SURVEY

Tripwire 2019 Vulnerability Management Survey

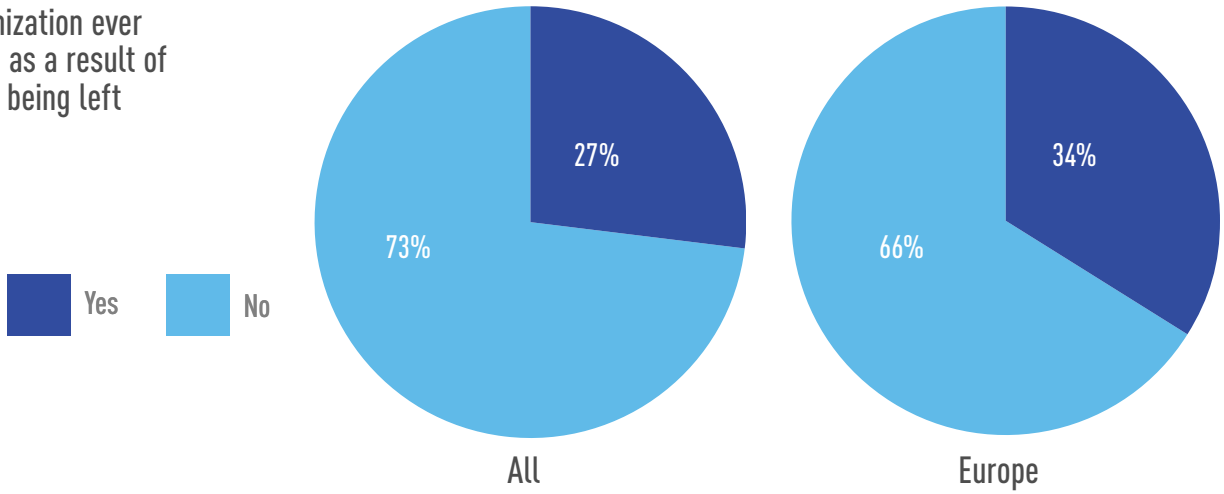
June 2019

Unpatched vulnerabilities remain the root cause of today's most serious data breaches. To understand how organizations are addressing vulnerabilities today, in May 2019, Tripwire partnered with Dimensional Research to survey 340 infosecurity professionals on vulnerability management trends.

FOUNDATIONAL CONTROLS FOR SECURITY, COMPLIANCE & IT OPERATIONS

More than one in four (27 percent) have been breached as a result in an unpatched vulnerability. This rate is higher in Europe, with 34 percent.

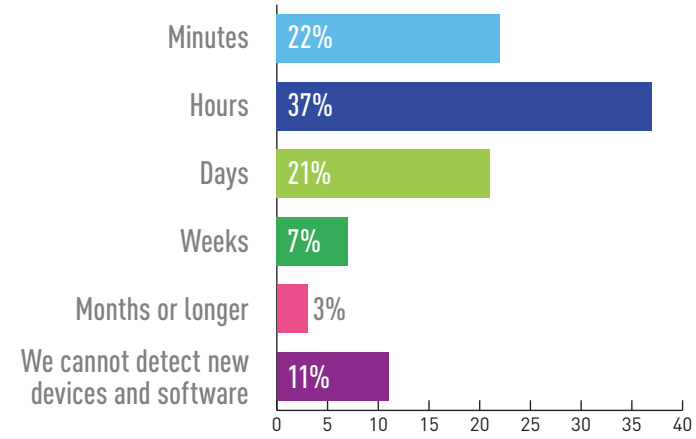
Has your organization ever been breached as a result of a vulnerability being left unpatched?



