SOLUTION BRIEF

IT Infrastructure Monitoring Strategies for the BYOD World

AccelOps' integrated security, performance and availability monitoring application allows you to confidently and securely support mobile device access to sensitive corporate IT resources

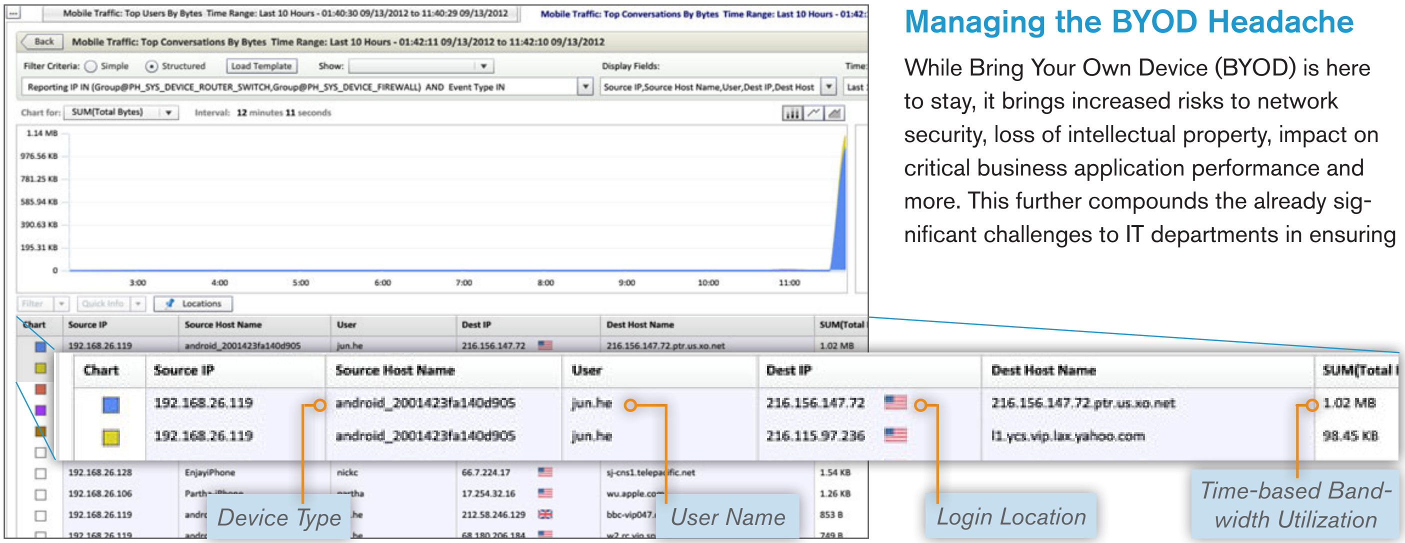
- Protect corporate networks from threats
- Control device activity
- Ensure key business application SLAs
- Safeguard intellectual property
- Detect unauthorized mobile devices
- Meet compliance requirements

Bring Your Own Device (BYOD) – It's Here to Stay

Just a few years ago, workers were limited by corporate policy to connect only company-issued devices to the network – desktop computers, laptops, and even smartphones. All that changed, arguably with the introduction of the iPhone and without a doubt, the introduction of tablet devices. The iPhone was not a device initially supported by most companies. But users embraced it and it became the most popular smartphone in the world. Naturally, employees wanted to use the same device for business purposes as well as personal. Now, there are even more choices.

Numerous studies have proven that giving employees their choice in mobile devices improves both productivity and job satisfaction. Workers use personal devices from home, on the road, and on the weekend to keep up with business demands. And they use personal applications during business hours.

As a result, companies are increasingly loosening policies to allow employee-owned devices to connect to corporate resources. More than 75% of the knowledge-based workforce uses a mobile device to access the corporate network. The typical knowledge worker now averages 2.8 devices that may connect to the network.   AccelOps makes this a no-compromise decision.



AccelOps' software reports device type, user names, login locations, and time-based bandwidth utilization. Rules based on this information can trigger automatic actions.

