MSP PARTNER RESOURCE

A GUIDE TO SELLING CYBERSECURITY

2019

CONTENTS

TEMPLATE INTRODUCTION

Keeping up with cybersecurity is hard. Advising non-technical owners of small and medium sized businesses is even harder. The Huntress team knows this is especially true when navigating budget constraints, regulations, and sales objections. To help ease this burden, we gathered our top security experts, sales reps, and marketers to create this channel focused sales guide. Inside, you'll find simple explanations, pros and cons, and pitch strategies for the key layers of an SMB focused cybersecurity stack.

It's important to stress that the world's largest businesses with multimillion-dollar security budgets cannot provide perfect prevention against hackers and insider threats. Expecting to do this on an SMB budget is a pipe dream. However, it is our job to reduce the risk of these attacks to a level acceptable by our clients' leadership. To help you understand and articulate these risks, we leveraged three decades of offensive cybersecurity expertise and identified which security layers will help reduce the risk of modern-day threats without breaking your clients' bank.

We tailored these recommendations to an MSP go-to-market strategy that can service five employee SoHos to 1,000 employee medium sized businesses. However, there's no such thing as a "one size fits all" business plan. Don't hesitate to further simplify this guidance to target different personas (e.g. creating a single best of breed offering that eliminates any basic/premium choices). With that said, we caution you against adding complexity if your goal is to scale beyond a lifestyle business. Although à la carte offerings provide your business maximum client flexibility, they also add significant overhead and can stifle the creation of repeatable streamlined processes. Don't underestimate the appeal and allure of giving clients a simple service decision.

Lastly, we wholeheartedly believe cybersecurity is a team sport that takes a community working together to secure the SMBs of world. As a result, we've designed this guide to be a living document that we frequently update. If you see something wrong, missing, or just have great advice to share with fellow MSPs, let us know! You can contact our team via email using marketing@huntresslabs.com.

Thank you so much for helping us raise the bar of SMB security and being part of the channel community!

The Huntress Team

COMPANY BACKGROUND

At Huntress, we believe the best defense is a good offense. We've spent our careers circumventing preventive security products to stay a step ahead of malicious actors. This mentality enables our products and analysts to tackle threats head-on. As a result, we force hackers to earn every inch of their access within the networks we protect and monitor.

Our team is extremely experienced and talented. Many of our security engineers regularly author cutting edge research to combat and counter global cyber-attacks. We're passionate about the problems we solve and pride ourselves in our ability to convey complex solutions in simple words. Most importantly, we're aligned with the goals of each organization we support—when your business prospers, so will ours.

Enterprise and SMB organizations partner with Huntress to reduce risk, maximize productivity, and protect their reputations. They value our tailored managed services and our customer-centric attitude. They also depend on our security guidance, user training, breach monitoring, and incident response services to complement the gaps in their security posture. This close relationship allows our partners to focus more on growing their business and less on the impacts of cyber threats.

Huntress – Our Offense is Your Defense.

ANTIVIRUS (AV) AND NEXT-GEN AV

The goal of Antivirus (AV) and Next-Gen AV is to prevent, detect, and remove malicious applications from laptops, workstations, servers, and mobile devices. All security stacks need to include one of these solutions to avoid claims of negligence. However, advising your clients of the right "flavor" can be tough. Simplify this process by only offering a basic or premium decision that will align with low and higher budgets. Make sure your MSA appropriately transfers risk, liability, and responsibility for cleanup to clients who choose the basic offering.

THE DIFFERENCE BETWEEN AV AND NEXT-GEN AV

Traditional AV takes a malware-centric approach and searches for pre-identified malicious patterns and behaviors exhibited by a program, script, or command. Next-Gen AV tends to focus more on the interaction of the entire operating system and analyzes the full context of an attack. AV and Next-Gen AV may use artificial intelligence techniques that can "self-learn" thereby improving detection of malware that slipped by initial inspection.

SALES STRATEGIES

To a non-technical business owner, these differences will likely fall on deaf ears so keep your pitch straightforward:

- *Many hackers perform complex attacks which require more costly solutions for more complete coverage. Cheaper alternatives exist, but you'll have to accept the full risk that comes with less comprehensive protection.*
- *Would you prefer to pay a little to find the simple threats or pay more to also find the complex threats that many attackers are currently leveraging?*

CLIENT BENEFITS

- Prevents detected malware from running which could cause client downtime, lead to data loss, and damage their business reputation.

GAPS IN PROTECTION

AV and Next-Gen AV are critical security layers, but are not bulletproof solutions. These technologies often fall prey to hacking techniques which abuse legitimate software for nefarious purposes, for instance, using OneDrive or Dropbox to exfiltrate stolen files to the attacker's cloud. When put between the tough choice of blocking potentially good software or allowing slightly anomalous behavior, many products choose not to immediately hinder productivity. As a result, perfect prevention from this technology isn't realistic. AV and Next-Gen AV are also limited in network monitoring capabilities and should be complemented with Firewalls with Intrusion Protection/Detection Systems and DNS Filtering.

