



The Challenge

The most common tactic utilized by cyber-criminals is exploiting unpatched vulnerabilities to infiltrate your systems. As a result, patching vulnerabilities on a regular basis is critical to preventing disruption of systems operations and patient care. Still, for many organizations, patching isn't getting done on the frequency it should.

Why do healthcare organizations struggle with consistently getting patching done?

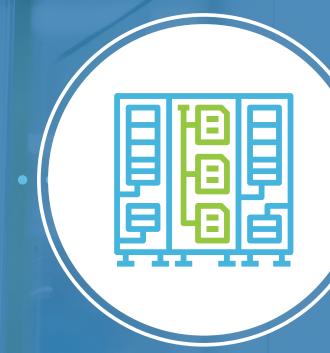
Here are the top reasons why healthcare organizations struggle with patching—leaving them open to performance slowdowns, regulatory compliance issues, and cyber-attacks.







Budget cuts



Legacy systems



Poor patching processes

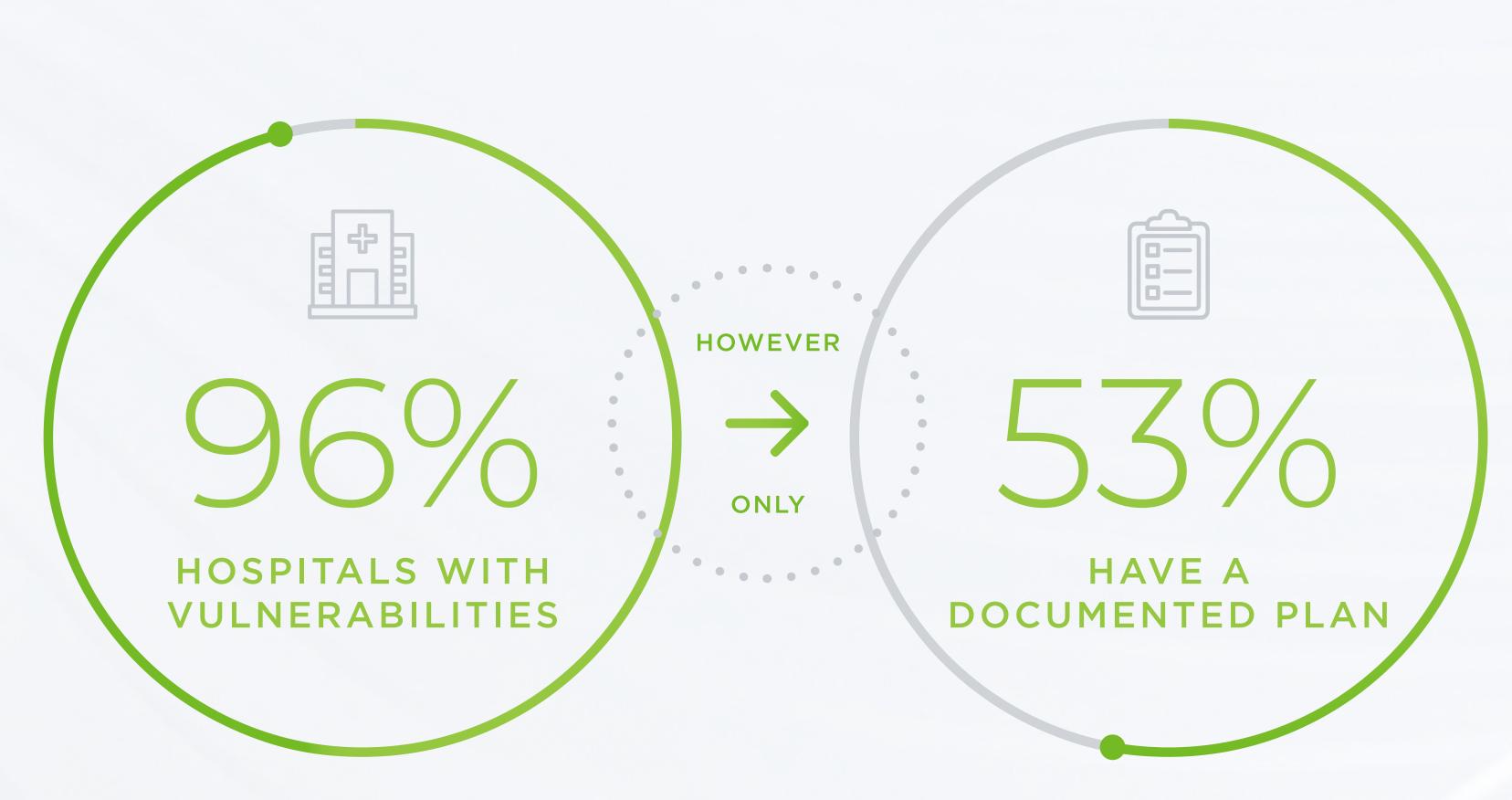


Bargaining with clinical staff for downtime



Managing high priority operational tasks

Healthcare Patching by the Numbers



96% of hospitals are operating with systems and software programs that contain known vulnerabilities. However, only 53% of surveyed hospitals stated they have a documented plan for addressing identified vulnerabilities.1



90% of vulnerabilities discovered in 2021 can be exploited by hackers with limited technical skills.²



In 2021, 57% of hospitals hit by cyber-attacks said their breaches could have been prevented had they installed an available patch.3



34% of those victims knew of the vulnerability but took no action.4

loud Wave Patches



more efficiently. Now, we are bringing this structured approach to you.



CloudCare+: Conducting Systems Maintenance to Achieve

The Solution

Operational Excellence, Security, and Compliance Fully-managed patching for healthcare. CloudCare+ was built

specifically to alleviate the burden that the never-ending patching cycle places upon healthcare IT. Our skilled service team takes on the entirety of your patching process with our proven cycle—allowing your team to take a hands-off approach to maintenance while we ensure operational excellence by keeping your environment compliant and secured against cyber threats.

Your primary goal is protecting patients, and that includes ensuring your systems, and their most sensitive information, remain secure. Let us reduce your risk while taking the burden

LEARN MORE

4. https://www.servicenow.com/workflow/it-transformation/ponemon-vulnerability-response-study/

off your IT team by executing patching for you.