

WHITE PAPER

**Troubleshoot Network
Performance Issues
7-10x Faster**

Executive Summary

When there's a performance problem on the network, you need to be able to troubleshoot and resolve it quickly. This requires that you know what is happening on your network both now and historically, what is typical, and who or what could be affected. This kind of holistic visibility is critical in order for you to quickly identify and resolve performance problems. Many of the tools used today provide pieces of the information but they do not provide a holistic view that shows the activity of users, applications, hosts, and devices and answer questions about who, what, where, when, what's typical, and what's changed.

Network Behavior Analysis (NBA) systems fill this gap. They analyze network traffic data from routers and switches throughout the network. They build a profile of the behavior of systems, users, and applications inside the network and continuously monitor their activity, alerting operations teams to performance issues, security events, and policy violations.

The Mazu NBA system provides the continuous global visibility you need to troubleshoot performance issues 7-10x faster, regardless of the source of the problem:

- Mis-configurations
- Unauthorized activity on the network
- Changes in the network environment
- Security breaches

The Challenges of Troubleshooting Performance Issues

With all the tools and technologies available to networking teams today, why is it still so difficult to *quickly* and *accurately* troubleshoot performance issues?

With all the tools and technologies available to networking teams today, why is it still so difficult to *quickly* and *accurately* troubleshoot performance issues? More often than not, the symptom provides no clues to the cause of the problem. There are a number of potential culprits, including: a mis-configured application or device, unauthorized activity on the network, changes in the network environment, or a security breach.

In order to quickly start down the right path of identifying and resolving the problem, you need global visibility to understand what happened on your network leading up to the problem.

Standard Tools Don't Provide Global Visibility

To reduce the time it takes to diagnose and fix performance issues, you need to be able to isolate the behavior change that contributed to the problem, no matter where on the network it occurred or what the cause.

Many tools provide information – packets, latency, bandwidth utilization, etc. – about the network's performance. Some even provide context at the level of an individual link. But they don't provide the global context needed to understand why the performance is suffering; instrumenting the entire network with these tools is cost- and effort-prohibitive.

You need a technology that lets you understand the activity of users, applications, hosts, and devices across the entire network and answer any question about who, what, where, when, what's typical, and what's changed. You also need to understand what's happening now, as well as what happened in the past.

Get Global Visibility with Network Behavior Analysis

The Yankee Group defines Network Behavior Analysis (NBA) as systems that “take information from existing network devices about how endpoints are using the network (where they go, what they use, typical traffic, etc.).” NBA systems analyze network traffic data – such as NetFlow, cFlow and sFlow – from routers and switches throughout the network. The system builds a profile of the behavior of hosts, users, and applications inside the network and continuously monitors their activity, alerting operations teams to performance issues, security events, and policy violations.

Mazu provides the continuous global visibility you need to dramatically reduce the time it takes to troubleshoot performance issues.

The Mazu NBA system provides continuous global visibility into how users, applications, hosts, and devices are behaving on your network, and tells you how their current activity differs from their typical behavior. You'll optimize network operations, secure your internal network, and maximize application availability because you'll always know what's happening on your network: who's talking to whom, what applications and services are running, where the traffic is flowing, and if there are any meaningful changes that indicate a network issue, security threat, or application problem. Mazu collects this information across any, or all, of your network using a passive, agent-less deployment model that delivers immediate value. The data is stored in Mazu's *Network Intelligence Database*, including both real-time and historical details. With this always-on, global view you'll understand usage patterns, consumption rates, and dependencies between users, applications, and network infrastructure. This dramatically reduces the time to troubleshoot network and security issues and provides critical information for accurate planning and impact analysis.

Mazu provides the continuous global visibility you need to dramatically reduce the time it takes to troubleshoot performance issues. Specifically Mazu shows you:

- Who is on the network
- Who is talking to whom
- What applications are running
- Over what ports/protocols
- Where the traffic is flowing
- What's happening right now
- What happened before
- What's typical

The information that Mazu provides can help you troubleshoot performance issues 7-10x faster.

