data) and inline bypass (so active security tools can operate without impacting application or network performance).

A few of the leading NPBs shifted to security packet brokers to help fight the growing number of cyber threats. NPBs have developed several security-specific capabilities such as pre-filtering,

### ABOUT THE AUTHOR

*Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.*

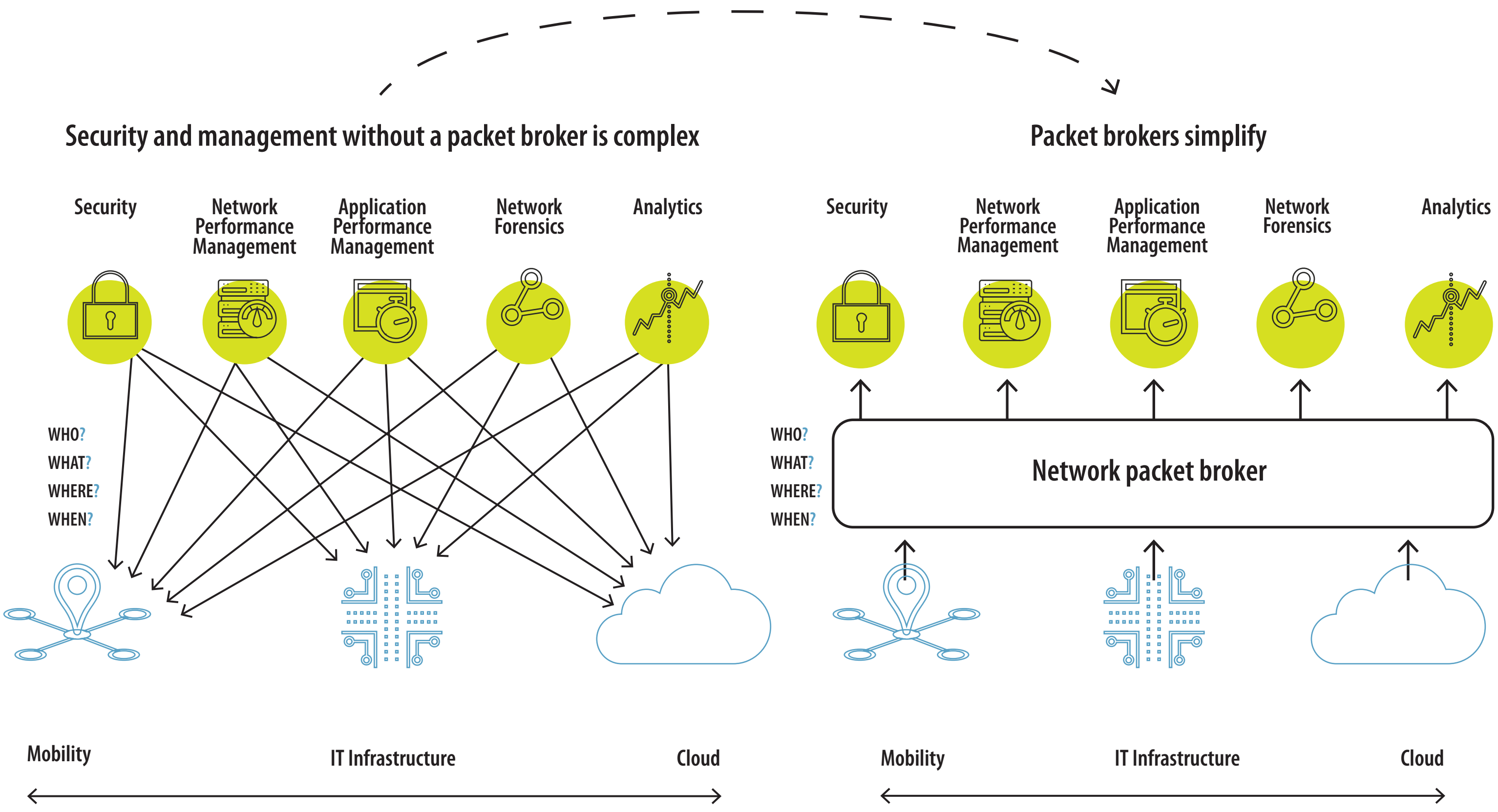
decapsulation, masking and the ability to operate out of band so the security tools will not disrupt application performance.