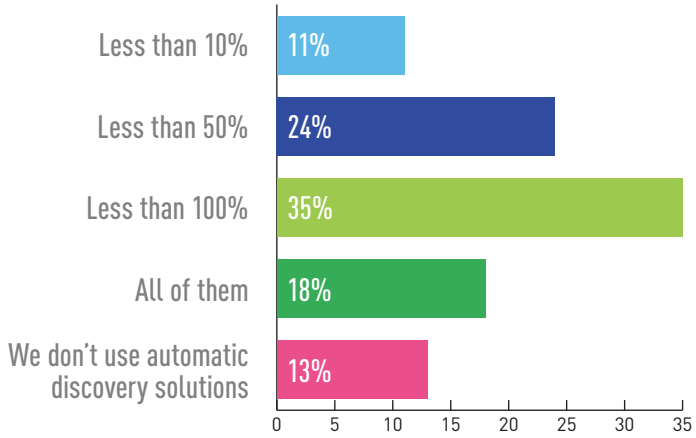
To understand where vulnerabilities lie, you have to have visibility of your attack surface.

How long does it take to detect new hardware and software added to your organization's network? Choose the answer that most closely applies.

59 percent can detect new hardware and software on their network within minutes. However, this is a difficult manual effort for many, with 35% saying less than half of their assets are discovered automatically.

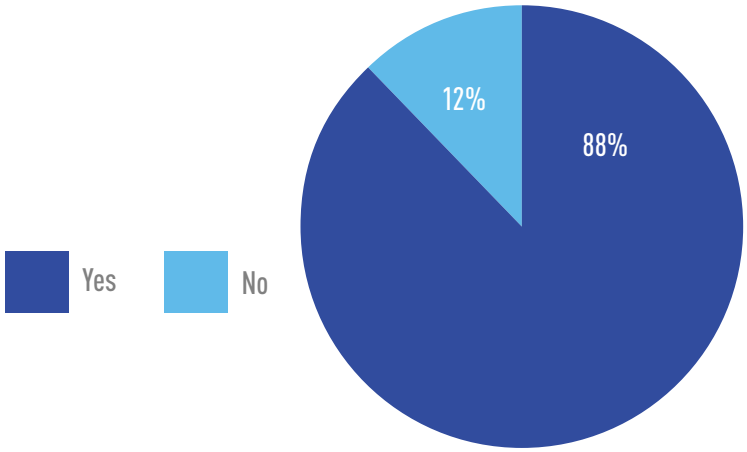


Approximately what percentage of hardware and software assets on your network are discovered automatically? Choose the answer that most closely applies.



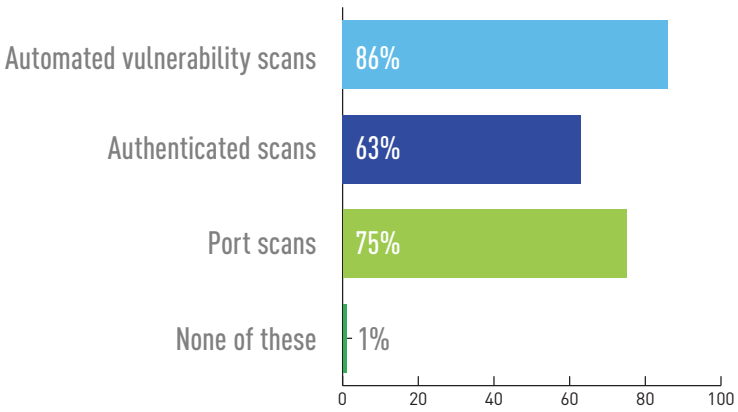
Organizations are running vulnerability scans with varied effectiveness.

Does your organization run vulnerability scans?



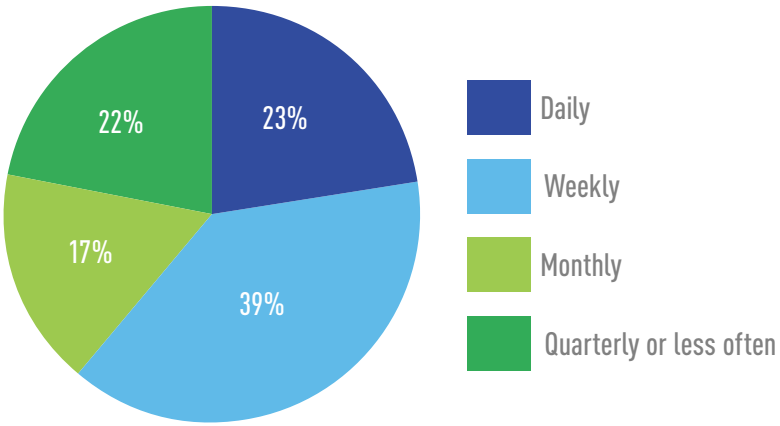
What kind of vulnerability scanning do you do? Choose all that apply.

