



The Hidden Costs of Downtime

Action Guide

Downtime is no longer a technical inconvenience; it's a business crisis. The consequences of an outage extend far beyond immediate financial loss. Dips in stock price. Delayed product launches. Slow, corrosive brand damage. These are just some of the hidden costs that haunt an organization long after systems are back online, compromising long-term growth and competitive standing.

In its 2026 Hidden Cost of Downtime report, created in partnership with Oxford Economics, Splunk calculated that the Global 2000's aggregate cost of downtime has soared to \$600 billion annually — up 50% from 2024.

Downtime is inevitable; prolonged disruption is not. That's why Splunk captured insights from security, ITOps, and engineering leaders on the front lines, as well as finance and marketing executives who see the brand and economic damage up close.

The most resilient organizations aren't the ones with the most tools or the boldest AI ambitions. They're the ones that align technology with business outcomes, empower their people with context, and design systems that bend — but don't break — under pressure.

Let's take a look.

\$600B

is the aggregate cost of downtime for the Global 2000

Advancing beyond the outage with Splunk and Presidio

Resilience isn't simply about keeping systems online. It's about protecting trust, enabling growth, and ensuring that organizations can move forward — even when things go wrong. A single point of failure rarely stays contained. The ripple effect of an outage can send a shockwave from the server room to the stock market, racking up fines, eroding brand trust, and stalling innovation.

Are your leaders up to the challenge? See how your organization can build digital resilience to bounce back faster, learn and improve, and build the advantage of predictive immunity.

Question to ask	What action should I take?
Does my institution treat downtime as a business risk? Yes: ☐ No: ☐	☐ Translate downtime into business language, mapping incidents to impact. ☐ Include downtime risk in board-level and executive decisions. ☐ Align functional teams around resilience metrics.
Are my systems designed to mitigate human error? Yes: ☐ No: ☐	☐ Reduce human error with safe-by-default changes and guardrails. ☐ Standardize change management and deployment practices. ☐ Build systems for faster detection with clear context to shorten MTTR.
Is there clear accountability for root cause analysis? Yes: ☐ No: ☐	☐ Connect platforms and establish a shared data source with shared context. ☐ Design an additional coverage layer with a data fabric architecture.
Is my organization using AI to accelerate insight? Yes: ☐ No: ☐	☐ Pair AI's analytical speed with expert human judgment and oversight. ☐ Require validation before remediation or automated actions are taken. ☐ Implement robust governance frameworks to manage shadow AI.

If you answered "no" to any of these questions, Splunk and Presidio are here to help.

Contact us now to learn how you can minimize downtime and champion a more resilient business.

Presidio

SplunkSolutions@presidio.com



PRESIDIO®

www.splunk.com
www.presidio.com