The Patch Apocalypse Survival Assessment

How prepared is your organization for the age of AI-accelerated threats? As exploit windows shrink and vulnerability volumes rise, most organizations face three critical blind spots. Check each statement that is true for your organization.

Survival Risk #1: Visibility

You can't protect what you can't see

Visibility gaps create risk long before a vulnerability is discovered. Without trusted visibility, every security decision is made with incomplete information.

Check all that apply:

- ☐ IT and security teams work from a shared source of truth.
- ☐ We maintain a trusted inventory of devices, software and endpoints.
- ☐ We can identify unmanaged devices and shadow IT.
- ☐ Our asset discovery is automated and continuously updated.

Score: _____ / 4

What this means:

- **0-1** Significant visibility gaps may be creating unknown exposure.
- **2-3** Core discovery capabilities are in place, but blind spots likely remain.
- **4** You have a strong visibility foundation for exposure management and automation.

Survival Risk #2: Prioritization

You don't know which risks to prioritize

Your organization can't reasonably remediate all vulnerabilities all the time. Success depends on understanding which vulnerabilities pose the greatest threat to your organization if exploited, and prioritizing remediation efforts based on overall business impact.

Check all that apply:

- ☐ Leadership has defined an acceptable level of cyber risk (risk appetite).
- ☐ Threat intelligence helps determine which exposures deserve immediate attention.
- ☐ We understand which systems represent the greatest organizational risk.
- ☐ We prioritize remediation using business context — not severity scores alone.

Score: _____ / 4

What this means:

- **0-1** Priorities are likely driven by compliance requirements, severity scores or patch volume.
- **2-3** Risk-based decision making is developing, but teams may still struggle to separate urgent risks from routine issues.
- **4** Your organization has established a clear risk appetite and can focus resources on the exposures that matter most.

Survival Risk #3: Speed

Your teams can't keep pace with AI-accelerated threats

As AI accelerates the scale and complexity of attacks, organizations must reduce operational friction and respond at machine speed.

Check all that apply:

- ☐ We can rapidly respond to critical risks outside traditional maintenance windows.
- ☐ Routine remediation is governed by predefined policies rather than lengthy approval processes.
- ☐ IT and security teams can act on emerging risks without significant operational bottlenecks.
- ☐ Automation helps us reduce manual effort and accelerate response to changing conditions.

Score: _____ / 4

What this means:

- **0-1** Process bottlenecks, manual workflows or approval delays may prevent your teams from responding quickly enough to emerging threats.
- **2-3** Response capabilities exist, but operational friction can still slow remediation efforts when risk conditions change.
- **4** Your organization has the operational agility to translate visibility and risk intelligence into action, enabling faster, more consistent responses to AI-accelerated threats.

Calculate your survival score Add your scores from all three survival risks.

Total Score: _____ / 12

Your Patch Apocalypse profile

0-3 Points

Critical Exposure

Your organization may have significant blind spots that limit visibility, slow decision-making and delay response. As exploit windows continue to shrink, these challenges can quickly compound and increase overall risk.

What's next?

Start by improving visibility into assets and exposures, then establish clear risk priorities and governance processes that enable faster action.

4-6 Points

High Exposure

Visibility gaps, competing priorities or operational bottlenecks may increase organizational risk. While existing processes may have worked in the past, they may struggle to keep pace with the speed and scale of AI-accelerated threats.

What's next?

Focus on establishing a trusted source of truth, improving risk-based prioritization and removing barriers that delay action.

7-9 Points

Strengthening Defenses

You have critical foundations in place, but opportunities remain to improve visibility, decision-making and response speed. Reducing operational friction and strengthening alignment between IT and security teams can help improve resilience as exploit windows continue to shrink.

What's next?

Identify the survival risk area where you scored lowest and focus on improvement efforts there first.

10-12 Points

Survival Ready

Your organization has established many of the capabilities needed to navigate AI-accelerated risk. Trusted visibility, risk-based prioritization and operational agility help your teams identify, evaluate and respond to emerging threats before they become larger business risks.

What's next?

Continue advancing automation, governance and continuous risk management to maintain your advantage as threats evolve.

Take the next step

The organizations best prepared for AI-accelerated threats aren't necessarily the ones applying the most patches. They're the ones with the visibility to understand their environment, the intelligence to prioritize what matters most and the agility to act before attackers do.

Understand the patch forward out of the Patch Apocalypse in our whitepaper: **The Patch Apocalypse: Why Traditional Vulnerability Management is Breaking Under AI-Driven Discovery.**

Click Here