Recently, market leaders have introduced the most current phase of NPBs, which are known as next-generation NPBs, or NGNPBs. These are designed for agile organizations that need to move with speed but also ensure security. NGNPB features include the following:

- Metadata generation
- SSL/TLS decryption
- Application intelligent filtering and statistics
- Inline bypass
- Physical, virtual and cloud deployment models
- Automation capabilities
- Centralized management

NGNPBs have grown from a technology that many considered a "nice to have" to an absolute "need to have." The primary driving force behind them is digital transformation, as businesses of all sizes are looking to move with speed and out-innovate their rivals. This requires IT to be more

**Exhibit 1: Network Packet Brokers Make Security and Management Easier**



ZK Research, 2019

agile, but a company can only be as agile as its infrastructure allows. NGNPBs enable the underlying infrastructure to be updated or replaced without disrupting management and security functions, as those tools are connected through the broker. Without it in place, all the tools would need to be disconnected and some possibly upgraded or modified to work with the new infrastructure—a very expensive proposition.

The NGNPB can be thought of as a network infrastructure abstraction layer that enables organizations to find more insights in the massive amounts of information being collected from the network infrastructure. NGNPBs have always been important, but they are now considered critical to digital success.

## SECTION II: JUSTIFYING THE PURCHASE OF NGNPBS

Modernizing infrastructure is critical to digital transformation success. In a recent study, ZK Research interviewed IT managers from digital innovators as well as laggards and found that the innovators are spending about 1.5 times as much on IT as the trailing companies.

One reason why some companies do not keep pace with spending is that it's often difficult to justify to business leaders why certain technology needs to be purchased. With tools that are employee or customer facing, such as contact center systems and collaboration tools, the reason may be obvious, as there's a measurable impact on employee productivity or the customer experience. However, infrastructure is often hard to justify because it works "behind the scenes" to make things operate better. NGNPBs are a great example of this, as IT may understand their value, but making the case to a company executive can be difficult because the value isn't as obvious to those outside the IT team.

Exhibit 2 outlines how NGNPBs can demonstrate a clear return on investment, with details presented in the sections that follow.

**Exhibit 2:**
**Deploying NGNPBs Delivers Technical and Business Value**

- Enables a faster transition to hybrid and multi-cloud solutions
- Speeds up the deployment of management and security tools
- Improves cybersecurity protection
- Future-proofs the IT environment
- Improves the application experience
- Shines a light on shadow IT
- Optimizes IT infrastructure and increases organizational agility
- Accelerates data center modernization
- Provides cost savings