"How you assess your environment for vulnerabilities is important if you want to effectively reduce your risk. If you are not doing authenticated vulnerability scans, or not using an agent, then you are only giving yourself a partial picture of the vulnerability risk in your environment," Tim Erlin, vice president of product management and strategy at Tripwire said.



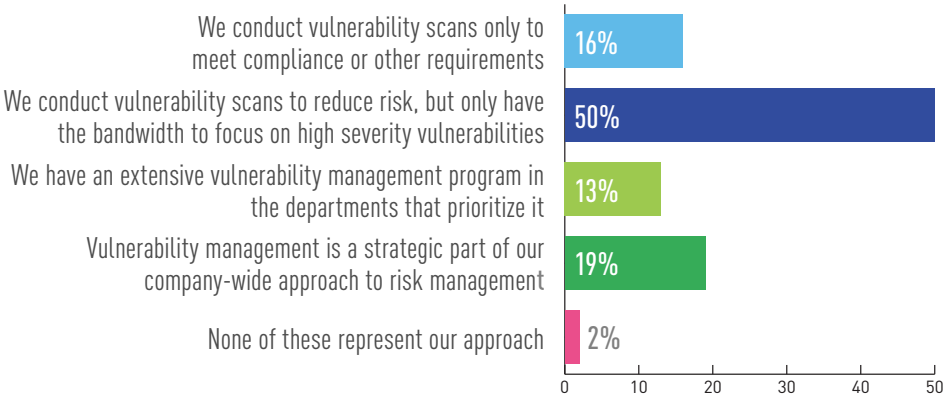
How often do you run vulnerability scans?

Organizations are recommended to conduct vulnerabilty scans at least weekly. "If you're not scanning for vulnerabilities frequently enough, you're missing new vulnerabilities that have been discovered, and you may be miss assets that tend to go on and off the network, like traveling laptops," Erlin said.

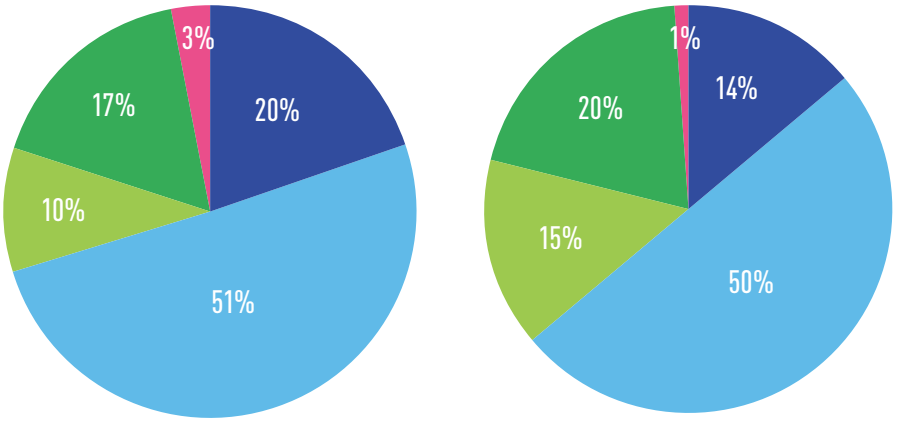


Most organizations want more mature vulnerability management, but are constrained.

Which of the following statements best characterizes your approach to vulnerability management?



