

WHITE PAPER

**Reduce the Headache of  
Infrastructure Change in  
Five Steps**

## Executive Summary

Optimizing planning and minimizing disruption are goals for any infrastructure change project. Whether you are managing virtualization, voice/data convergence, a data center migration, disaster recovery planning, or new application rollouts, you need to know what is happening on your network both now and historically, what is typical, and who or what could be affected by the change. This kind of holistic visibility is critical in order for you to make the best business decisions possible. Many of the tools used today provide pieces of the information but they do not provide a holistic view of activity across the entire network that shows 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.

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

The Mazu NBA system provides the continuous global visibility you need at every stage of the infrastructure change process to optimize planning, minimize disruption during deployment, maximize availability on an ongoing basis, and quickly troubleshoot issues. Mazu offers five opportunities throughout the infrastructure change process for optimizing and accelerating infrastructure change.

- **Pre-change planning**
  - 1) Better understand your pre-change environment
  - 2) Real-time and historical information for better planning
- **Change deployment**
  - 3) Minimize deployment disruption
- **Post-change monitoring and support**
  - 4) Accelerate problem identification and resolution
  - 5) Improve support capabilities and reporting metrics

# The Challenges of Planned Infrastructure Change

No matter how well prepared you are, managing change in the network infrastructure can be a bumpy process.

No matter how well prepared you are, managing change in the network infrastructure can be a bumpy process. There are many infrastructure changes that can cause significant problems for an organization if they are not appropriately planned, implemented, and supported with the right practices and technology. But “infrastructure change” is a very broad term that encompasses a wide range of activities and challenges. Following are just a few examples of projects that require infrastructure change with some common challenges highlighted\*.

**Virtualization** – It is difficult to have a clear understanding of who is accessing computing resources such as disk arrays or virtual machines in a virtualized environment. How do you:

- Ensure that network and application traffic is sufficiently distributed so that no single section of the infrastructure is overloaded, especially at certain times such as end of quarter or overlapping time zones?
- Protect these systems against internal security breaches?
- Optimally schedule change windows?

**Voice/data convergence** – Adding a response-time-sensitive and business-critical technology such as VoIP to the network infrastructure requires an understanding of critical information about the network that can be very difficult to get. How do you:

- Ensure that all VoIP traffic is running across the dedicated VLAN?
- Know whether other applications running with the VoIP are creating congestion that affect VoIP call quality?
- Know whether performance of other applications has suffered since the VoIP was deployed?

**Data center migration** – Most organizations will need at some point to relocate, consolidate, expand, or segment their data centers due to growth, mergers and acquisitions, or other organizational change. This can be extremely challenging. How do you:

- Know what applications will be affected?
- Know which users will be affected?
- Identify all the services that are in use within the current infrastructure?
- Identify how applications are used to ensure that prioritization maps to actual business usage?

---

\*Mazu Networks has usage briefs that cover each of these specific areas. These documents are available on [www.mazunetworks.com](http://www.mazunetworks.com).

One area where many organizations struggle is finding the right tools and processes to gain a holistic view of activity across the network.

**Disaster recovery planning** – In order to develop an appropriate disaster recovery plan that will allow for a business to continue operation in the event of a serious disruption, how do you:

- Know which applications are the most important to the business and must be able to transition to the backup sites?
- Understand which services (DNS servers, DHCP, etc.) those applications require to function properly at the backup site?
- Know which applications are used but will not be supported during the disaster recovery process?
- Understand the bandwidth usage for each application – especially in cases where hot sites are distributed – as opposed to aggregate bandwidth data?
- Monitor post-transition any resources, users, and dependencies that did not make the transition or are not behaving as expected?

**New application rollouts** – Rolling out large applications – such as CRM, ERP, SFA, HER, etc. – is challenging to ensure that the application functionality is made available to the users who need it without creating adverse affects on the network infrastructure. How do you:

- Understand pre-deployment who uses which services and components of existing applications?
- Quickly identify post-deployment performance or availability issues?
- Understand who consumes the application's resources and when they are consumed for tracking and future planning?

No matter how your infrastructure is changing, your goal is to optimize the planning and minimize the disruption for the change. All of the challenges outlined above can be addressed, but to do so you need to know what is happening on your network both now and historically, what is typical, and who or what could be affected by the change. This kind of holistic visibility is critical in order for you to make the best business decisions possible.

