What is your time to patch?

When it comes to patching your systems, you're on the clock. The longer it takes to patch, the more vulnerable they are to potential exploits. Research suggests that the majority of exploitation occurs within a few days of a patch becoming available.

Threat level timeline

Timeline	Event
Pre-Zero Day	Ongoing application control and privilege management
	Exploited zero day
	Public disclosure
	Unknown Vulnerabilities
Day Zero	
	Update Release
0-14 Days	Apply the patch and continue application control and privilege management
	Rising Risk
14-28 Days	
	50% of exploits have occurred
40-60 Days	
	90% of exploits have occurred
120 Days	

Did you know

60%
In 2019, 60% of data breaches were linked to a vulnerability where a patch was available, but not applied[1].

$3.92 million
Data breaches cost businesses an average of $3.92 million. The average size of a breach is 25,575 records containing sensitive and confidential information. Each record costs about $150 on average globally and $242 in the U.S[2].

Timely patching is critical to preventing data breaches.

Close the vulnerability gaps and reduce the attack surface with an Avast Business automation solution to assist you with vulnerability management and patching.

Peace of mind is worth the investment.

Learn more and get a free trial by going to avast.com/patch.