Troubleshoot Performance Issues 7-10x Faster

The continuous global visibility that Mazu provides offers a number of advantages that enable network professionals to dramatically reduce the time it takes to troubleshoot performance issues. Mazu shows you:

- All network activity leading up to the problem
- How that activity differs from typical behavior
- What users, applications, devices, ports, and protocols are involved

Whether the problems are due to mis-configurations, changes in the network environment, unauthorized activity on the network, or security breaches that affect performance, Mazu provides the global context needed to diagnose and resolve virtually any performance problem. This information is available from one console and without needing probes or inline devices deployed in the network. Once the problem is resolved, you can use Mazu to verify that performance levels have been restored.

Mazu in Action

A national food manufacturer was experiencing catastrophic network slowdowns due to bandwidth problems on a small frame relay to remote sites. The slowdowns would begin every day at 6 am. After two weeks of struggling with the problem, the network support team used Mazu to analyze application use on the link and identified a patch management server that was generating a large proportion of traffic. They discovered that this server was mis-configured to push updates to remote offices that did not need them. The server would mark the update attempt as "failure" and re-try the following day.

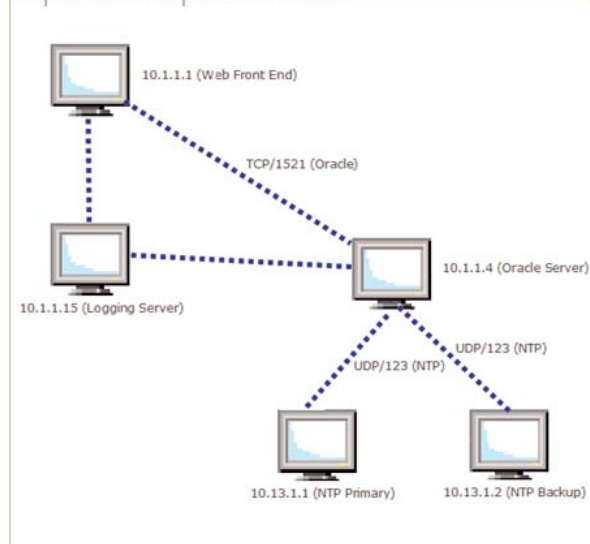
A business services provider's network was experiencing slowdowns every couple of weeks between 7 am and 10 am. The support staff was unable to identify the cause. The team suspected that the slowdowns might be due to backups, but the database administrators asserted that all backups were run only in the middle of the night. Mazu showed that, due to a configuration error, one of the backups was scheduled to run during morning hours. Further, the company used Mazu to implement a rule-based event to ensure this problem would not happen again.

Mis-Configurations

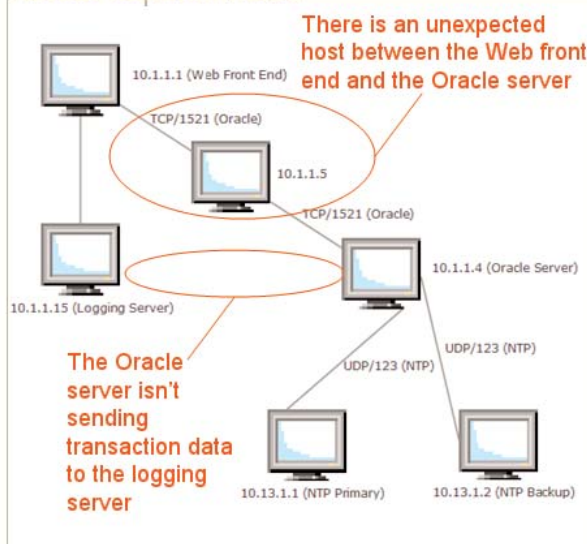
Mis-configurations can be extremely difficult to identify but can cause significant problems on the network. Mazu helps you:

- **Isolate the origin of the problem** – Because Mazu shows you exactly what applications and hosts are doing on the network and how their current behavior differs from typical activity, you can quickly isolate the source of the problem. For example, a load balancer that is mis-configured may not balance traffic effectively; Mazu shows you the traffic traversing each interface of the balancer in bytes, packets, and utilization percentages enabling you to identify the source of the problem. Because Mazu also provides historic context, you can see when the changes in behavior began, identifying when the mis-configuration happened and how severe the effect was.
- **Identify dependencies** – Mazu shows you actual dependencies, which may differ from expected dependencies on the network. This very important, but sometimes overlooked, distinction is critical for speeding up the troubleshooting process. Mazu shows how traffic flow and behavior changed due the change in dependencies, such as the addition or removal of a dependent host, application, or service.

Expected dependencies



Actual dependencies



Mazu identifies actual dependencies, which may differ from expected behavior, to help you identify mis-configurations that could cause performance problems.

Mazu in Action

A national insurance company had a policy prohibiting peer-to-peer and instant messaging on the company network for security and performance reasons. They had, however, no way of detecting violations or enforcing the policy. Using Mazu's rule-based events, the company is now able to identify unauthorized peer-to-peer and instant messaging traffic violations within minutes.

A national retail chain had no way to identify tunneled traffic between the internal network and proxies or external networks. Within 20 minutes of setting up a rule-based event, Mazu identified Gnutella being tunneled over HTTP. It also discovered a PC running "morpheus.exe" which was also out of date for patches and anti-virus protection.

Unauthorized Activity

The use of unauthorized applications and services on corporate networks is exploding. Despite the implementation of aggressive acceptable-use policies, it can be extremely difficult to enforce those policies. In addition to creating a security risk, unauthorized applications and servers can choke the network. Mazu helps you:

- **Identify unauthorized applications and their users** – Mazu shows you – by name – the applications running on the network as well as how much bandwidth they are consuming, which ports and protocols they are using, whether they are tunneled, and who – by user name – is using the applications.
- **Proactively enforce use policies** – You can develop the appropriate access and use policies and use Mazu to alert when policies are violated, enabling you to enforce those policies.

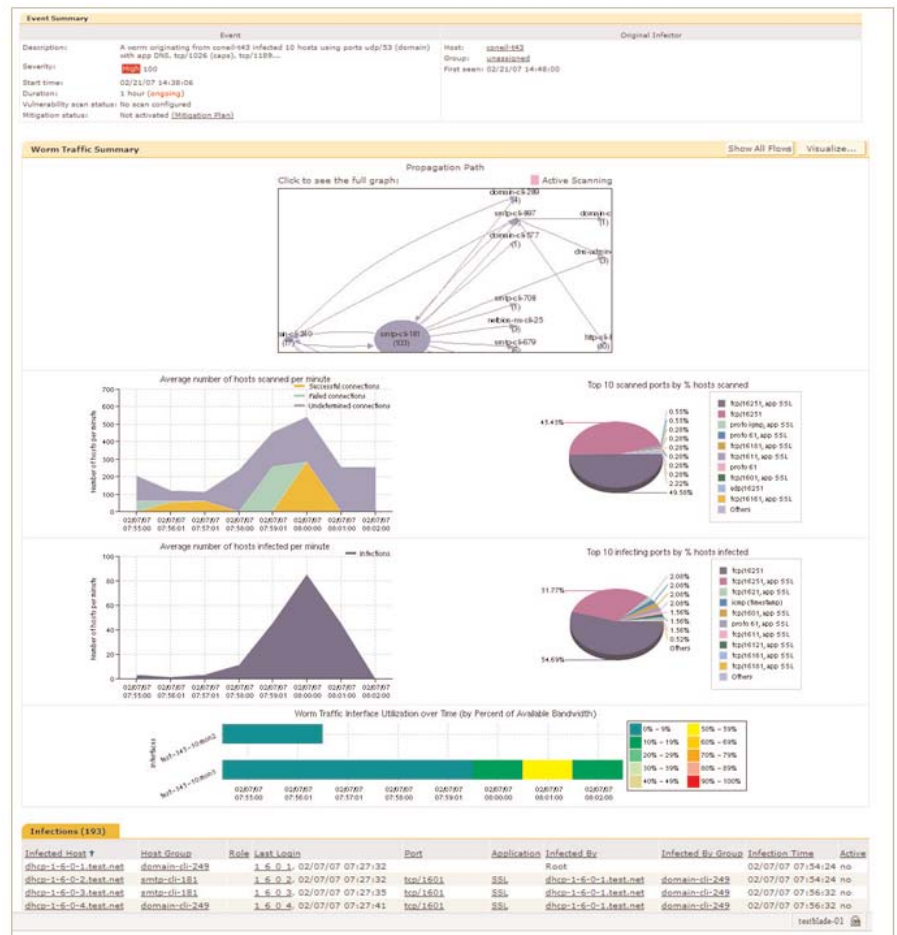
Mazu enables you to set and enforce policies on unauthorized applications.