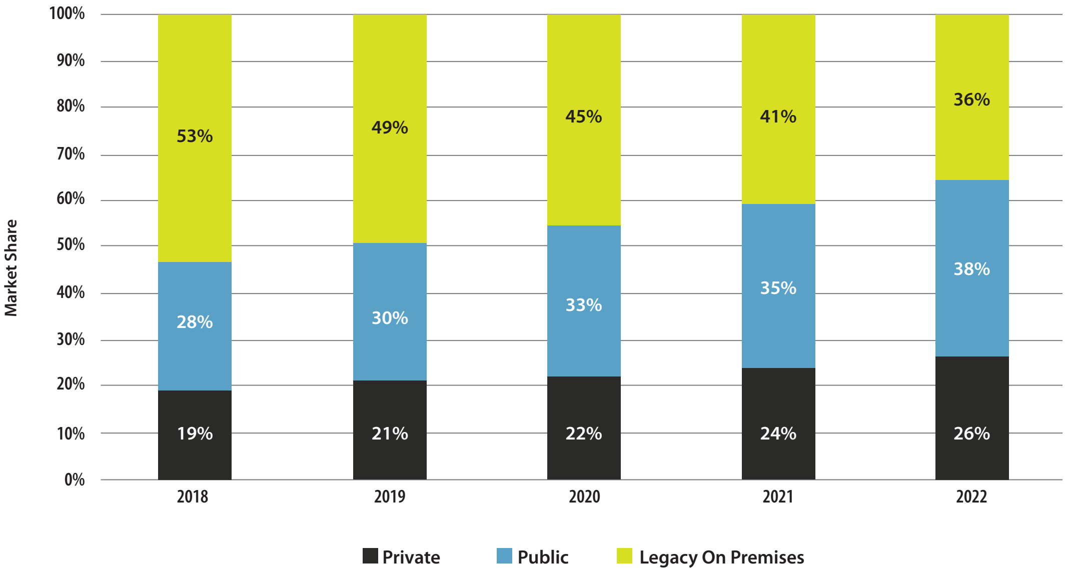
ZK Research, 2019

### Enables a Faster Transition to Hybrid and Multi-Cloud Solutions

Becoming a cloud-first company is a top initiative for most leading IT and business directors. However, when it comes to the cloud, there is no single way to deploy it. Each of the major cloud providers has its own strengths and weaknesses, and some workloads are better suited for private clouds. Consequently, 85% of organizations will adopt a hybrid, multi-cloud strategy utilizing a combination of private and public clouds, according to the ZK Research 2019 IT Priorities Study. In addition, the ZK Research 2019 Cloud Forecast shows the growth of both private and public clouds compared to legacy on-premises solutions (Exhibit 3).

The hybrid, multi-cloud model is certainly the best approach, but it's fraught with management and security risks, as tools need to be deployed in each cloud environment. The best way to migrate to this model is to deploy cloud-optimized NGNPBs in each cloud environment and direct the traffic back to centralized tools. This can normalize the information coming in, making it easier to analyze. The use of NGNPBs in the cloud enables businesses to move to a hybrid, multi-cloud model as aggressively as they want without having management and security get left behind.

**Exhibit 3: The Path Forward Is a Combination of Public and Private Clouds**



ZK Research 2019 Cloud Forecast

### Speeds Up the Deployment of Management and Security Tools

The process of upgrading network or security and management tools can be highly disruptive. For example, when a network is upgraded from, say, 10 to 40 gigabits, the management and security tools also need to be upgraded. With some devices, like firewalls, that can be extremely expensive. But with NGNPBs, a business could upgrade one component to the higher speed, change out the port on the NGNPB and then leave everything else the same. This leads to low-risk, rapid upgrades of security and management tools as well as network infrastructure.

Also, NGNPBs enable the tools to be deployed in multiple instances, such as in pairs, to have the traffic load-balanced across them, or to have one act as an inactive standby. When a tool is taken offline, all the traffic can be sent to the one that's still online or on standby, so service isn't interrupted. When the primary is then brought back online, the traffic can be redirected back and the alternate device then upgraded.

This obviates the need for maintenance windows and for IT to perform these tasks in the dead of night or over a weekend. In fact, this process could be done in minutes in the middle of the workday and no users would be impacted.

### Improves Cybersecurity Protection

In addition to enabling tools to be updated faster, NGNPBs make the environment more secure. Today, according to the ZK Research 2019 IT Priorities Study, organizations have an average of 32 security tools and experience what's known as "security sprawl," where having more tools doesn't actually make the company more secure. As more tools are added, it becomes increasingly more difficult to correlate data and find breaches.

With current architectures, despite the fact that businesses spend more and more on security every year, it still takes over three months to locate a breach. This is because so many blind spots are created by the cloud, bring your own device (BYOD), the Internet of Things (IoT) and other trends that are difficult to monitor.