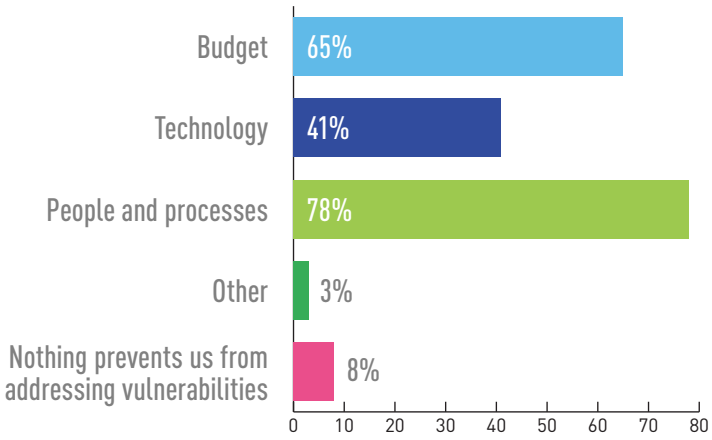
European respondents were more likely to say they were just concerned with meeting compliance.



"Meeting a regulation or compliance requirement does not necessarily mean you've effectively managed your security risk," Erlin concluded. "Compliance requirements are most often about protecting someone other than your organization. That might be the consumer or credit card companies or another entity. Securing your business requires that you define an acceptable level of risk and manage to that target."

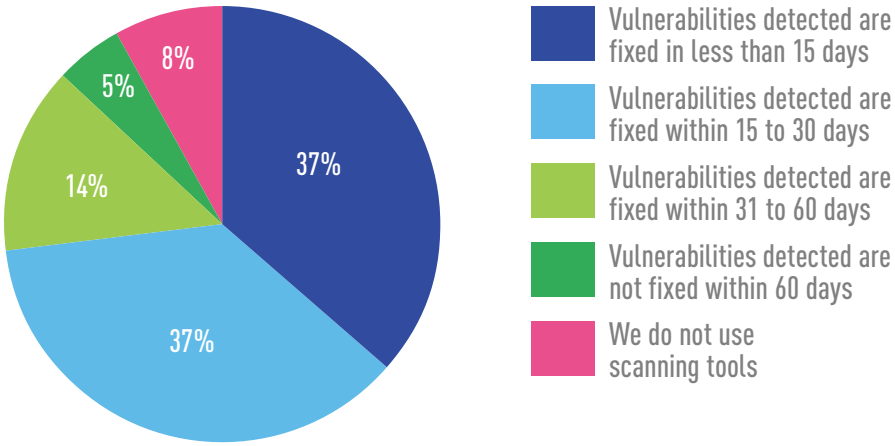
- We conduct vulnerability scans only to meet compliance or other requirements
- We conduct vulnerability scans to reduce risk, but only have the bandwidth to focus on high severity vulnerabilities
- We have an extensive vulnerability management program in the departments that prioritize it
- Vulnerability management is a strategic part of our company-wide approach to risk management
- None of these represent our approach.

What constraints prevent you from addressing all the vulnerabilities you want to address? Choose all that apply.

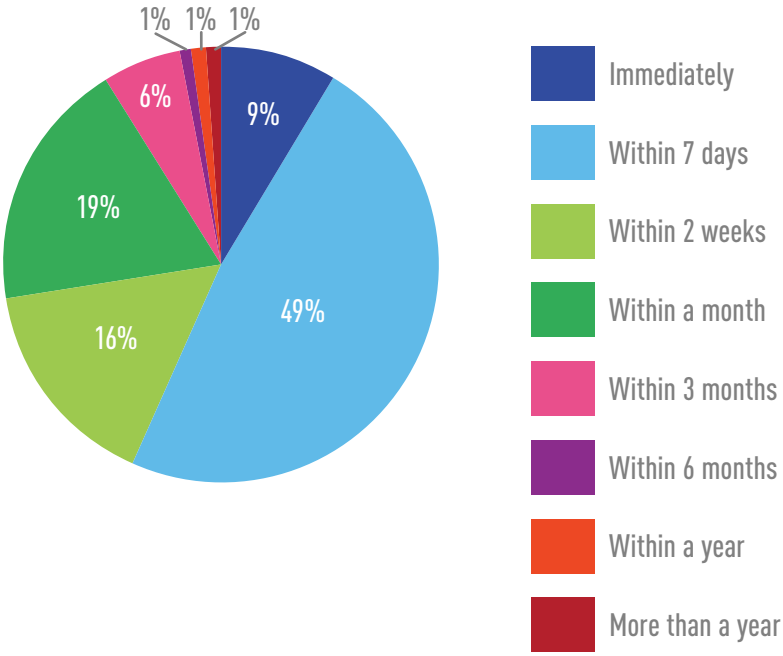


Most organizations aim to fix vulnerabilities within 30 days or less.

