RESEARCH
Influence and insight through social media

November 2020

Network Complexity Drives the Need for

OUTCOME-BASED NETWORK MONITORING

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

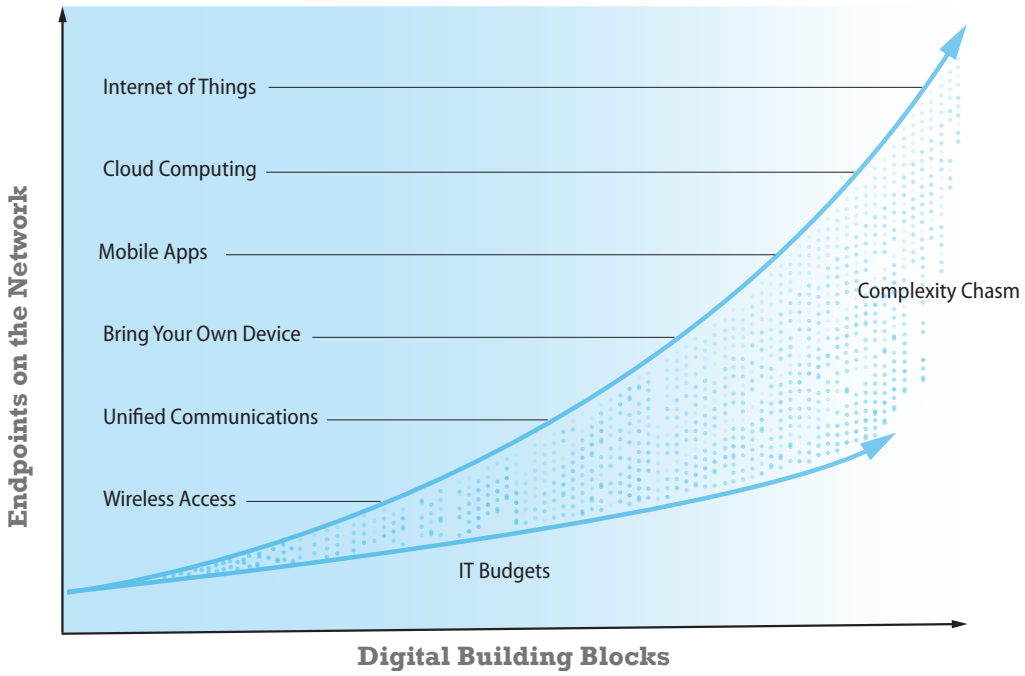
INTRODUCTION: NETWORK COMPLEXITY IS ON THE RISE

The role of the CIO has changed more in the past five years than any other position in the business world. Historically, CIOs and other IT executives were measured on technical metrics such as resource utilization, infrastructure performance and application uptime. However, the CIO's goals are now tightly coupled with those of the CEO. CEOs are tasked with driving digital transformation efforts to increase revenue, create new business models and improve profitability. In fact, CIOs are often expected to take a leadership position in driving the digital initiatives through completion. For the CIO, this means ensuring the services critical to the operations of the business are performing optimally and ensuring digital projects are completed successfully and on time.

These tasks are not simple, as the IT environment has grown in complexity. In an effort to be more flexible and more agile, businesses have introduced several technologies including virtualization, cloud computing and consumer technologies. This has widened the IT complexity gap (Exhibit 1) to the point where 71% of an average IT budget is used to maintain the status quo, according to the ZK Research 2020 IT Priorities Study.

The growing complexity of IT is at odds with the top priorities facing organizations as they plan for the post-pandemic world. Exhibit 2 shows the results from the ZK Research 2020 Work-from-Anywhere Study, which asked businesses what their top priorities were both during the stay-at-home period and then coming out of the pandemic. Complexity clearly works against all of the top initiatives.

Exhibit 1: Digital Transformation Increases Complexity



ZK Research, 2020

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.

Exhibit 2: Post–COVID-19 Priorities Are at Odds with Complexity

ZK Research 2020 Work-from-Anywhere Study

Improving security: With the majority of people working from home, organizations are focused on ensuring company data stays safe and the organization is not breached. Complexity makes securing the environment—particularly the network—more difficult, as it's hard to have a full understanding of the attack surface.