Mobile Traffic: Top Users By Bytes Time Range: Last 10 Hours - 01:40:30 09/13/2012 to 11:40:29 09/13/2012

Mobile Traffic: Top Conversations By Bytes Time Range: Last 10 Hours - 01:42:

Back | Mobile Traffic: Top Conversations By Bytes Time Range: Last 10 Hours - 01:42:11 09/13/2012 to 11:42:10 09/13/2012

Filter Criteria: ○ Simple ● Structured

Reporting IP IN (Group@PH_SYS_DEVICE_ROUTER_SWITCH,Group@PH_SYS_DEVICE_FIREWALL) AND Event Type IN

Display Fields: Source IP,Source Host Name,User,Dest IP,Dest Host

Chart for: SUM(Total Bytes)

Interval: 12 minutes 11 seconds

Chart	Source IP	Source Host Name	User	Dest IP	Dest Host Name	SUM(Total
🟦	192.168.26.119	android_2001423fa140d905	jun.he	216.156.147.72	216.156.147.72.ptr.us.xo.net	1.02 MB
🟨	192.168.26.119	android_2001423fa140d905	jun.he	216.115.97.236	l1.ycs.vip.lax.yahoo.com	98.45 KB
□	192.168.26.128	EnjayiPhone	nickc	66.7.224.17	sj-cns1.telepacific.net	1.54 KB
□	192.168.26.106	Parth	artha	17.254.32.16	wu.apple.co	1.26 KB
□	192.168.26.119	andr	he	212.58.246.129	bbc-vip047.	853 B
□	192.168.26.119	andr	he	68.180.206.184	w2.rc.vip.sp	749 B

Managing the BYOD Headache

While Bring Your Own Device (BYOD) is here to stay, it brings increased risks to network security, loss of intellectual property, impact on critical business application performance and more. This further compounds the already significant challenges to IT departments in ensuring

BYOD Security Scenario

Ryan Bolger was in the boarding area during a long layover at Heathrow Airport, on his way to a business meeting in Rome. He turned away only for a minute, but his iPad and his notebook were gone! He frantically looked around the gate area, but they were nowhere to be found. Luckily, his presentations for the week were on his laptop, safely in his computer bag.

Several hours later while Ryan was in flight to Italy, IT was alerted back at headquarters that Ryan was logged into the network on his iPad from an Eastern European country and was attempting to download engineering documents. Fortunately, IT was using AccelOps to monitor their infrastructure and pre-defined rules that included the list of countries in which the company did business. Any activity that violated one or more of those rules would trigger an alert as well as a script to automatically log off the offending device. The AccelOps event log also showed several failed login attempts since the thief had tried several different passwords Ryan had written down in the back of his notebook.

security, performance, and availability across the distributed IT infrastructure.

Next generation monitoring tools are needed to track user and mobile device activity, quickly remedy security breaches, and manage impacts to business application performance. To effectively monitor mobile devices, tools require additional context. For example, user identity and location information can provide the contextual intelligence necessary to identify a stolen device, possibly even before its loss is reported.

AccelOps Mobile Device Monitoring

When a mobile device logs in to the network, AccelOps identifies the device by IP address, MAC address, device type (iPhone, iPad, Android device, Blackberry, etc.), WLAN access point. As soon as the mobile user authenticates for network access, AccelOps combines the WLAN logon event with the user identity including the user name and his/her geographical location based on the logon IP address.

Once the mobile user initiates traffic, AccelOps correlates network flow information with the device metadata, providing complete visibility. The application monitors all activity against corporate policies including access privileges, allowable bandwidth utilization, and even which applications may be accessed remotely and which may not. Violations of a policy will generate alerts to notify IT administrators and can even trigger the execution of scripts to automatically log the offending device off the network and blacklist it in order to prevent future logins.

AccelOps' integrated security, performance and availability monitoring application allows you to confidently and securely support mobile device access to sensitive corporate IT resources.

About AccelOps

AccelOps is the industry's first application that integrates security (SIEM), performance, and availability monitoring in a single platform. We architected our monitoring solution from the ground up with the scalability and performance required for today's virtualized and cloud architectures. Unlike software suites built from disparate applications, we simultaneously monitor security, performance, and availability across your entire infrastructure – both physical and virtual – in a single application. Real-time analytics aggregate and correlate cross-domain activity, events, and incident data providing IT with service-level visibility and actionable intelligence. AccelOps is a software-only monitoring solution that runs on a VMWare ESX or ESXi virtual appliance and scales easily by adding virtual machines.

AccelOps, Inc.
2901 Tasman Drive, Suite 100
Santa Clara, CA 95054
USA

Web: www.accelops.com
Tel: 1 (408) 490-0903
Email: sales@accelops.com

accelops