Report – Q3 2016

BDNA State of the Enterprise Report

Breaking Away from the Vicious Vendor Audit Cycle

Vendor software and hardware audits have become so common in the enterprise IT landscape that they are beginning to be accepted as "business as usual." In fact, almost two-thirds – 61 percent – of enterprises received a vendor audit request in the last 18 months, and 17 percent of those companies were audited three or more times in that period, according to a 2016 survey conducted by BDNA®.

Companies have adopted the habit of reacting to audit notices by scrambling to compile the relevant data – an incredibly time-intensive process – and then, when they are ultimately found to be out of compliance (as most companies are, given the convoluted nature of license agreements), most organizations have no choice but to capitulate and pay up. The fact is that few enterprises purposely misuse assets, but are instead caught out of compliance due to the increasing complexity of license usage policies.

But vendor audits don't have to create an annual (or semiannual) fire drill, and they don't have to become another time-consuming task to undertake and high cost to bear. By changing a few aspects of how IT technology data is managed, businesses can become proactive in managing their software and hardware assets, literally ending the vicious vendor audit cycle or avoiding it altogether.

The Audit Landscape

Vendors dedicate a great deal of energy to pursuing license audits because they have a very clear motivation to do so: The fines and payments they are able to collect as a result of non-compliance represent a significant revenue stream, stretching into the billions of dollars annually.

Some customers have singled out the largest software companies in particular as using a "gun to the head" approach to licensing negotiations. So pervasive is this practice that compliance consultancies have sprouted up that exist solely to help their clients manage their audits.

The number of audit requests has vastly increased in recent years, with no signs of slowing down. The requests come from the usual suspects: Microsoft, Oracle, Adobe, IBM and SAP. Against this backdrop, analyst firm IDC estimates that organizations will spend an average of 25 percent of their IT budgets on software license complexity in 2016.

In the meantime, being hit by an audit is an incredibly time-consuming and costly exercise, forcing organizations to redirect resources toward finding and compiling the requested information. Audit preparations impact overall operations, disrupting workflow during the audit process and pulling personnel away from their jobs. This in and of itself can be the most arduous part of an audit.

In addition to potentially carrying significant monetary penalties, an audit comes with an implicit message of mistrust that can sour business relationships: By routinely auditing, the vendor indicates it simply does not trust its customer to properly use its assets.

The Pitfalls of License Management

Businesses so often fail to properly adhere to their license agreements, and vendors find auditing so lucrative, because most companies lack visibility into which assets they have and how they are being used. A recent BDNA survey found that only 17 percent have IT asset management tools in place to manage compliance.

As the complexity and velocity of business increases, so does the potential for error. Many tools that claim to entirely automate license compliance and optimization can add to the problem, introducing unneeded complexity to an environment and only deepening the problem with new details to manage, such as cross-functional buy-ins and vendor license aggregation.

At the same time, license usage policies are becoming more complex. Product use rights can change without notice, the meanings of licensing terms differ from vendor to vendor, software use cases shift and virtualization can bring a whole host of issues. While this may be seen as a consequence of the broader technological shift in how business is conducted, some critics of vendor practices would see a deliberate effort to make license compliance practically impossible.

Eliminating Vendor Audits

Eliminating vendor audits is an achievable goal if organizations can do the initial groundwork to create a proactive position from which they can confidently respond to an audit notice, as opposed to a reactionary stance that automatically puts them on their heels. Luckily, achieving this position does not have to increase complexity; often the greatest ROI can be achieved by creating accurate visibility and knowledge of your entire asset inventory — essentially, an actionable, automated accounting of the entire IT estate.

Once an enterprise has a handle on its IT asset information, it can reconcile actual use against license constraints, and even set about to eliminate any violations before they're flagged by a vendor.

One executive from a leading global technology company who frequently deals with vendor audits said that being able to respond to an audit notice by showing a lean and automated practice will often end the audit process from moving past the initial stages.

"Demonstrating the maturity level with which you are taking care of your assets is vital," said the executive, who requested anonymity. "If a vendor asks you to provide a report, and you can comply with the request in an automated fashion through a comprehensive, established

EXCERPT FROM THE GARTNER SOFTWARE AUDIT TOOLKIT

Six Tips for Navigating a Vendor Audit

1. Create processes that provide transparency and efficiency during the audit, and that allow the organization to return to business as usual as quickly as possible, with minimal disruption.
2. Improve audit handling maturity by highlighting issues that need to be addressed as part of the process of continuous improvement.
3. Ensure confidentiality and security of data throughout the audit process. Many audit management processes focus on controlling audit activity and the ability to provide proof of compliance, but overlook the need to control and manage the data being shared as part of the audit.
4. Prepare for audits proactively and validate the output of software asset management (SAM) reporting.
5. Validate the compliance status of a specific product or set of products, which can help in the assessment and effectiveness of SAM processes, and identify control gaps and areas for improvement.
6. Evaluate SAM tools that can help you plan for improved SAM and audit management reporting.

Source: Gartner, "Toolkit: Surviving a Software Audit," Feb. 23, 2016

process, the vendor often accepts the information, and the audit process usually ends on friendly terms, without an aggressive on-site audit."

Ideally, this automated data enables on-demand visibility into what software and hardware assets are being utilized throughout your organization. So instead of scrambling to pull together the data to answer that first audit notice, this information can be instantly called upon to account for and justify every install.

More often than not, organizations that put this solution into place find not only that they save money by avoiding future audit penalties, but they are also able to see and eliminate the extraneous, unused licenses that they had been paying for, needlessly, for years, by simply eliminating shelfware.

Operating in a Post-Audit World

Once enterprises can embrace the fact that audits do not have to be part of their annual IT routines, they are empowered to find and implement the processes, tools and solutions that best fit their needs, and eliminate their susceptibility to audits. Ideally, an organization should be able to respond to any audit request letter by immediately providing an active accounting of their inventory, which stops the process dead in its tracks.

Having proper SAM and ITAM processes and tools implemented also allows organizations to have quick and efficient budgeting and forecasting. They know exactly what software is being utilized, and can proactively send POs to vendors to correct, update or true-up their licensing positions before they are discovered in an audit.

Deflecting on-site vendor audits has to be a deliberate undertaking, but it is one that is within every organization's reach.

Being fully and constantly prepared for a vendor audit should be part of your business DNA.

Beware Phony Audit Requests

Not every audit request your company receives may be legitimate. Sometimes malicious vendors, often from foreign countries in which you have a local office, mask themselves with official-looking government type requests, but are really just vendors trying to sell services.

An executive with a leading global technology company shared stories about receiving these fraudulent requests.

"The first thing we do when we receive an audit notice or request for information is to verify its authenticity," he said.

His company utilizes a team approach – a local IT representative, legal counsel, a purchasing representative and the managing director of the targeted country – to work on an audit request. The first step is to verify it's legit.

Verifying that an audit really comes from a government is necessary and rather straightforward.

If it's legitimate, providing the information requested in a timely, automated fashion is key, he emphasized.

About BDNA

BDNA® creates the most authoritative enterprise technology data. Armed with this invaluable information, enterprises will make the best decisions possible, lower costs and risks as well as accelerate the pace of their business. To produce the most relevant results, BDNA maintains Technopedia®, the most complete, current and reliable content repository about hardware, software and medical devices. This catalog is the foundation from which BDNA creates the highest quality enterprise IT data in the industry, which in turn results in visibility, insight and information enterprises can trust. Venture-backed and based in Mountain View, Calif., BDNA operates globally with customers across all segments and vertical markets. For more information, please visit **www.bdna.com**.

BDNA