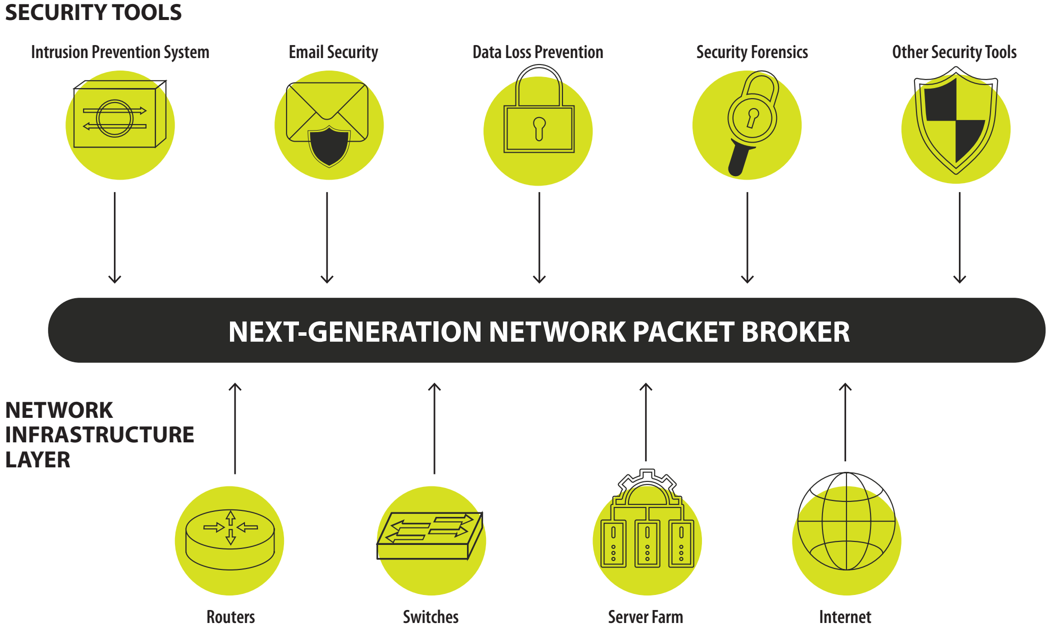
All network traffic is conditioned to be sent to security tools more effectively (Exhibit 4). This ensures all blind spots are uncovered and obviates the requirement to deploy tools everywhere, saving a significant amount of money.

### Future-Proofs the IT Environment

One of the most startling set of data points on digital transformation comes from the ZK Research 2019 IT Priorities Study, which found that 90% of organizations have at least one digital project underway but that 51% of CxOs admitted they do not know what their industry will look like in five years, while 72% stated that new competitors have emerged in the past three years. So, IT and business leaders need to plan for a future where they can't predict what will happen in five years or who they will be competing with, creating quite the conundrum.

This need for speed combined with market uncertainty underscores the need for business agility. NGNPBs form a management and security abstraction layer that separates the infrastructure from the applications. If a change must be made to the infrastructure to meet the needs of a digital initiative, this can be done without impacting the business.

**Exhibit 4: NGNPBs Eliminate Security Blind Spots**



ZK Research, 2019

### Improves the Application Experience

Applications used to be monolithic, vertically integrated software that ran in silos. This model optimized performance but was highly inefficient. With this architecture, infrastructure utilization was woefully low; ZK Research estimates storage and service utilization were roughly in the 25% to 30% range. In an effort to improve utilization, infrastructure has become increasingly disaggregated and virtualized, with application resources now existing in shared pools and apps having the ability to access them if necessary.

As an example, with the legacy deployment model, if server A was at 10% utilization and server B was at 90%, there was no way to migrate storage from one server to the other. Today, with modernized infrastructure, IT resources exist as shared pools—and if server B needed more storage, an IT administrator could provision it quickly.

This new model has many benefits, but it makes troubleshooting the application experience very difficult. With a vertically integrated approach, if an application was performing sub-par, IT pros could check the infrastructure and software within that particular silo. With a shared resource model, the problem could be related to one of the infrastructure components, network connectivity, a cloud provider or a wide range of other issues.