DNS SECURITY

DNS security refers to leveraging DNS data—records and queries—for security purposes. While firewalls, filters, and other security layers also inspect network traffic, DNS Security can provide unique context and visibility into internal and external networks requests. It is also used to monitor and classify internet infrastructure to discover anomalies before attacks are launched. As a result, DNS Security can prevent your laptop, workstation, server, and devices from making malicious internet connections used to download malware and communicate with hackers' servers.

Mature DNS Security providers analyze large cross-sections of global internet activity and are able to observe new relationships forming between domain names, IP addresses, and autonomous system numbers (ASN). With this visibility, these providers are able to discover where attacks are staged and often predict where attacks will emerge before they even launch.

SALES STRATEGIES

DNS Security could sound a lot like a Firewall to SMB clients, so focus on the key differences. This includes how it can protect their employees against threats on the internet wherever they physically go (not just behind the Firewall). Another key feature of DNS Security is how it can block threats before they ever reach your clients' network or endpoints.

- *Provide the same level of protection to your off-site computers that you do with your on-site computers.*
- *If your computers were connecting to dangerous places on the internet, would you rather detect and respond to the malicious traffic when it arrives or prevent you computers from starting the dangerous communication in the first place?*

CLIENT BENEFITS

- Prevents outbound connections to malicious sites that use DNS.
- Reduces the burden placed on Antivirus by stopping phishing and malware infections earlier, identifying already infected devices faster, and mitigating data exfiltration.
- Delivers a comprehensive picture of real-time internet activity for on-premise and roaming devices, with reports on security, usage, and cloud services being accessed.

GAPS IN PROTECTION

Malware that uses IP addresses rather than DNS names may bypass some DNS Security solutions. Similarly, malware campaigns that use newly registered domain names may also bypass DNS Security because the domain is unknown; preemptively blocking these unknown domains can lead to false positives and a bad browsing experience for clients. Hackers have also started distributing malware from legitimate/trusted domains such as Pastebin, Box, Dropbox, GitHub, and others; DNS Security does not typically block connections to legitimate domains.

FIREWALLS (FW), NEXT-GEN FW, AND UTM

Firewalls, Next-Gen Firewalls, and Unified Threat Management appliances are designed to establish a barrier between the "untrustworthy" internet and the devices you're trying to protect. All security stacks need to include these solutions to avoid claims of negligence. In addition to selecting from multiple vendors, Firewalls can offer many add-ons and upgrades for purchase. Like Antivirus, simplify your sales process by only offering clients a basic or premium decision that will align with low and higher budgets. Make sure your MSA appropriately transfers risk, liability, and responsibility for cleanup to clients who choose the basic offering.

THE DIFFERENCE BETWEEN FIREWALLS, NEXT-GEN FW, AND UTM

Traditional Firewalls are designed to restrict network traffic based on source, destination, port, and protocol details. The decision to allow or block is determined by a ruleset which may have a GUI or configuration file interface. They also feature basic network services like DNS, DHCP, and VPN. Next-Gen Firewalls and UTMs include traditional Firewall functionality as well as advanced features. These add-ons often include decrypting, inspecting, and filtering traffic for spam, viruses, unwanted content such as dangerous or prohibited sites, and unwelcome Geo-IP locations. Some Next-Gen Firewalls and UTMs may include IDS/IPS (Intrusion Detection/Prevention System) functionality to detect and prevent network attacks.

SALES STRATEGIES

Firewalls have been a staple in security stacks for years and face less resistance than newer layers. However, the adoption of more comprehensive features available in Next-Gen Firewalls and UTMs can be an uphill battle. Address this issue head-on:

> *Now that most network traffic is encrypted (including malicious traffic), you'll need more advanced firewall technology to have high-visibility into the content that is entering and leaving your network. Without this, you jeopardize early detection of an incident which could escalate into a breach. Are you okay with accepting this risk?*

CLIENT BENEFITS

- Reduces the attack surface of systems that must be externally accessible by filtering incoming traffic.
- Restricts anomalous outbound traffic to the approved and essential services, ports, and protocols.
- Prevents and removes malicious web content including spam, viruses, exploits.
- When devices are behind this invisible shield, unpatched vulnerabilities may not be reachable.

GAPS IN PROTECTION

Appliance based Firewalls only protect devices on-premises (those behind the Firewall), thus providing no protection for remote/traveling employees unless all traffic is routed through a VPN connection. Since these appliances typically live on the edge of the network, there is no visibility of internal network traffic. Also, if malicious activity occurs within the internal network, visibility into the threat may require monitoring logs and will be limited to the source host or IP address. This will require time and expertise to confirm and incident happened and determine which process on a device is the source of the malicious traffic. To complement these gaps and minimize labor costs, considering leveraging agent-based DNS Filtering, Antivirus, Managed Detection and Response (MDR), and Security Information and Event Management (SIEM).

MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor Authentication adds one or more additional authentication requirements after a user successfully authenticates with a username and password. This technology is based on the simple concept that "something you know" is not enough information to certify a user is who they claim to be. To provide an acceptable level of certainty, MFA often requires proof via "something you have" (e.g. security code from a cell phone) or "something you are" (e.g. your fingerprint or detailed facial imagery).

