cynet

How to achieve comprehensive protection without breaking a bank

REQUEST A FREE TRIAL

As a small to medium-sized enterprises (SMEs), you face the same cyber threats as larger enterprises but do so with a fraction of their cybersecurity budgets. This means fewer tools, fewer staff, and less cybersecurity expertise.

Limited budgets unfortunately translate to limited protections. Most SMEs are only able to deploy a smattering of disjointed technologies to help address a portion of their cyber risks.

The Solution

Achieving comprehensive cyber protection is actually easier, and more affordable, than you might think. Cynet provides broad Threat Visibility with Automated Threat Response on a single, natively built, seamlessly integrated platform. Moreover, the protections provided come at a fraction of the cost of purchasing them separately.

Threat Visibility

Seeing everything and looking everywhere across your IT environment isn't possible with just one security tool. True threat visibility starts by having all key the pieces to detect and address elusive threats sneaking through complex environments. The key pieces include:

EDR – Endpoints can be a target, entry point, or lateral leaping pad for many threats. Endpoint detection and response (EDR) solutions can prevent attacks from executing files and terminate suspicious runtime processes.

NGAV – Next generation antivirus (NGAV) uses signatures to instantaneously identify malware that carries a known signature or behavior so the security team can eliminate the "low-hanging fruit" of threats and focus elsewhere instead.

MTD – Over 60% of endpoints that access corporate data are mobile. Mobile threat detection (MTD) prevents security and privacy threats to mobile devices and should detect applications that put data at risk and attempt to infiltrate corporate networks.

NDR – When active threats infiltrate a network, the network detection and response (NDR) tool should pick up on it immediately. With visibility into standard communication between endpoints, network analytics tools are efficient in detecting post-compromise activities that surface in anomalous network traffic.

UBA – Since new and evasive threats can't be identified by a signature, it's important to monitor for unusual activity with a user behavior analysis (UBA) tool. They excel at spotting emerging threats that evade detection elsewhere.

Deception – Deceptive technologies trick attacks by luring them towards fake assets. Attacks that managed to evade detection elsewhere may be undone by deceptive technologies that lure the attack into a trap.

SSPM/CSPM – Most businesses now rely on multiple SaaS and Cloud applications. Leverage SaaS and Cloud Security Posture Management (SSPM and CSPM) solutions to automatically identify, prioritize, and fix security risks across all these applications.

Automated Threat Response

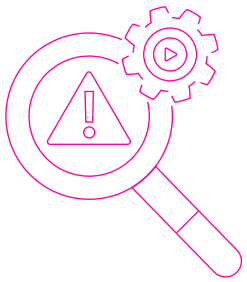
Advances in machine learning and artificial intelligence have enabled automated systems to outperform humans, especially on common, repetitive tasks. They are especially helpful for enforcing best practice approaches for users that don't have the domain expertise. Here's how automation can significantly improve threat response.

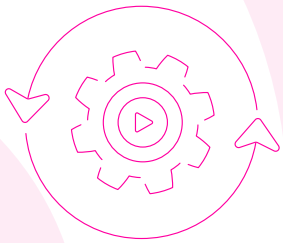
Visibility

Automated systems can ingest signals from multiple threat detection domains to detect threats more accurately with lower false positives. Seemingly benign signals may indicate a dangerous threat when combined – something perhaps not obvious to a non-expert human analyst, but something an automated systems can achieve instantaneously.

Automated Investigation

Cybercriminals know most SMEs lack 24x7 coverage, which is why most ransomware attacks target these organizations on off-hours. Therefore, every alert, no matter the risk or time of day, must be investigated to determine whether the threat is dangerous or perhaps part of a larger, stealthy attack. Automated threat response systems can instantly investigate alerts to determine the root cause and scope of an attack.





Automated Response

Preventing data breaches requires that identified threats are quickly and thoroughly eradicated. Automated Response systems are available 24x7 to perform simple remediation actions or execute highly sophisticated response playbooks that involve logic and multiple potential response actions. Response playbooks are especially useful to address dangerous threats like ransomware by not only containing the threat itself, but also the root cause and any traces of the threat across the environment.

Key Takeaway

Even the smallest companies can achieve comprehensive cybersecurity protection 24x7 within their existing budget by leveraging the right tools and partners. Cynet was built from the ground up to help SMEs achieve unparalleled protection with an intuitive, unified platform, backed by a 24x7 MDR service.

REQUEST A FREE TRIAL