Traditional network management looks at applications via a "bottom-up" approach, where each component typically is monitored with a physical agent and then IT correlates the information manually—leading to long troubleshooting times. An NGNPB has integrated application intelligence, so it can see the infrastructure in a top-down model through the perspective of the application. If there is a problem, the application intelligence capabilities can quickly identify where the issue is and what's causing it, enabling problems to be solved much faster.

Application and network performance can also be impacted by a security breach. Distributed denial of service (DDoS) attacks and other security breaches can flood networks with traffic, causing applications and the network to perform poorly. The data generated by NGNPBs can be used to find the source of breaches, and any anomaly can be quickly identified. This can save companies millions of dollars, as even small outages caused by a security breach can be damaging.

*The data generated by NGNPBs can be used to find the source of breaches, and any anomaly can be quickly identified.*

### Shines a Light on Shadow IT

The rise of the cloud has enabled line-of-business managers and individual workers to procure their own software-as-a-service (SaaS) applications. Meeting tools, email services, cloud storage, social media platforms and others are all commonly found inside companies today, creating one of the biggest blind spots for IT.

ZK Research has interviewed many IT leaders who have endured a cloud audit only to be completely blindsided by the number of apps found. For example, before an audit, a CIO from a regional bank thought the company was using about 30 cloud applications; during the audit, he discovered that number was more than 700.

The metadata generated by NGNPBs can be used to study applications and see what cloud applications are being used, helping them to discover the following:

**Which company-sanctioned cloud apps are being used and are known to IT?** The utilization can be studied to determine who is or is not using the apps.

**Which cloud apps in use should be sanctioned by IT?** Actions can be taken to work with the cloud vendor to ensure fair pricing and enterprise support.

**What unsanctioned services are being used?** IT can use the data to provide a company-endorsed alternative. For example, cloud storage capabilities can vary greatly, as those focused on consumers lack the level of security and management control available in enterprise versions.

Understanding sanctioned versus unsanctioned cloud services can have a big impact on an organization's security posture. For example, a business might discover that the accounting department is using a consumer file-sharing application to share documents, which could lead to data theft. Having visibility into the use of unsanctioned applications can help security operations teams implement the right controls to ensure workers are not putting the company at risk.

*By analyzing the traffic collected and the data generated by an NGNPB, companies can make investments in accordance with network utilization.*

### Optimizes IT Infrastructure and Increases Organizational Agility

The network, IoT endpoints and management tools are generating a massive amount of data that can be used to optimize IT infrastructure management and upgrades. For example, a company considering a network upgrade typically would tackle the entire network at once, which can carry a hefty price tag. But by analyzing the traffic collected and the data generated by an NGNPB, companies can make investments in accordance with network utilization. If the analysis shows that one part of the network is saturated while other parts are underutilized, the organization could upgrade the heavily used portion immediately and upgrade the underutilized portion later.

### Accelerates Data Center Modernization

Infrastructure modernization is critical to the success of digital transformation. In the data center, this means shifting to new technologies such as software-defined networking (SDN), containers and virtualization that are optimized for a flat data center carrying a significant amount of lateral, or East-West, traffic. Legacy data centers were built hierarchically with large volumes of traffic that flowed through the tiers, into the core and then back up the tiers, more commonly known as North-South traffic.

With North-South traffic, all management and security tools can be placed in the core because all traffic must flow through it. With East-West flows, the traffic moves across the tiers and bypasses the core, meaning it never passes through the tools in the core. To solve this issue, all security and monitoring tools could be placed on every East-West link—but there are thousands of these, and therefore this configuration would be cost prohibitive and too complex to manage. Another solution is to direct all traffic to an NGNPB, which could then direct the traffic to the correct tools. This gives companies the agility of a modernized data center with the same level of tool capabilities available in a North-South configuration.

