The Road to Security Hygiene:
How SMBs Can Attain Affordable, Enterprise-Grade Identity Security
Summary

There is no doubt a robust cybersecurity defense is a business imperative. But for SMBs who do not have the resources or time to build and run an internal security team—and who cannot compete with enterprises vying for the limited pool of cybersecurity talent—staying confident in their cybersecurity defenses is much more challenging. It is also tougher for SMBs to find the time to train their employees in cybersecurity awareness and practices, leaving them even more vulnerable to business email compromise (BEC), identity-based attacks, and other threats.

Huntress’ MDR for Microsoft 365 solution gives SMBs all the benefits of a SOC via the pricing they can afford. Tailored specifically to smaller organizations, MDR for Microsoft 365 delivers 24/7 cybersecurity defense of Microsoft 365 environments, offering a formidable defense against threats such as BEC and account takeovers.

1

SMBs - ‘the 99%’ - do not have the dedicated resources to build an in-house SOC, but face the same threats as those who do

Limited resources and budget for an in-house security team leaves SMBs’ cybersecurity hygiene open to compromise. Coupled with an IT security talent shortage, SMBs simply cannot compete with the salaries that enterprises offer to secure the limited talent that is available. As a result, smaller organizations—whether they are a nursing home, a local bakery chain, or a family doctor—are all prime targets for cybercriminals. In addition, they are particularly vulnerable to cybercriminals specializing in BEC and identity-based attacks. These attacks are often the first and easiest ways into a company’s IT system due to a lack of resources and time to invest in security awareness training (SAT).
Inadequate defenses do not just put SMBs at grave risk of current threats, it also opens them up to future compromises

It’s surprisingly easy for SMBs to slip into a situation where they end up in a cyber defense silo, treading water and only being able to defend themselves from current cyber threats. At the speed that new tradecraft is created and weaponized, SMBs’ knowledge is often outdated before it is even implemented. This only makes them more vulnerable as they are unable to deal with current threats—let alone anticipate future ones.

Due to a lack of robust defenses and security awareness training, SMBs are particularly susceptible to BEC and account takeovers

The FBI’s 2022 Internet Crime Report showed that “in 2022, the IC3 received 21,832 BEC complaints with adjusted losses over $2.7 billion.” The report also outlines how BEC attacks have become more sophisticated, with “an increasingly prevalent tactic by BEC bad actors of spoofing legitimate business phone numbers to confirm fraudulent banking details with victims.”

Small businesses often bear the brunt of these increasing attacks because they often lack the means to run their own in-house SOC or implement a robust SAT program. This makes SMBs far more vulnerable to identity crime, not least because it is also the easiest way for attackers to get inside a company’s system. Add to this the knowledge that once gaining access via identity-based attacks, that attackers often up the ante to ransomware. It’s no wonder that SMBs are feeling particularly anxious and at risk.
The effects of a ransomware or other iterations of a cyberattack are numerous and wide ranging, and SMBs must protect themselves against them.

Identity based attacks often escalate to ransomware. Although ransomware is not ideal for any size of business, they are particularly frightening for SMBs who do not have an enterprise’s financial status. Beyond the immediate financial hit of ransomware or other iterations of a cyberattack, there are other consequences:

**Future revenue losses**: not only does a ransomware attack demand a sum of money for an organization to get back into its IT system, it also threatens future revenues thanks to a loss of customer confidence in the organization and the weakening or termination of customer relationships.

**Increased cyber insurance premiums**: if a company has made a claim on their cyber insurance policy, its premiums will only rise. This is another potentially unseen financial consequence of an attack and can also lead to lower cover limits.

**Jeopardized partner and supplier ecosystems**: lack of trust in a company’s ability to defend itself from a cyber attack can have severe effects for its operations as partners and suppliers become wary of the business’ security posture.

