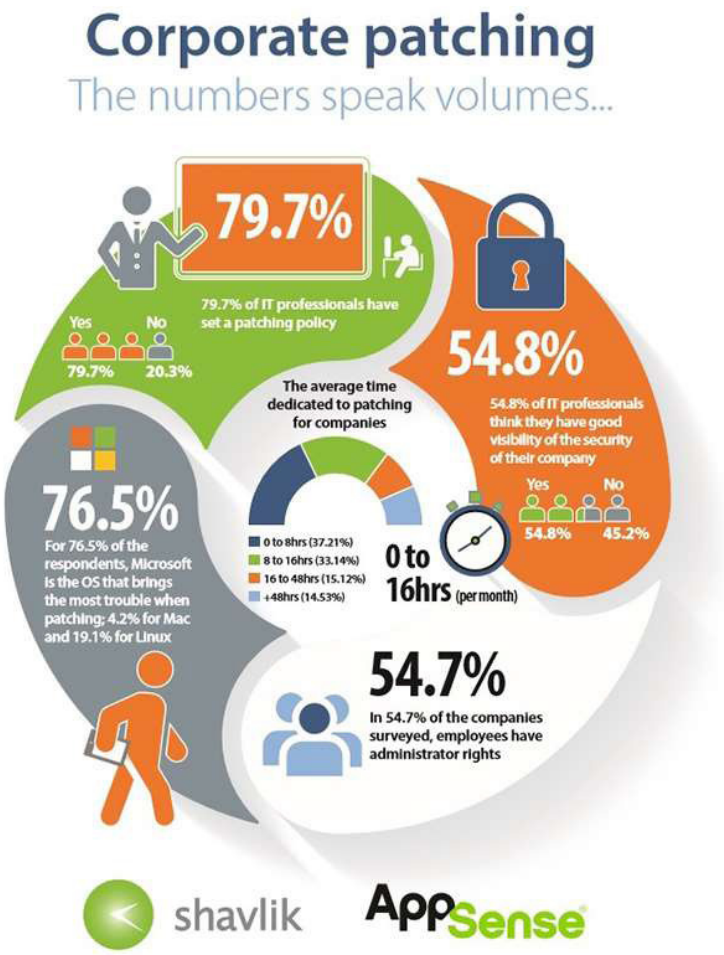
next I.T.

Patch & Security Management

Take 8 Hours Per Month For Most Companies

Patching the OS is only a small part of the equation when it comes to an effective patch management strategy.



When asked about the challenges of patching applications,

Java was mentioned as the most difficult application to update by 59% of respondents, followed by Adobe Reader/ Flash Player – 38%, Google Chrome – 21%, Firefox – 18% and Apple iTunes – 10%.

79.7% of I.T. managers have implemented a policy to manage patching, which is good news. However, while 37.2% report spending fewer than 8 hours a month on patching, 29.6% spend more than 16 hours a month, and 14% spend more than 48! This amounts to a day and a half on average for most organizations, which is far from efficient.

Finally, 54.7% of companies grant full administrative rights to their employees, making their systems more vulnerable to malware. This approach increases risk in the event of a malware attack, since there is no way to limit the damage by restricting user rights to infected devices.

Key findings

- 80% of I.T. professionals have implemented a patch policy to enhance their organization's security.
- 77% said that Microsoft OS represents the biggest challenge in terms of patching operating systems, and 59% indicated that Oracle is the most challenging 3rd party application.
- 55% of I.T. professionals believe that the visibility they have into their company's I.T. security posture is insufficient.
- 55% of the companies surveyed give employees' administrator rights, substantially increasing security risk.
- Patch management takes more than 8 hours per month for two-thirds of the companies.

“The results of this survey show that the need to establish a patch management policy is recognized by an increasing number of I.T. departments. Despite this, many companies spend too much time on patch management issues, and manage the rights of their employees in a way that unknowingly promotes risk. This confirms the importance of our work in supporting companies in managing their patches, enabling them to reduce costs, save time and minimize risks to the security of their I.T. assets,” said Andy Baldin, VP EMEA Shavlik.

Baldin emphasizes the importance of facilitating companies’ work to secure and manage their patching: “The results of our study shows that 7% of respondents do not have I.T. security systems in place or do not know if there is one, 3% have only one backup system, 13% just have antivirus, 7% a firewall and 10% an antivirus coupled with a firewall. This means, 40% of respondents could easily improve their endpoint security.