



# Xangati for Cyber Counter Intelligence (CyberCI)

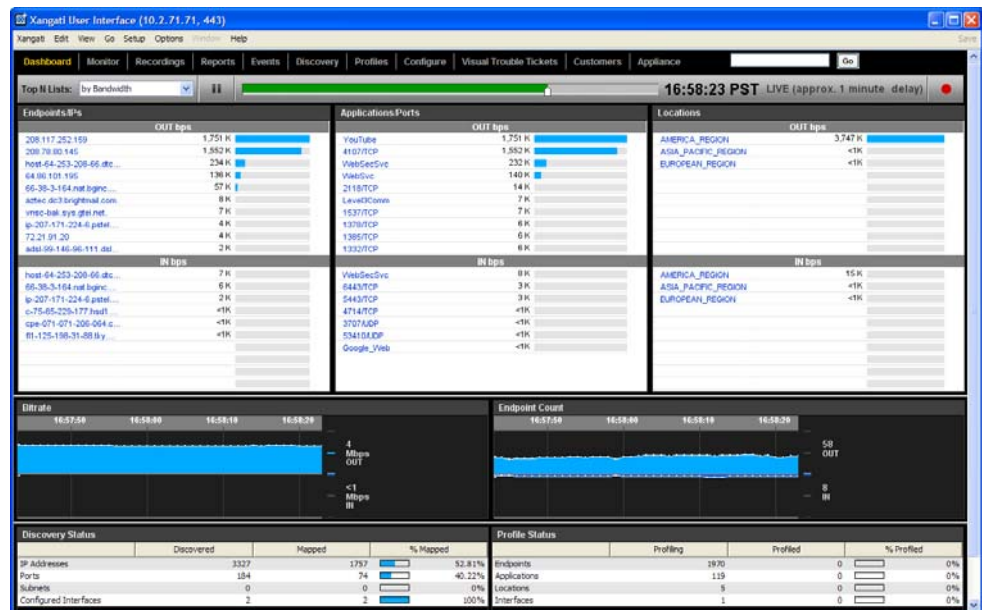
## Description

The live visibility of the Xangati Application Management 2.0 appliance is being leveraged by governmental organizations to have a clear view into traffic coming onto their networks from the outside world. In this deployment model, the Xangati solution is tracking the application activity of external IPs/endpoints with respect to interactions they are having with networked resources on the governmental organization's network. This information is invaluable to organizations trying to understand either what traffic is targeting their infrastructure and/or what is getting through to their infrastructure—what information is collected is ultimately determined by where the “NetFlow” information is gathered (in other words which side of the firewall).

And because this information is presented live someone in the Network Operations Center (NOC) or CyberSecurity Operations Center (CSOC) will always have acute visibility into activity without having to filter through a ton of log data.

*"Xangati fights fire with fire.*  
Xangati's most recent initiative is maybe the most exciting thing to happen to network management since the MoM. The company is applying concepts from the Web 2.0 world like streaming, collaboration and user-generated content to bring network and application management into this century."

—Zeus Kerravala, SVP,  
The Yankee Group



The Xangati dashboard gives live visibility into traffic coming onto the network from the outside world.

## Features

### Live to-the-second visibility

See activity as it happens for any identified external endpoint or unmapped external IP

### Mapping/tracking external IPs

Link the IP addresses to a DNS name for historical tracking or leverage the real-time WHOIS look-up capability of the system that identifies the ownership of the unmapped IPs



## AWARDS



GARTNER COOL VENDOR, 2009



STARTUP TO WATCH IN 2009



TOP TECH STARTUP, 2008



IT MANAGEMENT SOFTWARE TO WATCH, 2008



INFORMATION WEEK STARTUP 50, 2009



NEW PRODUCT OF THE YEAR, 2009 FINALIST



TECH STARTUP THAT MATTERS, 2007

### Multiple live top ten dashboards

- Top IPs in terms of bandwidth sent into/received from the organization
- Top IPs in terms of number of endpoints communicated with inside the organization
- Top apps/protocol ports in terms of bandwidth sent into/received from the organization
- Top apps/protocol ports in terms of number of endpoints communicated with inside

### DVR recording capability

Ability to record *any* dashboard, *any* IP (whether mapped as an endpoint or not) and even the conversation between two communication pairs. These recordings are available to be replayed at anytime and can even be emailed to peers.

### Historical reporting

For the external endpoints that have been mapped through DNS, the system will also be able to keep a 12-week reporting history in terms of their interactions with the governmental organization. For unmapped IPs, there are also reports that can be generated to track the top ones most active in communicating with endpoints within the organization. In addition, that information can be exported from the system and be data mined as an external database for longer time periods.

### Profiling/event alerting

For the external endpoints that have been mapped through DNS, the system will try to learn the activity pattern for that object. If the behavior of that object fits a profile, the system will establish it after a couple of weeks on the network. And if the object exceeds or falls below a profile threshold, the system can alert on that as well as it can trigger an event DVR recording. Profiles can also be manually adjusted if desired.

### For More Information

To learn more about the Xangati Application Management 2.0 solution, visit [www.xangati.com](http://www.xangati.com) to view product feature demos, watch customer videos and even take a test drive of the system.