Maximizing worker productivity: In this highly competitive digital era, organizations need to drive their revenue per employee to new heights. To accomplish this, businesses have adopted a wide range of new tools, such as meeting platforms and video. Network complexity leads to unplanned downtime and poor application performance, which makes workers less productive.

Ensuring business continuity: In the past year, the definition of business continuity has changed. It used to focus on running the organization for a defined amount of time with a minimal set of services and people. Today, business continuity is about running the entire orga-

Management platforms must evolve and align with today's requirements in order to enable digital transformation and a more agile network.

nization indefinitely. Networks must be dynamic and agile in order to connect workers wherever they are. The increase in network complexity has made this difficult, if not impossible.

Protecting revenue: Digital transformation has changed the business landscape faster than ever, and this is causing tremendous disruption in almost every industry. Organizations need to adapt quickly to market trends, but a complex network can hold them back.

Maintaining a high level of customer experience: The top brand differentiator is now the customer experience. Organizations that step up their customer experience initiatives will gain share quickly, while those that don't will risk churning customers. For example, the ZK Research 2019 IT Priorities Study found that two-thirds of millennials admitted to changing loyalties to a brand because of a single bad experience.

Many organizations have upgraded their network infrastructure in an attempt to increase agility, but network application programming interfaces (APIs), software-defined wide-area networks (SD-WANs), intent-based networks and other trends do not solve the network complexity problem. Simplifying the network requires a dramatic shift in infrastructure management philosophies. Most infrastructure management tools are focused on managing the performance of individual service components, which in no way indicates the performance of a business service. The performance of a service is a more accurate indicator of user experience and productivity.

Also, many management tools focus on understanding whether infrastructure is up or down. But because organizations made heavy investments over the past decade to ensure every system is now redundant, the focus on downtime is somewhat meaningless. Rather, management tools should focus on the quality of the service being delivered.

Another challenge involved in improving service quality is shortening the time to problem resolution. With today's management tools, 90% of the time taken to solve problems involves simply finding the problem, according to ongoing research conducted by ZK Research. This is the "mean time to knowledge" required to identify that the user experience is impacted and to determine the source of the problem in complex multi-tier and multi-vendor environments. IT departments need to find a way to shorten the problem identification phase.

Management platforms must evolve and align with today's requirements in order to enable digital transformation and a more agile network. This will lead to better network resilience and turn the network into the foundation for the digital enterprise. Legacy tools were designed for the pre-cloud era, but network operations should be aligned with business outcome monitoring.

SECTION II: THE PROBLEM WITH LEGACY MANAGEMENT AND MONITORING TOOLS

The archaic nature of legacy management tools does not give the IT department the information necessary to run a 24x7 environment.

Traditional IT management tools were designed for an era when "best effort" was the norm. Technology infrastructure was deployed in tightly integrated silos using static, physical infrastructure, and performance was controlled by adding more resources to the specific application silos. In essence, quality performance was assured through inefficient design. The management tools that were deployed in this era were optimized for this environment and were based on three pillars that, today, have the following problems:

Reports have been used by IT managers for years to review historical information on the performance of assets. However, reports do not provide the real-time information that is needed to quickly isolate problems. In fact, reports often "smooth out" information, as they provide aggregated information that has been averaged out over a period of time, creating a situation in which anomalies and other events can be missed.