The screenshot shows the 'New Rule Based Event' configuration window. The 'Look Up Applications' dialog is open, displaying search results for 'kazaA'. Two entries are listed: 'KaZaA' and 'KaZaA*'. A red circle highlights 'KaZaA*', with a red arrow pointing to it and the text 'Select the application'. The 'Threshold' section is also highlighted with a red circle and a red arrow pointing to it, with the text 'Define alert criteria'. The 'Threshold' section includes fields for 'Trigger' (Above 0 bytes per sec), 'Direction' (Either A to B or B to A), 'Duration' (00 hours 01 minutes), and 'Severity' (100). The 'Application' section shows 'KaZaA, tunneled KaZaA' selected. The 'Schedule' section shows 'Days to run rule' with checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The 'Host/Group B' section shows 'Select' options for Any, Within, and Outside, with 'Within' selected. The 'Application' section shows 'Select' options for Any, Within, and Outside, with 'Within' selected. The 'Threshold' section shows 'Trigger' set to 'Above 0 bytes per sec', 'Direction' set to 'Either A to B or B to A', 'Duration' set to '00 hours 01 minutes', and 'Severity' set to '100'. The 'Notification' section shows 'Low' selected for 'Log Only', 'Medium' selected for 'Owner', and 'High' selected for 'Owner'.

Changes in the Network Environment

In today's complex network infrastructures, small changes to the environment can have a significant impact on service availability. Often the cause and effect is not obvious, making it difficult to trace problems back to their original source, which could be as diverse as a faulty network device or a user unplugging a VoIP phone from one outlet and plugging it into another one. Mazu helps you:

- **Identify meaningful changes in network activity** – Mazu compares *current* behavior with *typical* network activity to identify meaningful changes that can cause performance problems. This information enables you to identify a change in the environment – even a small one – that otherwise would be difficult or impossible to find. For example, a well-meaning application developer decides to add the company logo to the login page of a high-volume application and uses a large graphic file. This creates an increase in the traffic load at certain times of the day (morning, shift changes, etc.) potentially resulting in performance degradation. It would be extremely difficult to trace the performance problems to this change. But with Mazu, you would see a significant change in outbound traffic and the details of that traffic would lead you to the source.
- **Context to understand the changes** – Mazu provides detailed information about the change to help provide the context needed to understand its impact on the network. In the example of a developer adding a logo to a login process, Mazu will alert you to a bandwidth surge that didn't previously exist. It will also show you that the source of the bandwidth surge is on the server, not the clients, and that the surge coincides with a large number of users logging in. This context leads you quickly to the source so you can eliminate the file or replace it with a very small, optimized version.



Mazu displays important information to provide context for a change such as when it occurred, which hosts/interfaces/applications are involved, and which parts of the network are involved.

Mazu in Action

An energy company's customer service center uses VoIP. They were experiencing significant problems such as inconsistent availability and dropped calls but were unable to identify the cause. As soon as they installed Mazu, they were able to quickly identify the problem, which was that several VoIP components were sending data to a decommissioned VoIP gateway. With this information the company was able to quickly fix the misconfigurations and resolve the problem.

