Sentinel Intrusion Prevention Systems
https://sentinelips.com
(972) 991-5005

NETWORK SECURITY FOR SMBs

HERE'S WHY SMBs ARE EASY MARKS FOR CYBERATTACKS

Some small and mid-size businesses believe they can't possibly be a target for hackers because they don't store valuable data, so they under-invest in risk mitigation or ignore basic security preparation. **The "it won't happen here" attitude can be the kiss of death**, according to Enterprise Strategy Group (ESG), who last year surveyed 400 security and IT professionals about the state of cybersecurity at SMBs.[1]

ESG says criminals sometimes target SMBs to extort money or steal valuable data, but t**hey can also use small businesses as a beachhead for attacking connected customers** or partners. (That's how Target got breached.) They exploit vulnerabilities through poor patch management, configuration errors, and lack of security policies.

SMBs also tend to have a small staff responsible for cybersecurity and IT, and those tasked with cybersecurity can't keep up with the workload. Here are 3 ways SMBs can assess just how vulnerable they are to cyberattacks:

Routine Vulnerability Assessments

A vulnerability assessment tests computers, servers and networks to identify and rank their weaknesses. The process doesn't have to be complicated and expensive. Sentinel routinely performs internal and external vulnerability assessments for its customers, detecting anomalies in each device's OS and software, assessing the severity of each vulnerability, and suggesting solutions for remediation of each issue.

Network Gateway Assessment (NGA)

Before building a security stack, learn how your network shows itself to the bad guys and find infected machines hiding on your network. With an NGA, you can also test drive Sentinel's Network Cloaking™, a proprietary defense methodology that dynamically drops all traffic from malicious networks, effectively 'cloaking' your network from hackers.

Hybrid Managed Detection and Response

In-house IT staff may be able to apply certain patches on time, but the exponential growth in the number of alerts may overwhelm them. The Sentinel Outpost's NGIPS filters out the background noise, proactively notifies you of any critical alerts, and lets the you focus in on the important information quickly. Any questions? Sentinel's support team is there, 24/7.

A single security breach can cost an SMB several weeks' or months' worth of profits. In worst-case scenarios, as many as 60% go out of business within six months of an attack.

As many as 46% of all cyberattacks target SMBs, resulting in measurable financial impact, lost productivity, and disruption of business applications and IT system availability. It can, and will, happen to SMBs who don't exercise network security vigilance.

[1] Download the report here: https://www.esg-global.com/research/esg-master-survey-results-cybersecurity-trends-at-smb-organizations