Are all vulnerabilities detected by scanning tools fixed or remediated promptly?

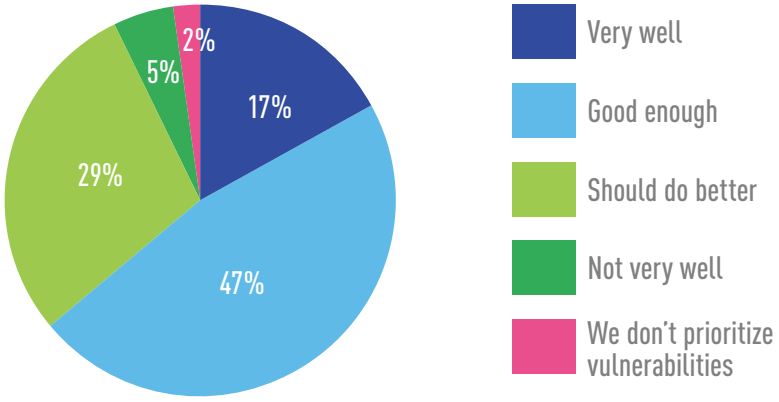


In general, how long does it take to deploy a security patch in your environment?

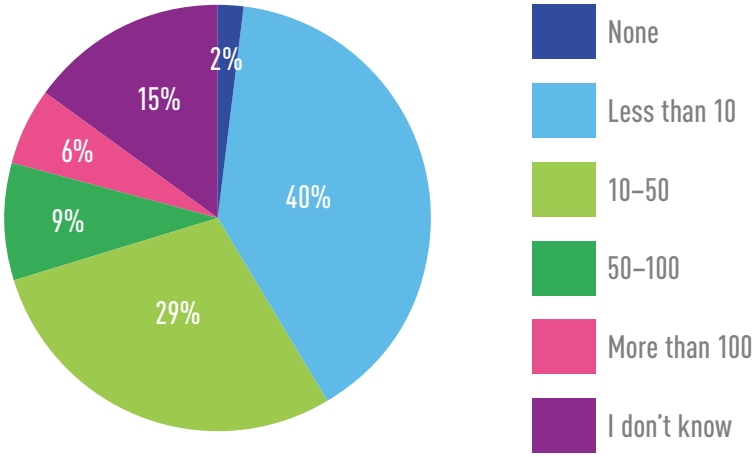


Most organizations recognize a need to prioritize vulnerabilities more effectively.

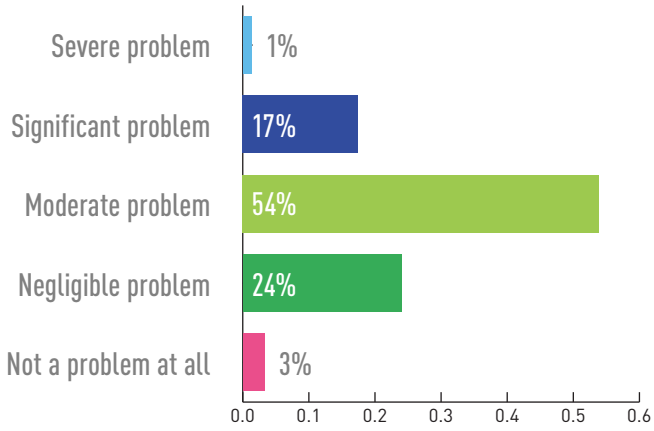
How would you characterize your organization's ability to prioritize security vulnerabilities? Choose the one answer that most closely applies.



Approximately how many vulnerabilities does your organization patch every month?

