SERVICE BRIEF

Understanding Shadow IT

Unauthorized software can be a major pain for network administrators.

The Detriments of Unauthorized Software

Can an organization's data and network security really be tested by unapproved applications?

When a business sets out to add to their IT, they often choose the solutions based on their immediate needs. This is because when trying to look to the future an organization cannot know what obstacles will pop up. For this reason your organization's IT department, whether you have in-house IT technicians or you utilize managed IT services from Indevtech, has to be the ones that handle the implementation and management of your crucial IT.

With so many malignant situations to navigate and threats to squelch, having a dedicated software deployment strategy for all of your company's needs is important. It is not uncommon for an employee to have several pieces of software on their workstation or device that haven't been approved for use by the organization. This is what is known as Shadow IT, and there are significant threats that every business owner, network administrator, and end-user will need to acknowledge in order to keep your organization safe.

Reasons for Shadow IT

In the continuous race that is business, sometimes end-users will find solutions that may do more harm than good.

Many times, workers will have everything they need to do their stated jobs. This includes hardware and software solutions. Typically, a business will buy licensed software that has been vetted by the IT department as secure and reliable for the production needs of a business. Any other software on the company-owned-and-managed workstation, tablet, or smartphone is Shadow IT. This can be simple titles such as third-party weather and traffic applications or games, but they are often applications users have downloaded deliberately to help them stay productive.

Shadow IT is often present in the software development world, where developers are constantly searching for software that can produce higher efficiencies in the management process, as well as the testing of new applications. This isn't the only place you can find Shadow IT, however. In many organizations, where there is no true uniformity to a software deployment strategy, and department heads decide what software works best for their departments, an organization's IT administrators are often mistakenly kept out of the loop.

Of course, user-implementation can have some pretty serious side effects. These Shadow IT applications are almost definitely set up outside the security solutions that protect your network, making them ripe for infiltration by nefarious entities. Shadow IT is serious business to your IT support team. Consider that they are the guards attempting to protect the gates of a giant, self sustained castle, only to have the people that work inside the castle order resources from outside the castle walls. Even if Shadow IT applications, and the data created with them, are fine, what happens the one time they aren't?

Solutions

To keep Shadow IT from putting your organization's network and data at risk, we suggest that your IT administrator consider these four practices:

- **Consolidate applications when you can.**—If you can find a solution to handle multiple needs, such as Microsoft 365 or Google Workspace, it makes your software (and the data it produces) significantly easier to manage.
- **Monitor user activity.**—By assessing what your employees upload, download, and share, you will be able to ascertain if you have all of your bases covered. You can also enforce policies to block risky app activity by eliminating functions that aren't core to the success of the application's organizational use.
- **Research applications.**—Your administrators should try to ascertain the possible risks an application could have, and choose whitelisted applications diligently.
- **Educate your users.**—Your organization will definitely want to have an understanding of every possible task and the risks of using software that is outside of the management capabilities of the organization.

Get proactive and call us TODAY!

(808) 529-4605| indevtech.com | info@indevtech.com

Indevtech Incorporated
Pacific Guardian Center, Mauka Tower
737 Bishop Street, Suite 2070
Honolulu, Hawaii 96813-3205