3 Elements of a Successful Managed Security Services (MSS) Bundle

October 19, 2018 / in Partners, Small & Medium Businesses / by Joe Velderman

The small- and medium-sized business (SMB) market is rapidly accelerating its adoption of converged managed IT services to alleviate headaches and prevent risks.

More and more businesses use cloud-based services for enterprise applications, processing or communications, placing an even higher priority on network performance and reliability. Yet many SMBs are facing a cybersecurity crisis.

Cyber threats are continuing to get more sophisticated and frequent; SMBs are becoming a more routine target. 61 percent of SMBs experienced a cyber breach in 2017, compared to 55 percent in 2016.

Most managed IT service providers recognize that SMBs don't have the awareness, knowledge or resources to implement cyber defense mechanisms to effectively protect their data, devices and people. Furthermore, the cybersecurity services market has developed enterprise-class solutions aimed at large enterprise businesses because they have historically been prime targets.

> "The challenge for MSPs is finding effective tools that pair well with internal processes to mitigate the risk of a cyber breach, threat of downtime or damage to customers' reputation."

There are incredible opportunities for MSPs to develop service options customized for SMBs to address cybersecurity woes while accommodating limited budgets. MSPs that are focused on this will continue to add real value to the services they are providing and strengthen customer relationships by building trust.

The challenge for MSPs is finding effective tools that pair well with internal processes to mitigate the risk of a cyber breach, threat of downtime or damage to customers' reputation. If bundled intelligently, these services are any easy sell. No business owner wants to see their organization featured on the six o'clock news for a data breach.

Consider three foundational elements of an MSSP plan. These may consist of several individual services, but those services are aimed at protecting specific functions.

Data Protection

Just like their enterprise counterparts, small businesses have a growing data footprint. Storage keeps getting less expensive and many SMBs don't have a data governance policy, causing the gigabytes to pile up.

Whether the data is stored on-premises or in the cloud, it's important to have appropriate protections in place, but also the ability to restore data in the event of a disaster or cyberattack. Good MSSP bundles aimed at protecting data will include:

- **Content Filtering:** Having a web filtering service to block inappropriate, unproductive or malicious websites is a major first step in preventing cyberattacks.

- **Email Security:** Implement secure email solutions to protect SMBs from email-borne threats, such as ransomware, zero-day attacks and spear-phishing attempts, and comply with regulatory mandates to encrypt sensitive emails.

- **Backup & Disaster Recovery:** Ensure that an SMB's data is effectively backed up; whether it lives on a workstation, on-premises device or in the cloud. Being able to restore information that has been compromised is the best insurance policy.

Device Protection

Endpoint devices come in all shapes, sizes and flavors, but the quantity of devices continues to grow. This means that there are more potential intrusion points than ever before. It's important for a good MSSP bundle to include services aimed at protecting and monitoring endpoint devices.

- **Endpoint Management:** MSSPs should have a comprehensive inventory of all devices associated with an SMB customer. Good endpoint management solutions will allow MSSPs to push updates and security patches as they are released to ensure that endpoints stay hardened.

- **Endpoint Security**: It almost goes without saying, but having a solid antivirusendpoint security solution in place is still one of the best defenses for protecting endpoint devices.

- **Endpoint Rollback:** Mistakes happen. Phishing emails are opened. Malicious links are clicked. But MSSPs can add value for their customers by using endpoint protection solutions that include automated rollback features for those events when a device is compromised.

People Protection

The human element is the most difficult to control and the hardest to protect. But it is critical.

Provide convenient and easy pathways for people to adopt sound security behavior. A consistent security awareness culture makes it easier for users to be aware of security threats. Consider the following bundled services as part of your MSSP offering.

- **Virtual Private Network (VPN):** Provide a secure lane for all SMB endpoints to work over a VPN connection. A VPN client may route back to the customer's network if there are on-premises connectivity demands, or it may be more generic VPN connection to an MSSP's gateway. VPNs are prevalent and not just for workstations anymore. Modern VPN services offer clients for just about any type of endpoint and are especially important for mobile devices.

- **Policies & Procedures:** Provide template policies and procedures to your SMB customers. Again, many of them are leaving IT management, including governance, up to you. Providing basic templates for things like password management, backup and user provisioning is an easy way to get them to create a more robust security awareness culture.
- **Security Awareness Training:** For SMBs that subscribe to your MSSP bundle, provide them with routine threat awareness and simple tips and tricks to enforce that security awareness culture.

The most effective MSSP program is dependent on partnerships. Partnerships between SMBs and their IT partners, but also partnerships between MSSP providers and solutions providers. MSPs that bundle services to offer an MSSP will be well-suited to work with security vendors able to offer a comprehensive spectrum of services for their SMB customers.

About ProviNET

ProviNET is a SonicWall SecureFirst Gold Partner. For nearly three decades, ProviNET has delivered trusted technology solutions for healthcare organizations. Whether it's a single project or full-time onsite work, ProviNET designs and implements customized solutions so healthcare organizations can focus on core services.

ProviNET's tight-knit group of experienced, industry-certified personnel are focused on customer satisfaction. They are a reputable organization, fulfilling immediate IT needs and helping plan for tomorrow. They are ready to put their extensive knowledge to work for healthcare, developing strategies and solving challenges with the latest technology.

To learn more about ProviNET, please visit **www.provinet.com**.

JOE VELDERMAN

Director of Consulting Services | ProviNET Solutions

Joe Velderman has extensive experience providing advisory services to the senior living and long-term, post-acute care industry. ProviNET Solutions is a full-service technology consulting partner that was born out of a senior living provider and aims to help organizations be successful with technology. Joe developed a passion for ensuring healthcare organizations maintain regulatory compliance, but also mitigate cybersecurity risks. He routinely contributes thought leadership on this topic through whitepapers, blog posts, educational webinars and speaking engagements.

Tags: Cybersecurity, Data Protection and Encryption , endpoint security, MSSP