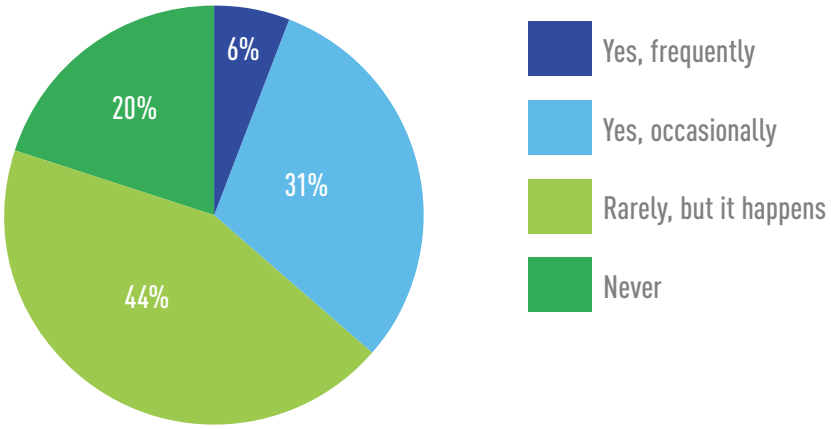


How much of a problem are false positives for your organization's vulnerability management program? Choose the answer that most closely applies.

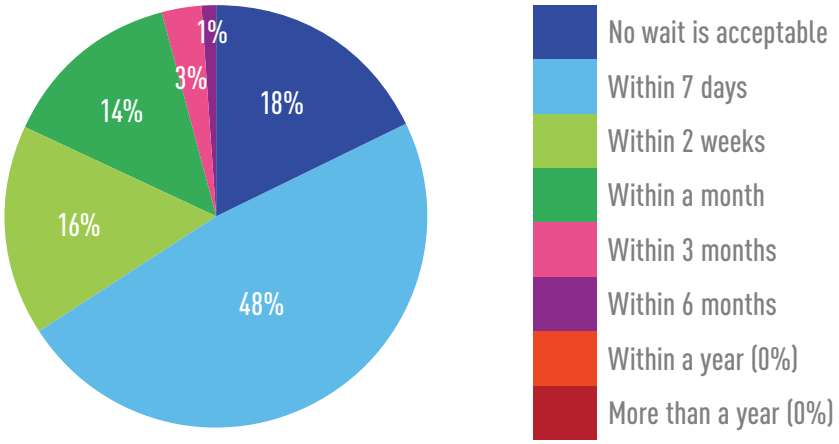


Organizations will in some cases stop using products as a result of vulnerabilities.

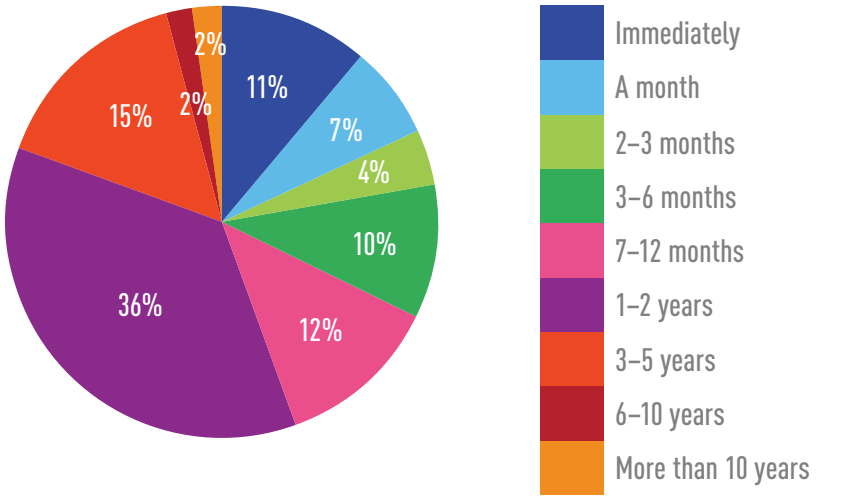
Has your company ever stopped using a product due to vulnerability disclosure?



What is an acceptable time frame between the discovery of a vulnerability and the release of a patch? Choose the answer that most closely applies.



In your opinion, how long after a product goes end of life is it reasonable for vendors to stop releasing patches? Choose the answer that most closely applies.



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPLLLLNa YYMM