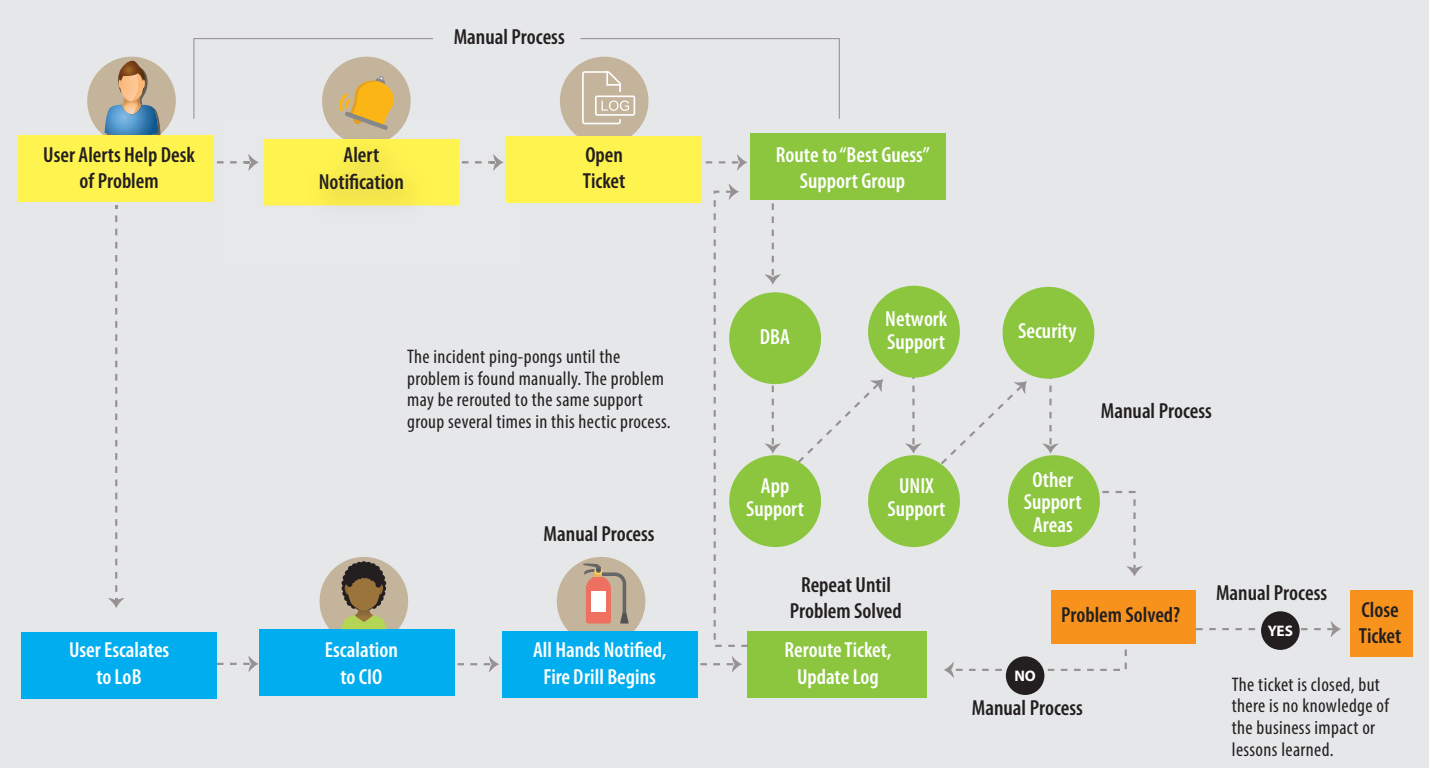
Red/green lights (fault management) are used to help IT managers identify whether elements of the infrastructure are up or down. Today's environments are built with high levels of redundancy, so an actual up/down alert can be meaningless. However, it's common to have a scenario in which all elements are green but an application is not performing properly. Therefore, it's more important to understand where congestion is occurring and which elements are not performing properly than it is to have insight into which elements are actually up and down.

Static maps have been used to show the physical topology of the network and other infrastructure. Static maps work well in an environment that is static. But today, because of WiFi, cloud, virtualization and consumerization, infrastructure can be created instantly and then removed, and devices are brought on the network without IT's knowledge—making static maps far less relevant than they were even a few years ago.

The archaic nature of legacy management tools does not give the IT department the information necessary to run a 24x7 environment. This lack of information has led to several operational challenges such as high amounts of human error and resolution "ping-pong" (Exhibit 3), which leads to long troubleshooting times.

In the future, legacy management tools will continue to fall farther behind because they lack machine learning (ML) capabilities. Network management tools are gathering significantly more data than ever before, making it challenging to derive insights manually. ML-based capabilities are a must for management tools moving forward, and most legacy tools do not have this capability.

Exhibit 3: Legacy Management Leads to Resolution "Ping-Pong"



ZK Research, 2020

SECTION III: WHAT TO LOOK FOR IN A BUSINESS OUTCOME MONITORING SOLUTION PROVIDER

IT management needs a new model that aligns network operations with DevOps to drive digital transformation efforts without the associated risk. The network management industry is filled with vendors, some old and some new, making it difficult to decide which one to select. ZK Research has done extensive research in this area and has identified the following criteria to help decision makers choose a vendor that can deliver business outcome monitoring:

Business insights: As highlighted in Section II, legacy monitoring tools are focused on informing IT professionals which devices are up and down. This can be highly misleading, as having a "down" device might not mean a business service has been impacted. Similarly, when things are "up," applications can perform poorly. Instead, the management tool should analyze data and present the results in terms of their impact on business services. This is the only way to understand business outcomes.

