

Gain Cyber Resilience with a Layered Security Solution

ANATOMYIT

Security today is no longer about having tools in place.

It's about whether those tools work together to detect and respond to modernized cyber incidents and unknown threats.

As a technology partner and advisor, we recommend a defensible security stack with a layered model to safeguard your organization.

"63% of organizations cited complex and evolving threat landscape as their greatest challenge to becoming cyber resilient."

*World Economic Forum,
Global Cybersecurity Outlook 2025*

Cybercriminals Move in All Phases and You Need Visibility Across To Limit Impact

Attack Phase	Business Reality	Stack Capability
Initial Access	Phished credentials, vendor access, shared / unmanaged accounts	ITDR + EDR
Execution	Compromised endpoints, servers, cloud workloads and user devices	EDR
Expansion	Lateral movement into critical business systems, applications, data stores, and backups	EDR + ITDR
Cross-Cutting Visibility	Correlating identity and endpoint signals across the environment to detect threats early & reduce blast radius	SIEM
Impact	Ransomware, operational downtime, data loss, regulatory exposure, revenue and reputational damage	Unified Stack = EDR + ITDR + SIEM

We're finding many organizations are missing one or more critical components.

Legacy software or missing tools in your security stack can leave you vulnerable. Build a better defense with the guidance from Anatomy IT.

- ✓ We'll quickly develop your cyber resilience model
- ✓ Help you align with a commercially reasonable security standard
- ✓ Plus review other potential gaps such as security training, audits, and compliance

"Technology resilience begins and ends with a strong digital core: a strategic blend of technologies and practices that include digital platforms..."

*- Forbes Online Article
2025*

Let's Connect and Review Your Security Stack

anatomyit.com