*NGNPBs can have a significant impact on cost.*

**Provides Cost Savings**

While cost savings should never be the primary driver for technology projects, NGNPBs can have a significant impact on cost. One of the most immediate and tangible cost savings is achieved by filtering irrelevant data, which makes monitoring and security tools more efficient. Without an NGNPB, traffic is often duplicated and sent to multiple devices. The use of de-duplication, filtering, packet slicing and other features reduces duplicate traffic and unnecessary data content by more than 60%, according to ZK Research estimates—in many cases, resulting in thousands of dollars in savings per tool, as companies no longer must overspend on application performance management (APM), network performance management (NPM) and security tools. This is just one aspect of cost savings. There are many other ways that NGNPBs help companies save money, including the following:

- Lowering capital expenditures of security and monitoring tools
- Lowering operational overhead
- Providing investment protection by extending the life of existing infrastructure
- Optimizing infrastructure
- Reducing the number of agents and probes that need to be deployed

## SECTION III: CONCLUSIONS AND RECOMMENDATIONS

The digital era has arrived, and it will change the business landscape forever. In this IT-driven era, competitive advantage is based on an organization's ability to be agile and adapt to changes as well as to make rapid shifts to capture market transitions. Trends such as virtualization, mobility, containers, the cloud and IoT enable businesses to rapidly become digital organizations, but they have significantly increased the complexity level within IT.

NGNPBs play a critical role in businesses' understanding of how their infrastructure and applications are performing and improving their cybersecurity posture. However, because NGNPBs are not directly end-user facing, they can be difficult to justify to business leaders who do not fully understand their value. To help organizations build a solid business case for NGNPBs, ZK Research summarizes the top benefits to be gained via the purchase and widespread use of these solutions:

**Enables a faster transition to hybrid and multi-cloud solutions** by creating a normalized data set that provides visibility into cloud performance

**Speeds up the deployment of management and security tools** by enabling tools to be upgraded or replaced without disrupting the operating environment

**Improves cybersecurity protection** by eliminating the many blind spots in traditional security architectures

**Future-proofs the IT environment** by creating a security and management abstraction layer that separates the infrastructure from the applications, enabling quick changes and upgrades

**Improves the application experience** by using application intelligence, where the infrastructure can be viewed through the lens of the application

**Shines a light on shadow IT** by providing metadata that can be used to discover which cloud apps are being used

**Optimizes IT infrastructure and increases organizational agility** because the data provided by an NGNPB can be used to prioritize upgrades based on utilization

**Accelerates data center modernization** by enabling organizations to better manage and secure East-West traffic, which is not possible without an NGNPB

**Provides cost savings** by facilitating intelligent de-duplication, filtering and slicing so companies can reduce the overall volume of traffic sent, in addition to lowering operational costs, extending the life of infrastructure and other factors

ZK Research also offers the following recommendations for companies navigating the NGNPB purchase process:

**Speak the language of the business when justifying NGNPBs.** CxOs and line-of-business managers have difficulty relating to metrics that are presented in technical terms. Instead, demonstrate the value of NGNPBs in terms that decision makers do care about. CEOs will listen if the NGNPB can improve the customer experience and increase the company's cybersecurity posture, while a CFO cares when operational costs can be driven down, and a sales leader would be interested if the NGNPB leads to quicker transactions.

**Select your NGNPB vendor based on modernized capabilities.** There are numerous packet brokers on the market, many of which claim to be NGNPBs. Low-cost NPB vendors claim the next-generation features aren't important and push their "good enough" solutions. Make a decision based on the business's current and future needs. NGNPBs are critical to ensuring IT success both today and in the future, and therefore application intelligence, cloud form factors and security capabilities should all be part of the decision criteria.

**Collect and analyze data for best results.** IT departments should be continually analyzing the data generated by an NGNPB. This can help them understand exactly what is happening today, who is accessing what information, where apps reside and other critical information. As the environment changes, NGNPBs can shine a light on blind spots and points of risk and enable IT to move to a predictive model.

**CONTACT**

*zeus@zkresearch.com*

Cell: 301-775-7447

Office: 978-252-5314