### **There's a Gap in Technologies**

One area where many organizations struggle is finding the right tools and processes to gain a holistic view of activity across the entire network. While there are many tools and approaches on the market today, most suffer limitations. Many tools provide visibility in areas where they are physically connected and for specified conditions. Link-based solutions provide only a piece of the picture. Fault-driven technologies are “noisy” and focus on alerts and snapshots. In addition, deployment of many of these solutions requires a costly array of agents, probes, or inline devices that ultimately increase the complexity of your infrastructure. Other technologies work very well for specific tasks but can't effectively be “stretched” to watch the wire, not just the end points. Similarly, troubleshooting tools (e.g. protocol analyzers or IDS/IPS) are effective when you know what you are looking for and where it is likely to be found; they won't, however, show you what happened before an event occurred that precipitated the problem.

To fill the gaps, 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.

Mazu provides the continuous global visibility you need at every stage of the infrastructure change process to optimize planning, minimize disruption during deployment, maximize availability on an ongoing basis, and quickly troubleshoot issues.

## Network Behavior Analysis Fills that Gap

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 systems, users, and applications inside the network and continuously monitors their activity, alerting operations teams of security events, performance issues, and policy violations.

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 at every stage of the infrastructure change process to optimize planning, minimize disruption during deployment, maximize availability on an ongoing basis, and quickly troubleshoot 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 improve and accelerate infrastructure change by improving your ability to plan, deploy, operate, and support your network systems.

# Five Opportunities for Improvement

The continuous global visibility that Mazu provides offers a number of advantages that enable network professionals to optimize and accelerate their infrastructure change projects. Following are examples of five opportunities throughout the infrastructure change process – from pre-change planning to deployment of the change to post-change monitoring and support – where Mazu provides unique capabilities for improvement:

- **Pre-change planning**
  - 1) Better understand your pre-change environment
  - 2) Real-time and historical information for better planning
- **Change deployment**
  - 3) Minimize deployment disruption
- **Post-change monitoring and support**
  - 4) Accelerate problem identification and resolution
  - 5) Improve support capabilities and reporting metrics

## Mazu in Action

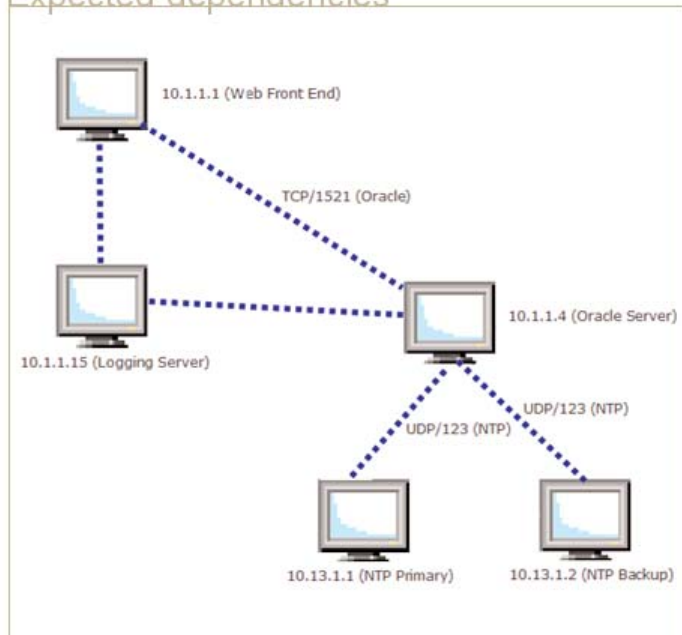
A large financial organization was planning to move its data center to a new location. Mazu was implemented just prior to the move and immediately showed that there were a number of applications on the system that were either improperly documented or completely unknown to IT. Mazu also demonstrated that the number of users who were accessing data center services was significantly higher than they had accounted for. Because Mazu was not available during the planning process, the company had used incomplete application documentation and out-of-date network maps. If the migration had moved forward, a number of critical applications would have been rendered non-functional and the business would have suffered serious disruptions. As a result, the company postponed the move and integrated Mazu into the planning process.

