## Cover Focus Articles

***General Information***
*October 8, 2010 • Vol.32 Issue 21*
*Page(s) 24 in print issue*

# Understanding App Usage

## Get A Better Handle On Who s Using What Applications & How Often

Although some companies allow employees to use all available applications, there are distinct advantages to having more in-depth knowledge about who's using which program and to limiting usage based on productivity and appropriate use.

### Key Points

• Tracking application usage can benefit an enterprise in numerous ways, including licensing, productivity, accountability, and bandwidth management.

• To get a handle on app usage, consider a flow management solution that can report on different types of traffic on the network.

• An app usage policy should clearly set out the guidelines for access, including which departments have access to which applications, and should include what will happen if applications are accessed or used inappropriately.

"Determining application usage has several advantages throughout the company," says Daniel O'Connor, product manager at AppSense (www.appsense.com), a provider of virtualization solutions. "There's benefit in terms of licensing and making sure that the people can run the correct applications they are licensed for."

Also, a large percentage of network bandwidth is consumed by applications, adds Marina Gil-Santamaria, director of product marketing for the Network Management Division at Ipswitch (www.ipswitch.com), and many of those apps are consumer-oriented external applications such as social media sites and toolbars.

"Tracking cross-departmental application usage can help maintain departmental productivity, as well as manage corporate bandwidth costs," she says. "When dealing with internal applications, determining departmental application usage could also help with auditability and accountability."

### Get A Clear View

In order to obtain a good look at who's using what application, Gil-Santamaria suggests that IT managers should go deep into their flow data and look for a flow management solution that will let them analyze, alert, and report on the different types of traffic traversing the network.

Each flow-enabled router or switch collects and aggregates information about traffic passing through it, she notes, and when configured to do so, it transmits the info to a flow-enabled network management and monitoring system. This can help a manager understand which users, applications, and protocols are consuming bandwidth and also gives insight into the quality of service received by all applications, especially those that are mission-critical.

The strategy can also help in verifying ISP billing and properly planning for spikes in

bandwidth usage, potentially resulting in fewer dropped packets and delays. Finally, this type of analysis can protect a network by tracking traffic anomalies, helping to detect viruses and worms on the network.

Another strategy is to build a usage profile for the application and its associated data, says Jon Heimerl, a director of strategic security for Solutionary (www.solutionary.com), an information security firm. “The brute-force method is to perform an information asset inventory,” he says. “Each type of data is associated with its relevant applications. All staff members are functionally denied access to any application and data. Then, on a case-by-case basis, users or a user group are granted explicit access based on a manual review of all users and user groups by some set of knowledgeable staff within the organization.”

An “access review” process is probably more realistic, though, Heimerl notes. In that case, IT compiles a list of all current user IDs that have access to the applications, and IT staff review the currently “as-built” access, approving continued access for known, authorized personnel and removing unauthorized personnel.

“In either case, user access is best controlled by managing group and profile access rather than managing individual access,” he says.

### Don’t Forget Mobile

It’s important to add mobile applications into the overall plan, as well, because monitoring mobile usage is vital for cost control, security, and policy management, notes John Blyzinskyj, president of software firm Avotus (www.avotus.com).

“Implementing a comprehensive inventory and usage management system is central to gaining and maintaining control over mobile usage,” he says. “These systems track who is using which devices, how much cost they are incurring, and what their pattern of usage is.”

When coupled with effective policy enforcement--including device and plant selection, rate plan optimization, and unapproved use policies--IT managers can reduce their costs, improve policy compliance, and reduce risk without impacting usability, Blyzinskyj notes.

### Address App Misuse

Creating a culture of accountability can sometimes be tricky. Zohar Gilad, executive vice president for Precise Software (www.precise.com), notes that quite often, departments don’t want others to have visibility into their activities or software assets.

“They are afraid of transparency,” he says. “For example, a user of an HR application may not want a database administrator or user from another department to have visibility into what’s happening on his or her turf.”

Because of those sensitive issues, having a strong user application policy is crucial, as well as articulating what will happen if applications are used improperly.

If an employee goes against policy and is accessing applications inappropriately, the handling of the situation will really depend on how the app is used, Gil-Santamaria notes. For example, if someone in the accounting department is watching online videos and consuming bandwidth, the response might be to prevent that person from accessing the Web or to issue a warning.

But if that person works at a healthcare services firm and gets curious about a particular patient’s data, the response would be very different because it constitutes a compliance violation. In that case, there should be a real-time notification in writing and an activation of well-defined response policies.

Heimerl says the ultimate question when creating an app usage policy and enforcing it should be “Does the employee need access to do his or her job?” If the answer is no, then there should be no access, and if the answer is yes, then it’s time to determine the level of access that’s needed.

““There will be times when reviewing staff just don’t know if access is appropriate,” he says. “In such a case, they must take time to review, discuss, and decide on allowing or disallowing access. More often than not, this almost always comes down more to someone’s feelings being hurt than it does to a technical issue.” ■

*by Elizabeth Millard*

## Top Tip: Create An Overview Document

Rather than simply employing app usage tracking software, the effort should be a larger strategic plan, believes Marina Gil-Santamaria at Ipswitch (www.ipswitch.com). She notes that it's important to prepare an overview document containing project scope, goals and objectives, constraints, and high-level risks. The document should be reviewed and agreed upon with all key stakeholders and should be re-reviewed when new applications are deployed or re-architected. She says, "Also, if this initiative is driven by security or compliance regulations, you might rally more support than when you are focused mainly on internal accountability."