**The threat of litigation**: customers and partners impacted by an SMB’s cyberattack sometimes decide to file a lawsuit against the compromised company. This is not only potentially financially damaging but extremely stressful for an SMB to deal with, whose reputation will inevitably take a hit.
Despite all this, there is hope out there for SMBs

Given the reality of what an SMB is up against when it comes to building a robust defense against cybercriminals, the threat of an attack can feel like something of a perfect storm.

But there is help at hand. Huntress’ MDR for Microsoft 365 is built specifically for the 99% and meets SMBs where they are most at risk by anticipating the types of threats most likely to exploit them—particularly BEC. The platform includes features and functionalities that look to prevent issues and stop the problems that plague SMBs and crucially, it’s backed by 24/7 experts who use the human element to their advantage. Years of practical cyber knowledge have combined to build powerful software that utilizes automated detectors and determines whether an event is suspicious or legitimate. And not only is Huntress’ MDR for Microsoft 365 solution built for and tailored to the SMB market, it’s priced for the SMB too—there’s no enterprise level pricetag or jargon.

Huntress knows that cybersecurity takes a village, and that SMBs do not always have access to this village in the same way that corporations do. The driving ethos behind its MDR for Microsoft 365 platform is to make security simple and accessible, and to help fill the skills gap through Huntress’ team of experts, who act as an extension of their customers’ teams. This also means that MSPs and SMBs benefit from being in a feedback loop, enabling their MDR defense to evolve in step with the changes in cyberattackers’ behaviors.
Huntress’ MDR for Microsoft 365 gives SMBs all the defenses and benefits of a SOC via an affordable platform

Built by experts specifically for the SMB, Huntress’ MDR for Microsoft 365 platform provides continuous monitoring for suspicious indicators and behaviors of a potential compromise. It is fully up to date on tradecraft developments, giving MSPs the benefits of herd immunity (Huntress has been hunting malicious actors across hundreds of thousands of user accounts for its MDR for Microsoft 365 product), and it pairs the human element with AI developments. As such, the platform utilizes AI for better security posture, while also managing against threats potentially caused by AI itself.

Data collection also spots irregular behavioral patterns and activities that are then investigated for cybersecurity risk. To minimize false positives, SOC analysts validate the analytics to confirm if it is malicious activity. Incident reports via email and tickets summarize Huntress’ findings and outlines recommended remediation steps. These steps can often be executed in one click, with full details on any manual steps required. This makes both threat protection and threat resolution as easy and straightforward as possible.

Businesses that have benefited from Huntress’ MDR for Microsoft 365 include Ultra IT in New Zealand, which used the platform to defend itself against a BEC attack. “We liked that Huntress MDR for Microsoft 365 is purpose-built to meet the needs of smaller service providers like us,” says Andrew Fergus, Ultra IT’s managing director.

“Huntress understands that today, most small businesses are run from the Cloud, so, for our clients, email protection is absolutely critical. With 230 tenants under management, it is impossible for us to stay on top of every login and monitor all activity. Having the Huntress solution working in the background prevented what could have been a hugely costly and dangerous compromise for my client.”

For more customer success stories, visit www.huntress.com/success-stories.
Outpace cybercriminals with an MDR for Microsoft 365 platform that lets SMBs do more, with less

Despite the pressure of trying to protect their businesses from cybercriminals, there is help out there. SMBs face the tough balancing act of not having the budget or resources to create an in-house IT security team with the very real anxieties of what could happen if they do not protect theirs and their customers’ data. From revenue losses to reputational damage, increased cyber insurance premiums and the threat of lawsuits if an attack is successful, it’s tough for SMB leaders to stay calm in that climate.

But they are not alone: Huntress MDR for Microsoft 365 is built for the demands they are facing. Tailored to the needs of the 99%, Huntress’ platform gives IT resellers and SMBs the peace of mind and reassurance to let them focus on what they do best: serving their customers.
For more information on Huntress MDR for Microsoft 365, visit huntress.com/ProtectYourIdentities

This content was commissioned by Huntress and produced by TechTarget Inc.