## 1. Pre-Change Planning: Better Understand your Pre-Change Environment

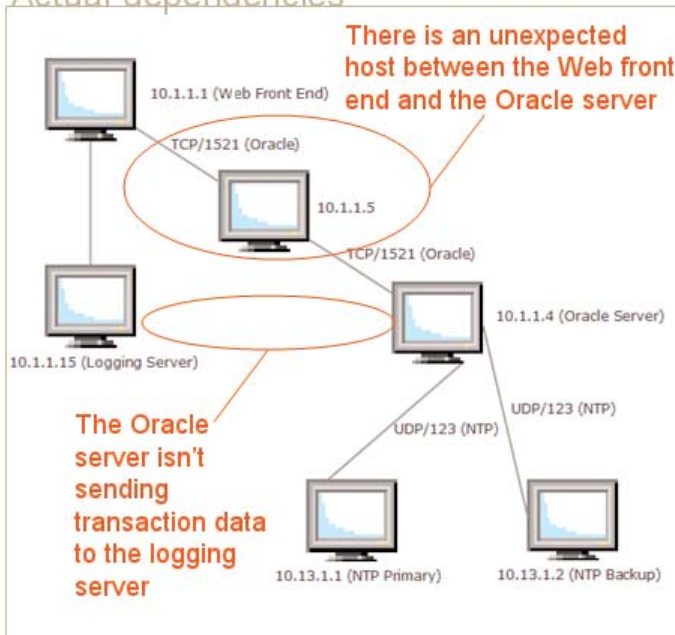
Before you make any changes, it is important to understand the current environment. This is usually a piecemeal process with data gathered from inventories, old project plans, and interviews. Even if you can construct a complete picture, it will reflect what you *think* the current environment looks like, not what is *actually* happening. Mazu can easily and quickly provide you with a complete inventory of all applications running and with current and historical profiles that include bandwidth, use, and dependency information. This inventory helps you:

- **Identify undocumented applications** – Unauthorized applications can be eliminated from the infrastructure. Authorized but undocumented applications can be incorporated into the planning process to reduce surprises during deployment.
- **Understand activity on the network** – Identify the route path of network activity. Understand the dependencies on the network. Understand bandwidth consumption. Identify which application resources are being used and by whom. See which ports and protocols your applications use and how different applications, ports, and protocols interact with each other in real time. Identify servers, hosts, and clients who are generating abnormal levels of traffic and identify whether that traffic is related to a security breach. Compare your current application architecture library to how the applications are behaving.
- **Uncover trends** – Understanding bandwidth usage over time, who consumes applications, and consumption fluctuations over time gives planners more complete information to incorporate into the process to build in appropriate thresholds.

### Expected dependencies



### Actual dependencies



Mazu identifies actual dependencies which may differ from expected behavior to enable you to implement changes without surprise consequences.

