CloudWave

Unpatched Vulnerabilities Are Inviting Cybercriminals to Your Door

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.

- Staffing shortages
- Budget cuts
- Legacy systems
- Poor patching processes
- Bargaining with clinical staff for downtime
- Managing high priority operational tasks

Healthcare Patching by the Numbers

96% HOSPITALS WITH VULNERABILITIES

HOWEVER → ONLY

53% HAVE A DOCUMENTED PLAN

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% EXPLOITED WITH LIMITED TECHNICAL SKILLS

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

57% COULD HAVE BEEN PREVENTED

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

34% TOOK NO ACTION

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

CloudWave Patches

1,000+ SERVERS PER WEEK

150+ HOSTED HOSPITALS

We had to scale and streamline our maintenance process to patch more efficiently. Now, we are bringing this structured approach to you.

OpSus CloudCare+

The Solution

CloudCare+: Conducting Systems Maintenance to Achieve 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 off your IT team by executing patching for you.

LEARN MORE

LEARN MORE AT

GoCloudWave.com

CloudWave

SOURCES
1. https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf
2. https://www.rediscan.com/news/nist-nvd-analysis-2021-record-vulnerabilities/
3. https://www.servicenow.com/workflow/it-transformation/ponemon-vulnerability-response-study/
4. https://www.servicenow.com/workflow/it-transformation/ponemon-vulnerability-response-study/