Despite password-related incidents at an all-time high, MFA remains unpopular with SMB clients due to the added cost and perceived inconvenience of MFA services. However, a recently unsealed indictment in Pennsylvania, USA[1] detailed that SMBs in construction, finance, healthcare, legal, and manufacturing were targeted for their banking credentials and the situation "had the potential to cause an excess of $100 million in losses." Considering the equally targeted attacks against MSPs in 2019 which also leveraged compromised passwords, not using MFA on all systems that provide remote access is reckless and borderlines negligence.

SALES STRATEGIES

Many clients only exposure to MFA is with text message delivered one-time pins and easy to misplace backup codes. Considering this user experience, it's no surprise that clients feel inconvenienced by MFA. In sales scenarios like this, it's important to show how things have improved and how they would be protected from hackers. Live hacking demos are an ideal way to close this business:

> **[Sales Rep]**: *As you see on the attacker's screen, we've used the recently leaked passwords from Yahoo to brute force a theoretical remote desktop server.* <succeeds>
>
> **[Audience]**: <silently in awe of how easy this is>
>
> **[Sales Rep]**: *With this access, I can steal sensitive files and turn your webcam on.*
>
> **[Audience]**: <slightly uncomfortable, regretting they threw away that webcam cover>
>
> **[Sales Rep]**: *With MFA enabled, the brute force succeeds but the employee denies the push notification.*
>
> **[Audience]**: *Will that work with Office 365 and how much is it?*
>
> **[Sales Rep]**: [$(͡° ͜ʖ ͡°)$]

CLIENT BENEFITS

- Reduces the potentially devasting risks associated with compromised passwords caused by phishing, keystroke logging, brute force attacks, 3rd party data breaches, and password reuse.
- Helps ensure the confidentiality and integrity of systems are not compromised by hackers or unauthorized users which could result in lawsuits and/or fines.
- Begins the path to Zero Trust by making sure all users pass the same tests before they are "trusted".

GAPS IN PROTECTION

MFA, while critical, is only one component of a layered security stack. Since it only deals with authentication, you need the other layers to build a comprehensive security solution.

[1] https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled

MANAGED DETECTION AND RESPONSE (MDR)

Managed Detection and Response services provide threat monitoring, detection, and response without the need of dedicated security staff. Implementation and response actions vary from vendor to vendor but most tend to include advanced analysis, threat intelligence, and human expertise. The goal of MDR is to quickly identify threats that bypassed preventive security controls before incidents escalate. These solutions may examine unaddressed host or network-based indicators of compromise in order to complement gaps in existing security layers.

For MSPs, MDR can work as force multiplier that enables junior IT staff to address complex security incidents. Response capabilities can also reduce labor costs by providing non-technical, risk-based overviews, explicit remediation guidance, and automated disruption or containment of an incident. Depending on the structure of your MSA, MDR services also have the potential to generate new project review from security findings. Industry analysts estimate 15% of worldwide organizations will adopt MDR services by 2020.

SALES STRATEGIES

Unlike Antivirus and Firewalls, newer approaches to cybersecurity can feel complicated and overwhelming to SMB prospects. MDR is one of few layers of security that proactively takes the fight to the hackers. Use simple analogies to demonstrate the value:

- *MDR is similar to a guard dog in your backyard. When a burglar hops your fence, the dog chases down the intruder—preventing the theft of any valuables.*
- *When hackers slip into your network, you have two choices: wait for their actions to trigger an alarm or hire a Seal team to hunt them down. When it comes to your business, which approach would you prefer?*
- *Like routine health checks, MDR does not prevent an incident from happening. However, these frequent screenings proactively discover infections before serious harm occurs.*

CLIENT BENEFITS

- Discover hard-to-detect persistent threats that abuse legitimate software and operating system features to bypass Antivirus and Next-Gen Antivirus.
- An offensive approach to cybersecurity means you are not waiting for something catastrophic to happen before you are able to respond.

GAPS IN PROTECTION

Managed Detection and Response focuses on threat hunting but does not block incidents from occurring. Due to this specialization, MDR is not a suitable replacement for Antivirus, Firewalls, and other preventive solutions. Depending on the indicator of compromise analyzed by your MDR solution, it's possible MDR could overlap or duplicate the functionality of other existing security layers (e.g. inspecting DNS traffic may also be performed by DNS Security or Next-Gen Firewalls). Lastly, the price of some MDR solutions may be cost prohibitive for many SMB clients.

FUTURE RESEARCH TOPICS

As mentioned in the introduction, this is a living document that we plan to frequently update. Based on feedback received thus far, we expect to cover the following cybersecurity solutions in the future:

- APPLICATION WHITELISTING (AWL)
- BACKUPS AND DISASTER RECOVERY (BDR)
- CLOUD BASED EMAIL SECURITY
- DARK WEB DATA MONITORING
- END USER SECURITY AWARENESS
- SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
- VULNERABILITY ASSESSMENTS AND PENETRATION TESTS