

## Cybersecurity Myth Busters: Three Things You Might Be Getting Wrong

Cyber threats and defenses are evolving, but many organizations still base decisions on outdated assumptions. Here are three common cybersecurity myths, and what the cybersecurity community recommends instead:

**Myth: “Cybersecurity is just about stopping threats.”**

**Reality:** Prevention is only part of the equation. The rest is about **resilience**.

Every system has blind spots. A determined attacker may eventually succeed, which is why **incident response, backup planning, and business continuity** are just as critical as firewalls or antivirus software.

**Think of cybersecurity like public health.** You need vaccines and masks to prevent disease, but you also need hospitals and treatment plans when illness hits. The goal is not just to block threats, but to minimize impact and bounce back quickly.

**Myth: “Zero Trust is too complex or advanced for most organizations.”**

**Reality:** Zero trust is not a product; It is a mindset, and any organization can start applying it.

At its core, Zero Trust means **no user or device is granted access just because it is on the network**. Every request must be verified, every time, based on identity, context, and behavior. This applies whether the user is inside the physical organization or logging in remotely. While applying zero trust will look different in different environments, like IT v OT, but the principles remain sound.

**Think of Zero Trust like airport security.** Even if you have a boarding pass, you still go through ID checks, metal detectors, and bag scans, because the goal is to verify at every step. Organizations should start where they are: map out who has access to what, and why. Then begin tightening the controls.

**Myth: “AI is inherently unsafe.”**

**Reality:** AI systems are not automatically insecure. The risks depend on how they are built, trained, and deployed. A well-governed AI system can actually **enhance** cybersecurity.

Today, many cybersecurity platforms use AI to **identify vulnerabilities, detect anomalies, and respond to threats faster** than manual processes allow. From predictive risk scoring to real-time traffic analysis, AI is becoming a core tool for defense. Some organizations like Accenture [report](#) 60% faster responses to an attack by incorporating AI into cybersecurity solutions.

**Think of AI like a power tool.** In skilled hands with proper safety measures, it increases efficiency and precision. Without safeguards or training, it can do real damage. Secure-by-design principles, red-teaming, and transparency in how models are trained and used are all essential guardrails.

---

**Overall:** Cybersecurity today is not about any one tool or tactic; it is about mindset, design, and readiness. Whether adopting Zero Trust, deploying AI, or building resilience into operations, the goal is to reduce assumptions and increase control.

**Hot tip:** You don't have to worry too much about which wifi you hop onto anymore - with a new protection called TLS, all of your traffic is encrypted by websites these days!

[www.monumentadvocacy.com](http://www.monumentadvocacy.com)

Follow us on LinkedIn [@Monument Advocacy](#)