"As a service": Historically, network management tools were delivered in appliance form or in software deployed on premises. Network management as a service (NMaaS) is an emerg-

ing market with many advantages. Like all cloud apps, NMaaS leads to fast deployment times and ongoing innovation delivery. Also, by collecting data in the cloud, NMaaS systems can take a "big data" approach to network management to align it with next-generation network operations, also known as NetOps 2.0.

Programmability: Modern network management tools need to be fully programmable. The advanced programming capabilities enable full customization of monitoring and alerting, as well as the embedding of business-specific logic in the workflow. This helps NetOps 2.0 align network metrics with key performance indicators (KPIs) that are relevant to business operations. The tools should be extensible through Python scripts, enabling automation and ad hoc queries and reporting. Also, synthetic variables aggregate other element-level variables to conduct more complex analyses. The output from these computed variables can be sent back into the data pipeline on the platform itself to be used and tracked on an ongoing basis as part of the regular workflow. This enables an exceptionally high level of visibility into very specific business and technical parameters.

Best-in-class device-level visibility: Deep device visibility is one of the biggest problems with legacy tools. This causes network engineers to "fly blind" with poor operational information—and you can't manage what you can't see. Decision makers should look for automated, zero-touch topology visualization with depth. If something is connected to the network, the monitoring platform needs to see it and provide granular information about it. The management system should also automatically build and dynamically update topology maps, showing the operator exactly what's going on and obviating the need for constant updating of systems and documentation.

Simplified deployment: It's critical that the deployment of the system not require a retrofitting of the network. This means the vendor should have complete multi-vendor device coverage for a wide range of applications such as SD-WANs, firewalls, load balancers, voice and wireless. It should also consolidate monitoring data from multi-vendor, disconnected, cloud-based network management system platforms by using APIs, giving operators a unified view of all infrastructure and eliminating "swivel chair management" where an operator is constantly jumping between multiple screens.

Cloud simplicity: Using NMaaS systems means there's no need to purchase hardware or software. This removes up-front costs as well as maintenance spend and provides the ability to cost-effectively scale to an unlimited number of devices under management. NetOps 2.0 teams need the ability to get started with network discovery, maps and monitoring data collection in minutes. Additional ongoing configuration should require minimal to no effort.

Automation: ML-based automation enables enterprise-class scale across the network. All variables and alerts should be fully programmable and can perform functions such as automated troubleshooting. The automated discovery process for new or changed devices eliminates on-site configuration errors, which can lead to unplanned downtime.

Business-relevant insights: Solutions need advanced programmability to deliver insight to the business based on complex business logic and time-series telemetry data. This could include performance against service-level agreements (SLAs) and KPIs, network uptime and utilization, and device profiles. Ideally, the platform would present graphical data to management that's easy to understand and aids in regulatory compliance by making data readily accessible.

Intelligent search: Modern products should have easy-to-use, Google-like search capabilities to provide network operators and other parts of the business—such as procurement and customer service—with a powerful and intuitive tool for identifying and drilling down on network elements based on multiple search criteria.

SECTION IV: NETSPYGLASS OFFERS BUSINESS OUTCOME MONITORING

ZK Research has conducted extensive research in the area of network management and believes NetSpyGlass is the only solution that offers the combination of visibility, scripting and the ability to add data from all computed variables back into the data pipeline on the platform with internet-class scale. NetSpyGlass provides a native application programming environment that supports the development and execution of custom business logic in the data pipeline. It also offers rich third-party integration and works with ServiceNow, PagerDuty and Slack. This lets companies get more value from the investments made in other IT operations platforms.

Case Study: NetSpyGlass Enables Retailer to See More and Improve Network Reliability

A U.S.-based clothing and accessory retailer with revenue topping $16 billion in 2019 was struggling to find the root cause of network problems, and this was having a direct impact on network reliability. As is the case with most businesses today, the network has become critical to this global retailer because the organization has thousands of branch offices that need connectivity to network-based services.