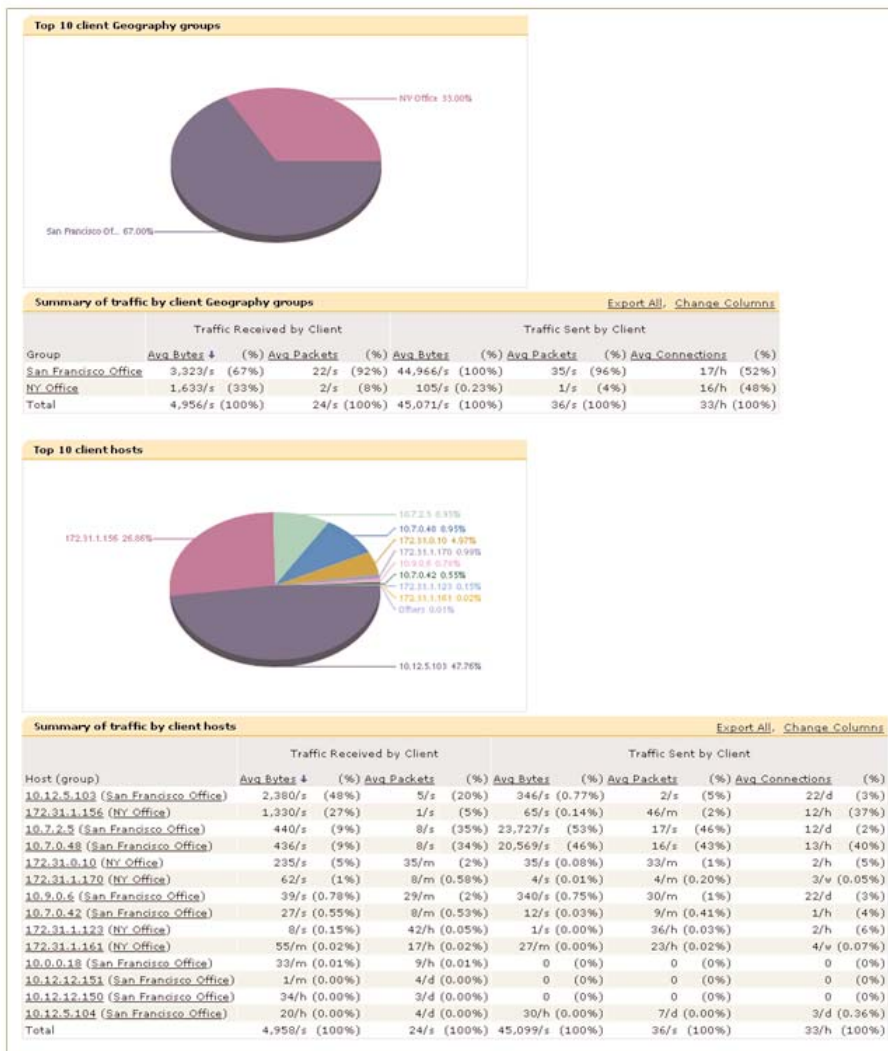
## Mazu in Action

To accommodate recent growth, a financial organization was migrating to a new data center. A particular set of securities trading applications housed in the old data center were a critical component of their operations; if the servers were not running, the company could not effectively trade securities. Therefore, these servers needed to be moved together at a time when the least number of users would need them. With Mazu, the company was quickly able to see who used the applications, as well as when they were most and least often used, helping them determine the best time to perform the move. During the move, they used Mazu to monitor the progress of the transition, noting new users as they came on line, and ensuring that the transfer was completed successfully.

## 2. Pre-Change Planning: Real-Time and Historical Information for Better Change Planning

Once you understand the current environment, you want to ensure that you have a complete plan to get you where you need to go and that you understand what it will look like when you get there. Mazu provides you with the information you need to:

- **Perform a gap analysis** – A gap analysis helps you evaluate what needs to be done and can uncover important requirements. Mazu shows you what you have, who uses it, where it is used, and how it is used, and the dependencies. You can then compare this information to the plan and identify the gaps that need to be filled.
- **Perform impact analysis** – Once you've identified your plan, Mazu can show you what the impact of implementing that plan will be on the network. This helps minimize unintended consequences during deployment.
- **Uncover trends** – Understanding bandwidth usage over time, who consumes applications, and consumption fluctuations over time gives planners more complete information to incorporate into the process to build in appropriate thresholds.



