Private Communications Corporation

How to Sell ZTNA

Introduction

The cybersecurity landscape for small and medium-sized businesses (SMBs) is becoming increasingly perilous. Despite a common belief that their size makes them less attractive targets, cybercriminals view these businesses as easier targets due to their often weaker security infrastructures. Moreover, many SMBs remain unaware of the critical role they can play in the supply chain as entry points for larger attacks on enterprises. With limited IT resources and the challenges of evolving threats and regulatory requirements, SMBs are vulnerable and ill-prepared to recover from significant cyber incidents.

Amid this environment, Managed Service Providers (MSPs) have a unique opportunity to position themselves as trusted advisors, helping SMBs adopt modern cybersecurity solutions like Zero Trust Network Access (ZTNA). ZTNA offers a more robust security approach that directly addresses the limitations of traditional VPNs and firewalls, making it an ideal solution for today’s complex and dynamic IT environments. Yet, selling ZTNA to SMBs requires overcoming common objections, such as perceived high costs, lack of visible benefits, and misconceptions about their risk levels.

This white paper provides MSPs with the tools and strategies needed to effectively sell ZTNA to SMBs. It explores the current cybersecurity challenges faced by SMBs, the advantages of ZTNA, and how MSPs can communicate its value to clients. By reframing cybersecurity as a critical investment and demonstrating the real-world benefits of ZTNA, MSPs can empower SMBs to safeguard their future and thrive in today’s digital world.

The SMB Cybersecurity Landscape

SMB are very vulnerable to cyberattacks, with over 40% of cyberattacks targeting these businesses. Many SMBs believe that their size makes them less attractive to hackers. However, cybercriminals increasingly see SMBs as low-hanging fruit due to their often weaker cybersecurity infrastructure.

SMBs also face unique challenges, including limited IT resources, evolving cyber threats, and increasing regulatory pressures. These businesses are often unaware that they serve as entry points into larger enterprises. A breach at an SMB can lead to a larger attack on a more significant target within their supply chain. Furthermore, SMBs often lack the financial resources to recover from a severe cyberattack, with statistics showing that 60% of SMBs go out of business following a cyber incident.

Given these vulnerabilities, MSPs have an opportunity to play a crucial role in raising awareness of these risks and offering modern cybersecurity solutions like ZTNA to protect SMBs from such attacks.

Overcoming SMB Resistance to Cybersecurity Investment

Despite the rising threats, many SMBs remain resistant to adopting stronger cybersecurity measures. This resistance stems from several factors:

- **Perceived cost:** Many SMBs believe they are already paying enough for cybersecurity and feel that additional investment is unnecessary.

- **Invisible benefits:** Unlike other business investments that offer visible returns, cybersecurity's value lies in what does *not* happen—successful attacks prevented, and breaches avoided. It can be difficult to justify the expense of solutions when their success is measured by the absence of incidents.

- **Misconception of risk:** SMBs often assume they are not high-value targets for hackers due to their size. However, SMBs are, in fact, prime targets for cybercriminals because their defenses are typically easier to penetrate.

MSPs must address these concerns by reframing the conversation around cybersecurity risks and focusing on the existential threat cyberattacks pose to SMBs. A critical part of this conversation is educating SMBs about the potential costs of not investing in stronger security, such as lost revenue, damage to their reputation, and regulatory fines.

The Case for Zero Trust Network Access (ZTNA)

Traditional cybersecurity models, such as Virtual Private Networks (VPNs) and firewalls, are proving inadequate for today’s complex IT environments. With the rise of remote work, cloud computing, and IoT devices, SMBs need a more robust security framework.

This is where ZTNA comes in.

ZTNA operates on the principle of "never trust, always verify." It assumes that no one—whether inside or outside the network—can be trusted by default. Every user, device, and application must be continuously authenticated and authorized before gaining access to resources.

Key principles of ZTNA include:

- **Least privilege access:** Users are granted access only to the specific resources they need, reducing the potential attack surface.

- **Continuous verification:** Access is granted only after users and devices are authenticated and authorized at every request.

- **Micro-segmentation:** Permission is granted to the individual resource – app, website, SaaS app, IoT (Internet of Things), etc. This limits the scope of any potential attack and reduces the impact of breaches.

For SMBs, ZTNA offers enhanced security for remote and hybrid workforces, reduces the attack surface, ensures compliance with industry regulations, and helps mitigate insider threats.