Like most companies, the retailer had been adding to its network over the years, which created a high degree of technical complexity for network management and monitoring. The retailer's global network consisted of over 30,000 connected devices—including WiFi access points, switches, branch routers in the stores and a full campus network—and the network equipment needed to power an online shopping portal and global distribution points. The network was continually evolving, and the organization was going through the process of standardizing on WiFi and SD-WANs—as multiple vendors were being used, including both established and emerging companies.

The process of managing the network was fraught with many of the typical problems large companies encounter when networks are grown over time. For example, the naming of devices had an arcane convention and required deep knowledge as well as a background in manually updated spreadsheets, homegrown scripts, open source alerting products and other tools. This meant that doing even the simplest reporting required many layers of processes to correlate data across the tools. Also, any kind of reporting output was provided in operations terminology that did not translate easily into the metrics business leaders were looking for.

One of the biggest challenges was the dichotomy between alerting versus root cause analysis. The alerting tool provided a massive number of alerts, which did nothing to help find the root cause of a problem. In large networks, device-level issues are common, and some cause problems while others do not. The legacy tools the retailer was using provided no context, causing the network team to effectively be blinded by the massive amount of data.

After struggling with open source tools and legacy management vendors for years, the retailer decided to look for a more modern solution. After careful evaluation, the retailer chose NetSpyGlass, with the main appeal being its ability to deliver proactive operations in the style of Google. NetSpyGlass requires no hardware and is delivered as a pure software-as-a-service (SaaS) offering that talks to a handful of lightweight telemetry agents, so running a proof of concept was fast and easy. The proof of concept was a success, and the retailer decided to move forward with the deployment.

One of the biggest benefits of NetSpyGlass for this retailer was the enhanced and automated visibility. The tool created a real-time map of the network that was continuously and dynamically updated. Naming and tagging devices upon deployment moved from manual integration of the inventory system and spreadsheets to a few clicks on a centralized dashboard. Also, the maps could be organized graphically, and the data collected could be used within applications included with the NetSpyGlass services and shared with other users. This made it easy to focus on certain areas and show the business owners the information they required in a format they could understand.

NetSpyGlass is able to see trends and changes that occurred in the past and can use that data to help prepare for the future. Because the tool is fully cloud based, it is scalable and enables easy storage and graphical presentation of data.

"We can see the whole network, broken down into NetSpyGlass maps. Even with multiple technical evolutions going on, including the move to SD-WAN and adopting cloud-managed WiFi, we have maintained automated network-wide monitoring and grown from SNMP [Simple Network Management Protocol] polling to telemetry-driven business-level alerting."

—Network architect at a large U.S. retailer

SECTION V: CONCLUSION AND RECOMMENDATIONS

Digital transformation has introduced many new technologies and has dramatically changed the way businesses operate and the way people work. Although tremendous innovation has occurred in almost every area of infrastructure, management software has stood still—and consequently, IT is unable to close the complexity chasm.

Legacy management tools operate in a "bottom up" manner, focusing on the actual infrastructure elements and providing information on the status of specific devices. Although this type of information is still valuable, data must also provide a "top down" view in which it is easy to understand the impact of outages and alerts on business services.

This new model of management can help companies proactively avoid outages, rapidly identify problems that could cause service disruption, and provide a view into what isn't working properly instead of just what's up and what's down. To help companies transform their approach to network management and improve the end-user experience, ZK Research makes the following recommendations:

Shift IT management dollars away from legacy tools and toward solutions that can provide end-user experience management. Investing further in legacy management tools will not enable companies to meet the current challenges created by digital transformation. Having an end-user view will help reduce problem identification time, which will have the biggest impact on reducing mean time to repair.

Utilize baseline application data. It's hard to determine where to make infrastructure investments without understanding the state of the current environment. Baselines will provide visibility into how each component of the application delivery stack is performing, and this information can be used to prioritize investments to maximize the user experience.

Choose a vendor that is built for the digital era, even if it means moving away from the incumbent vendor. The IT management needs of digital businesses are significantly different compared to a decade ago. Companies should avoid building their own management tools with open source code and rather should leverage the power of the cloud with a tool like NetSpyGlass that can evolve along with the organization.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314