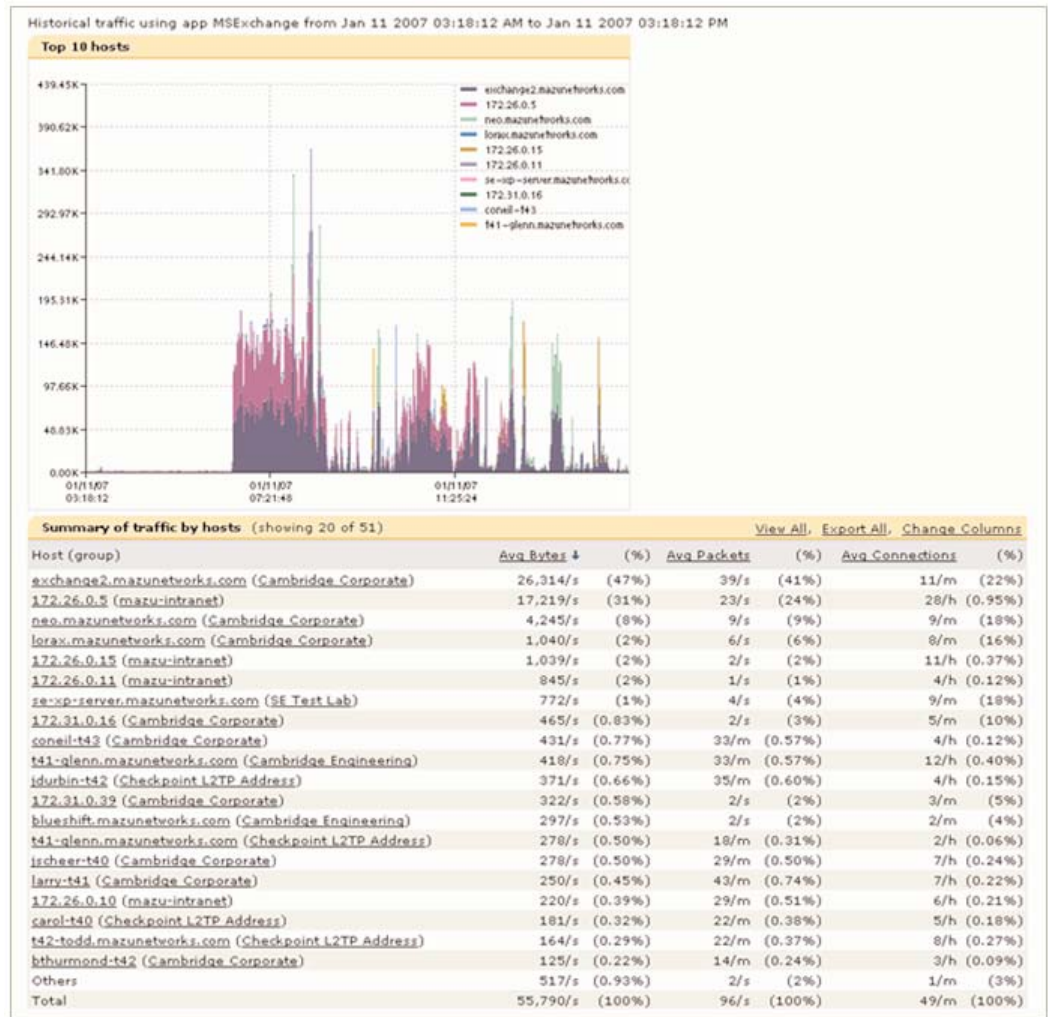
Mazu can show the impact of a proposed change. For example, the screen shot to the right shows which remote offices – in this case, the San Francisco and New York offices – and which hosts in those offices will be affected if a specified application is taken offline.

### 3. Change Deployment: Minimize Deployment Disruption

#### Mazu in Action

A customer who used Mazu during the roll-out of a new Citrix implementation was able to quickly identify spikes in traffic that were slowing down the application. They were able to quickly resolve the issue before it became a widespread problem, and were able to stay on their deployment schedule.

Even the most carefully planned changes can cause unexpected problems such as network slowdowns and interruptions in service or application availability. Mazu enables you to minimize these problems by comparing current behavior to historical norms. As the deployment is underway, Mazu can evaluate how users, applications, servers, etc. are currently operating and compare that to historical norms to flag problems. This enables the deployment team to proactively identify a problem rather than having to rely on users' complaints. In the event that a problem is identified, Mazu helps isolate the problem and identify solution areas by providing information about what led up to the disruption, who is affected, and what applications/systems/hosts are involved. Mazu delivers time savings throughout the deployment process; being able to quickly identify behavior changes, understand why the behavior changed, and verifying that a problem has been resolved helps reduce the time needed to resolve issues.



Mazu can provide real-time data that shows the progression of a deployed change and helps the team quickly identify trends or potential issues that could affect the success of the deployment.

## Mazu in Action

An energy company was experiencing significant VoIP issues – leading to litigation with customers over dropped calls – but was unable to identify the cause. The IT staff had been working on this problem for weeks without success. As soon as they installed Mazu, they were able to resolve the issue in just a few hours. Mazu quickly identified several VoIP components that were sending data to a decommissioned VoIP gateway. There was, naturally, no response from the gateway and all traffic from these devices was dropped. With the information that Mazu provided, the company was able to quickly fix the mis-configuration and resolve the problem.

