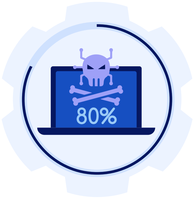
Remedio

Separating Fact from Fiction:
10 Cybersecurity Myths That Need Busting

Are faulty assumptions silently undermining your decision making? It's time for a reality check! One fact at a time...



Myth #1:
It Won't Happen to Us.

Over 80% of businesses are hit with cyberattacks.

No sector, size, or location is immune. Assume you're a target.

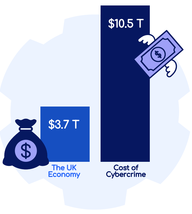
Source: Remedio Factbook

Myth #2:
If It Worked Then, It'll Work Now.

Cybercrime cost the global economy $10.5 trillion dollars in 2025, an increase of more than 10% from the year prior...

Underscoring the fact that yesterday's defenses are failing to keep up with today's threats

Source: Cobalt.io





Myth #3:
We're Safe Because We Do Annual Audits.

Attacks happen every 39 seconds, and 108 new CVEs are published every day, on average..

So once yearly audits will always be too little, too late.

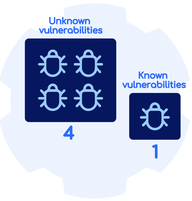
Sources: Astra, Jerry Gamblin

Myth #4:
We Just Patched for That Last Breach, so we're good.

There are at least 4 unknown vulnerabilities (that can't be patched) for every 1 known vulnerability.

Plus, more than 36 new vulnerabilities are found in end-of-life software each month — with patches never made available for most of them.

Sources: Remedio, Chainguard





Myth #5:
Once Configured, Always Configured.

Configurations frequently drift. Which is why 81% of cloud-related breaches exploit misconfigurations.

Reliable security is impossible without continuously monitor endpoints for risky configurations and drift.

Source: Cybersecurity News

Myth #6:
Business Optimization Conflicts with Security.

Remedio boosts IT productivity by 22%.

Smart security benefits the business.

Sources: Remedio





Myth #7:
It's Someone Else's Job.

42% of companies suffer from cyber fatigue.

Alerts fall through the cracks without clear context and well-defined responsibilities..

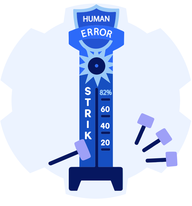
Source: Integrity360

Myth #8:
Hiring More People Will Solve It.

82% of cloud breaches involve human error.

Headcount alone won't fix systemic gaps.

Source: SentinelOne





Myth #9:
Tools Work Out-of-the-Box.

61% of breaches stem from failed or misconfigured controls.

Dangerous defaults need real oversight.

Source: Gartner

Myth #10:
Group Policies Secure Everything.

35% of cyber incidents stem from misconfigurations where GPOs fall short.

GPOs ≠ Enforcement. Validation is vital.

Source: SOCRadar



Why Remedio?

Misconfigurations are silent threats. Remedio delivers real-time detection, safe remediation, and continuous alignment — so you can harden every device, prevent drift, and bust cyber myths before they cause real damage.

See For Yourself

Remedio