Why SMBs Should Adopt ZTNA

- **Enhanced security for hybrid workforces:** The shift to remote and hybrid work environments has expanded the attack surface for SMBs. Traditional VPNs and firewalls were not designed to handle the complexities of dynamic work environments, where employees, contractors, and third-party vendors need access to corporate resources from various devices and locations. ZTNA ensures that every access request is authenticated, minimizing the risk of unauthorized users exploiting vulnerabilities related to remote work.

- **Reduction in attack surface:** ZTNA significantly reduces the attack surface by adhering to the principle of least privilege. This approach ensures that users only have access to the resources they need to perform their job functions, minimizing the opportunities for attackers to exploit weaknesses in the system.

- **Compliance and risk management:** SMBs in industries like healthcare, finance, and manufacturing face stringent regulatory requirements, including standards such as HIPAA, PCI-DSS, and GDPR. ZTNA's continuous authentication makes it easier to implement the strict access controls required by these regulations. Additionally, ZTNA provides detailed audit logs, making it easier for SMBs to demonstrate compliance during regulatory assessments.

- **Cost efficiency and scalability:** While many SMBs are concerned about the cost of adopting new security technologies, ZTNA can be more cost-effective than traditional solutions in the long term. By reducing the need for extensive on-premise infrastructure and minimizing security risks, ZTNA helps SMBs save on operational costs. ZTNA is also scalable, allowing businesses to grow and adapt without significant increases in security expenditure.

- **Mitigating insider threats:** Insider threats, whether malicious or accidental, pose a significant risk to SMBs. ZTNA continuously monitors user behavior, detecting suspicious activity that could indicate an insider threat. By authenticating each access request and monitoring for abnormal behavior, ZTNA provides early detection of insider threats, allowing SMBs to take swift action before a breach occurs.

The MSP Opportunity: Selling ZTNA to SMBs

MSPs are in a unique position to help SMBs adopt ZTNA and strengthen their cybersecurity posture. However, selling cybersecurity solutions requires a different approach than selling traditional technology products.

MSPs must take on the role of trusted advisors, offering consultative sales approaches tailored to the specific needs and vulnerabilities of each SMB. The key to success lies in conducting thorough assessments of an SMB's security posture and helping clients understand the real-world risks they face.

While some MSPs may be hesitant to push ZTNA due to SMB resistance, MSPs should focus on framing cybersecurity as a critical investment that can save SMBs from potentially devastating financial and reputational losses. MSPs can overcome objections by educating SMBs on the benefits of ZTNA and how it addresses modern cybersecurity challenges.

MSPs should also leverage case studies and real-world examples to demonstrate the tangible benefits of ZTNA. By sharing success stories from other SMBs, MSPs can illustrate the value of ZTNA and how it helps businesses stay secure in an increasingly complex threat landscape.

How MSPs Can Help SMBs Overcome Resistance

When selling ZTNA to SMBs, MSPs should focus on the following strategies to overcome resistance:

- **Educate SMBs on the risks they face:** Many SMBs are unaware of the severity of the cyber threats they face. MSPs should provide real-world examples of attacks on SMBs and the devastating financial and reputational consequences of these breaches.

- **Highlight the benefits of ZTNA:** MSPs should explain how ZTNA addresses the limitations of traditional security models and why it is essential for today's hybrid work environments. This includes emphasizing the cost savings and compliance benefits of ZTNA.

- **Offer tailored security solutions:** MSPs should conduct thorough assessments of each SMB's security posture and recommend customized ZTNA solutions that address their specific vulnerabilities.

- **Build trust as a cybersecurity partner:** MSPs must position themselves as trusted advisors who are invested in the long-term security and success of their SMB clients. This means offering ongoing support and education to help SMBs stay ahead of evolving cyber threats.

ZTNA: The Next Generation of Cybersecurity for SMBs

Managed Service Providers (MSPs) play a vital role in helping SMBs navigate the complex world of cybersecurity. By offering ZTNA, MSPs can provide SMBs with a modern, scalable solution that addresses the challenges of remote work, evolving cyber threats, and regulatory pressures. For SMBs, ZTNA is not just an option—it is a necessity in today's rapidly changing cybersecurity landscape.

MSPs that successfully position themselves as trusted advisors and offer tailored ZTNA solutions will be well-positioned to help their SMB clients protect their networks, data, and reputation from increasingly sophisticated cyber threats.