## 4. Post-Change Monitoring and Support: Accelerate Problem Identification and Resolution

Ensuring performance and availability beyond the deployment is necessary for ongoing support. To do this, you need to be able to quickly detect problems, identify root cause, formulate and implement a fix, and verify successful resolution. This acceleration allows IT staff reduce the time needed to resolve critical business problems related to infrastructure change planning and deployment.

- **Identify meaningful changes** – Mazu continuously monitors the current network activity against typical and expected behavior. Mazu identifies meaningful changes enabling you to act quickly to resolve any issues before they have a serious operational or security impact on the environment.
- **Identify root cause** – Because Mazu shows you not just what happened at the time of the problem, but what activity and behavior led up to it, you have important information to help you determine the root cause of the problem.
- **Formulate and implement a fix** – Once the root cause has been identified, you can formulate an appropriate response. Mazu's impact analysis capabilities enable you to identify who is affected to ensure that your response doesn't create unintended consequences. This also enables you to be proactive and helps prioritize resolution actions during a large or complex event.
- **Verify success of fix** – After the resolution has been implemented, you can ensure that network activity is back to normal.

**Mazu identifies meaningful changes that could represent operational or security risk to the environment.**



## Mazu in Action

The network engineering team at a financial firm is routinely notified of new applications to be deployed. Unfortunately they often receive these notifications just prior to the deployment instead of during the planning process. Since experience has shown that new applications usually cause problems in the operating environment, they try to delay the deployment until they can model the application. The modeling tools they used, however, did not monitor availability or behavior of an application after it has been deployed. The IT department now uses Mazu to “fingerprint” the relationship of the distributed components of the applications using rule-based events. If applications violate the rules, the network team is notified. This enables the group to more successfully support the organization as it rolls out new applications and services to users.

## 5. Post-Change Monitoring and Support: Improve Support Capabilities and Reporting Metrics

Ongoing support and appropriate reporting metrics are necessary to ensure that the IT environment keeps pace with the requirements of the business and to improve planning for the next iteration of the infrastructure change.

- **Create and enforce policy** – With the continuous global visibility Mazu provides into the behavior of users, applications, hosts, and devices on the network, you can develop appropriate access and usage policies. Furthermore, Mazu can alert you when violations occur, enabling you to not just develop policies but to enforce them.
- **Reporting** – Because Mazu collects and saves information about all the activity across the entire network, virtually any type of report can be generated for a variety of needs including measuring QoS metrics, capacity and usage analysis, planning, audits, just to name a few.

New Rule Based Event

<b>Identification</b>	<b>Schedule</b>
Name: User Policy Violation	Days to run rule: <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Description: Alert when hosts are using unauthorized applications	Start time: 00:00:00
Enabled: <input checked="" type="checkbox"/>	End time: 24:00:00
<b>Host/Group A</b> Look Up...	<b>Host/Group B</b> Look Up...
Select: <input type="radio"/> Any <input checked="" type="radio"/> Within <input type="radio"/> Outside Internal Hosts	Select: <input type="radio"/> Any <input checked="" type="radio"/> Within <input type="radio"/> Outside External Hosts
Statistics: Track Per Host	Statistics: Track In Aggregate
Role: Client	Role: Server
<b>Service</b> Look Up...	<b>Threshold</b>
Select: <input checked="" type="radio"/> Any <input type="radio"/> Within <input type="radio"/> Outside	Threshold: Upper Limit
	1 Bytes per Sec.
	Direction: A to B or B to A
	Duration: 00 hours 01 minutes
	Severity: 70
	Notification: Low Default Medium Default High Default
<b>Application</b> Look Up...	
Select: <input type="radio"/> Any <input checked="" type="radio"/> Within <input type="radio"/> Outside gmail Limewire eDonkey Go To My PC.com Skype Kaza	

Mazu enables you to write custom policies to be alerted when specified violations occur.

## ► 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 contribute significantly to the success of planned infrastructure change. 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 can be a key component for optimizing and accelerating infrastructure change throughout the entire lifecycle from planning to deployment to ongoing monitoring and support.

# 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's 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](http://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](mailto:sales@solutioncentre.co.uk)  
[www.solutioncentre.co.uk](http://www.solutioncentre.co.uk)