An application critical to one of a business services provider's largest customers was periodically being disrupted and, as a result, the account was in jeopardy. The first time this occurred after Mazu was installed, Mazu immediately detected a suspicious connection from the application development group to the server moments before the outage. A quick call revealed that an application developer had, in the interest of time, ignored the procedure and made a small application change directly to the production system. The problem was immediately fixed and the customer proactively notified.

Mazu in Action

A major beverage company often uses unpatched operating systems on their manufacturing system, which is a network that usually does not have external connectivity. Someone doing maintenance, however, had connected to the network using an infected laptop. Mazu was able to detect the infection before it took down the entire assembly line, which would have been extremely expensive.

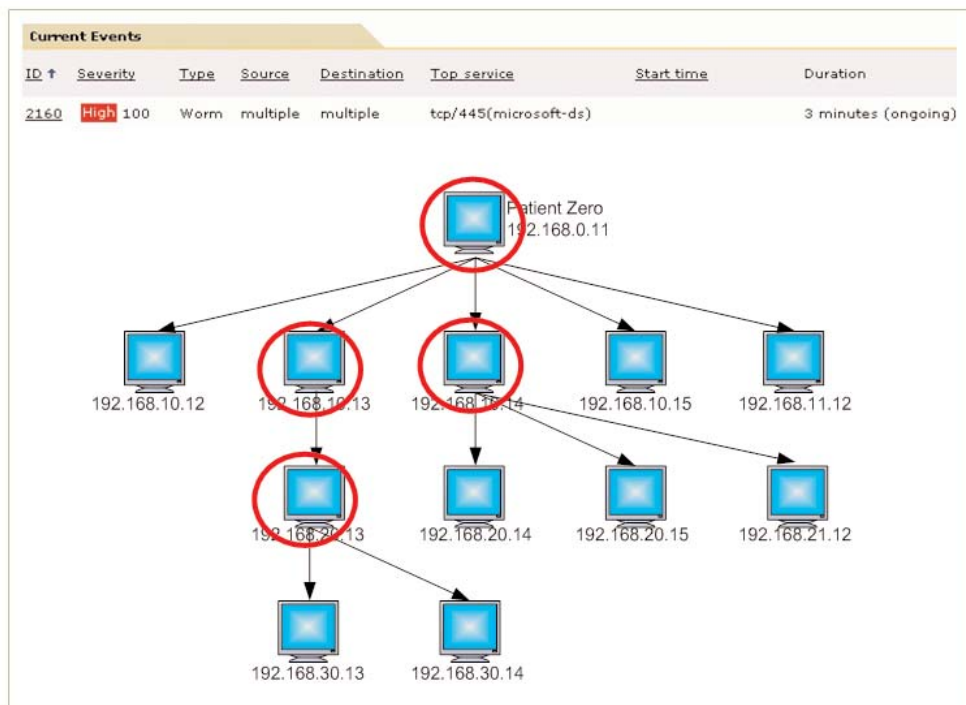
A cable company had spambot-infected machines that were being blacklisted, but they couldn't tell which hosts were infected. On average, it was taking 24 hours to find each infection. Once Mazu was installed, they were able to identify infections within five minutes.

Security Breaches

No matter how strong your perimeter defenses, worms and other malware can still penetrate your network and create application outages and network performance issues. Worms and other malware need to be identified and isolated immediately to contain the damage and minimize the impact on the network's performance. Mazu provides:

- **Behavior-based security heuristics** – Mazu's security heuristics detect a broad range of security breaches that signature-based systems can't identify, including zero-day worms, massive port scans, and credentialed attacks.
- **Propagation and scope of breach information** – With Mazu you can identify patient zero and see the propagation path to help you understand how to contain the infection. In the case of credentialed attacks, Mazu provides complete historical context to identify which systems have been compromised.
- **Resolution** – Before you take action, Mazu will show you the impact of the proposed response to ensure that no critical systems are needlessly disrupted. Mazu enables you quarantine compromised systems directly through the routers and switches on the network. Mazu also integrates with IPS and other mitigation applications enabling you to integrate your mitigation workflow.

