Why Relying Solely on Antivirus Isn't Enough for Cybersecurity 🛡️💻

Did you know? Having just an antivirus solution in your business isn't sufficient to combat today's cyber threats. Here's why:

Advanced Persistent Threats (APTs)

Sophisticated, targeted attacks bypass traditional antivirus defenses, lingering undetected for months.

Zero-Day & Unknown Malware

Antivirus relies on known threat signatures – leaving new or evolving malware undetected.

Phishing & Social Engineering

Cybercriminals exploit human behavior via fake emails or scams. Antivirus can't stop these entry points.

Ransomware Attacks

Once malware encrypts data, antivirus often can't reverse the damage – disrupting operations irreparably.

Network & IoT Vulnerabilities

Firewalls, endpoints, and IoT devices are common attack vectors. Antivirus doesn't address these gaps.

Lateral Movement & Privilege Escalation

Hackers infiltrate systems, spread across networks, and escalate access — requiring advanced monitoring.

No Real–Time Threat Response

Solutions like EDR (Endpoint Detection & Response) or XDR are critical for instant threat detection and mitigation.

Outdated or Misconfigured Antivirus

A lapse in updates or settings creates false confidence, leaving systems exposed.

Weak Data Protection

Antivirus fails to prevent unauthorized access to sensitive business data.

Novatech

www.novatech-global.com