SOLUTION BRIEF

Why SMBs Became Easy Targets for Cyberattackers

Small business owners who assume that cybercriminals won't bother trying to hack their data stores, systems, and employees make an incorrect and dangerous assumption. Attackers see SMBs as attractive targets for myriad reasons. Yet, even among those who understand it's not a question of "if" but "when" an attack will occur, many admit they are unprepared.

A recent survey of SMB senior executives by backup and disaster recovery solutions provider Infrascale reveals that more than a quarter of companies do not have a plan to mitigate a ransomware attack. And nearly a fifth of all respondents worries their organizations are completely unprepared for a ransomware attack.

Cybercriminals are indiscriminate while selecting their targets. They know that all organizations - from the Fortune 100 to small businesses - manage and store sensitive data. So, not surprisingly, nearly one-in-three breaches included in Verizon's 2020 Data Breach Investigations Report (DBIR) involved small businesses.

According to the DBIR's authors, "Credential theft, social attacks (i.e., phishing and business email compromise) and errors cause the majority of breaches (67% or more). These tactics prove effective for attackers, so they return to them time and again. For most organizations, these three tactics should be the focus of the bulk of security efforts."

Whether attempting to steal sensitive data or launch ransomware to extort money from the company, the resulting costs can devastate a small business. The IBM and the Ponemon Institute's The Cost of Insider Threats Global Report 2020 states that small organizations spend an average of $7.68 million to recover from ransomware and other incidents resulting from employee negligence.

NYOTRON
SECURING THE WORLD

Nyotron Security
2880 Lakeside Drive
Suite 237
Santa Clara, CA 95054
+1.408.780.0750
www.nyotron.com

Why SMBs?

While the threat to small businesses is constant, their IT teams simply put aside their priority projects to focus on identifying and thwarting attacks that too often slip past their antivirus software and other "Negative Security" solutions.

Gain the Upper Hand

Nyotron is the only company to offer a true zero trust security platform for endpoints and servers that blocks attacks in real-time **without any need for threat detection or learning**. Put simply, we remove the burden of protecting your systems from your IT team's shoulders.

Nyotron's Paranoid solution takes the complete opposite approach of all the Negative Security solutions that monitor for known threats - a technique called "blacklisting."

We have fully mapped the one constant across your organization: the operating system (OS). Paranoid utilizes the map to automatically and instantly block specific system calls resulting from bad OS behaviors. This list is much, much shorter than the millions of known and unknown pieces of malware.

Paranoid complements your existing security solutions to not only significantly strengthen your organization's security posture, but it also eliminates management overhead. Your endpoints and employees are protected, and your IT personnel can focus on their priorities.

Visit www.nyotron.com to learn how Nyotron's Paranoid solution will protect your endpoints, data stores, and employees from even new, never-seen-before, and file-less malware threats.

NYOTRON
SECURING THE WORLD

Nyotron Security
2880 Lakeside Drive
Suite 237
Santa Clara, CA 95054
+1.408.780.0750
www.nyotron.com