Mazu shows you how a worm got into the network, who is "patient zero," who is infected, and how the worm is spreading.



► Why Mazu is Unique

- **Continuous global visibility** — Rapidly resolve issues. You'll get *global* visibility from Mazu's holistic view of the activities, usage, and dependencies between your users, applications, and IT infrastructure. You'll also get *continuous* visibility because Mazu is always-on, constantly collecting the details of your network's traffic and retaining them in Mazu's *Network Intelligence Database*. Mazu also continually updates a moving profile of your network's typical behavior to reflect your changing business conditions. This allows you to analyze your network behavior from many dimensions. What's happening now? What happened before? What's changed? This unique combination of behavioral profiling with real-time monitoring and historical logging gives you the data to diagnose urgent incidents, resolve repeating problems, identify trends for effective planning, and conduct forensic analysis.
- **Rapid, agent-less deployment** — Fastest time-to-results. You'll deploy Mazu quickly and with very little effort, because you won't have to install any agents or inline devices. Just install the Mazu appliance on your network, and it will immediately begin collecting your flow data to give you continuous, global visibility within hours of deployment. And because Mazu can collect your flow data from a subset or across all of your network, you can start small and expand your visibility, or you can view your entire network from day one — the choice is yours.
- **Automatic and custom behavior analysis** — Detect network and security issues before they disrupt your business. You'll use Mazu's patented behavior analysis to determine if your current network activity is meaningfully different from its typical behavior to warn you of a network issue, a security threat, or an application problem — before your users do. Mazu provides two types of behavior analysis: automated heuristics supplied by Mazu that run out-of-the-box with no configuration or maintenance, so they provide immediate and ongoing value with no effort. And custom policies that you define using a point-and-click interface to look for specific conditions that you want to monitor. Both types of analysis use the global behavior profiles that Mazu automatically and continuously updates to reflect the changing nature of your network activity. Mazu's behavior analysis provides you with a low-effort, low-noise, high-value way to ensure that your network is operating properly and securely.
- **Superior integration with security and networking solutions** — Works with your existing environment and operations. Mazu adds value to the networking and security tools you currently have through Mazu's two-way integration with over 30 products, including network management systems, security incident/event management systems, identity management solutions, intrusion prevention/detection systems, vulnerability management products, routers, switches, and sensors. These integrations work out-of-the-box. For custom integration needs, Mazu offers a unique API that allows vendors and customers to build their own integrations. Mazu's extensive integrations allow you to add Mazu's Network Behavior Analysis into the operational models and management systems you have today or may use tomorrow.

Conclusion

The Mazu NBA system can significantly reduce the time it takes to identify and resolve performance issues on the network. By delivering continuous global visibility into how users, applications, hosts, and devices are behaving on your network – including how their current activity differs from their typical behavior – the Mazu NBA system can enable your team to troubleshoot performance issues 7-10x faster.

MAZU NETWORKS

About Mazu Networks

Mazu Networks provides continuous global visibility into how users, applications, hosts and devices are behaving on a network, and detects if there are meaningful changes from their typical behavior that indicate a network performance issue, a security threat, or an application problem. Through Mazu, enterprises understand usage patterns, consumption rates and dependencies between users, applications and network infrastructure. Only Mazu offers continuous global visibility, automatic and custom behavioral analysis benefits for network operations and security and superior integration with network and security products. Mazu Networks' customers optimize their network operations, secure their internal networks and maximize application availability.



Mazu Networks

125 CambridgePark Drive
Cambridge, MA 02140
Tel (617) 354-9292
Fax (617) 354-9272
www.mazunetworks.com



Solution Centre Limited
Vickers House
Priestley Road
Basingstoke, RG24 9NP.
Tel: 01256 818600
Fax: 01256 819600
E-Mail: sales@solutioncentre.co.uk
www.solutioncentre.co.uk