SMBs: How to Strengthen Your Cybersecurity

The average cost of a cyber attack is

$3.6 million.

60%

of businesses attacked shut down six months later.

Experts say that the number of cyber attacks on companies, especially small and medium-sized businesses (SMBs), will continue to increase. No organization can afford to be unprepared. In this article, you'll learn how Cisco Start security solutions can help secure your SMB against such attacks.

As an SMB owner, you may think twice about spending money to strengthen your company against cyber attacks, and that's understandable. But you may want to think again when you consider this: One expert estimate puts the average cost of a cyber attack at $3.62 million;[1] another report notes that 60 percent of businesses attacked shut down six months later.[2]

If you are convinced of the financial risks associated with a cyber attack and want to shop for cybersecurity solutions, know that there is no one-size-fits-all solution.

Here is a checklist of suggested questions[3] you can ask to help you assess and choose the appropriate cybersecurity solution for your SMB:

- **Will the solution help you achieve security or just compliance?**
  Remember, being compliant does not equal being secure. It's better to buy a solution that provides both compliance and security.
- **How experienced must your employees be to manage the solution?**
  Putting it another way, would your SMB get the same results from the solution if you didn't have the best IT staff?
- **Will it support your SMB throughout a risk-management lifecycle?**
  You need support through risk identification, risk assessment, risk mitigation, and risk monitoring.
- **Will it help you differentiate between daily activity and real cyber threats?**
  Your security solutions should not impede daily work as they differentiate between normal and suspicious cyber activity.
- **What do you know about the vendor's stability and performance record?**
  Research how well qualified and reliable the vendor is before you buy its solution.
- **Does the vendor provide good tech support and good customer service?**
  At no point should your SMB be stranded if something goes wrong. Your vendor must stand by you 24-7 and have a clear solutions roadmap that evolves with technology changes and your business.

Start with Cisco

With these questions in mind, you can now take the first step in enhancing the cybersecurity of your SMB–starting with the best.[4]

Cisco® cybersecurity solutions are consistently rated as having the fastest time to detection and are known to detect 100 percent of malware, exploits, and evasions in less than 5 minutes.

Cisco Start's customizable suite of security solutions–which covers cloud, network, and endpoints–is appropriate for companies that demand enterprise-class technology on a budget palatable to the scale of small and medium-sized businesses. If that resembles your business, here are three Cisco Start cybersecurity solutions that can strengthen your defenses against cyber attacks.

Cisco Umbrella[5]–The First Line of Defense

Cisco Umbrella® is a cloud-delivered security service that provides the first layer of defense against threats. It offers the simplest, fastest way to protect every device on your branch network and uses the Internet's infrastructure to block malicious destinations before a connection is ever established.

The key features of Cisco Umbrella are:

It is preemptive: Umbrella uses Domain Name Servers (DNS) to stop threats over all ports and protocols–even direct-to-IP connections–before they reach your endpoints or network. It can do this because it uses big data and data mining methods such as machine learning, graph theory, anomaly detection, and temporal patterns to predict the Internet origin of attacks before they happen. The data is sourced from the 80 billion DNS requests that Cisco routes and resolves daily for 65 million customers in more than 160 countries.

It uses world-class intelligence: Cisco Umbrella uses Cisco Talos™ and other third-party feeds to determine if a URL is malicious. Talos is Cisco's threat intelligence organization, with hundreds of industry-renown security experts who research attacks and vulnerabilities and feed this intelligence across Cisco products. You can also create a list of custom URLs to be blocked based on your policies.

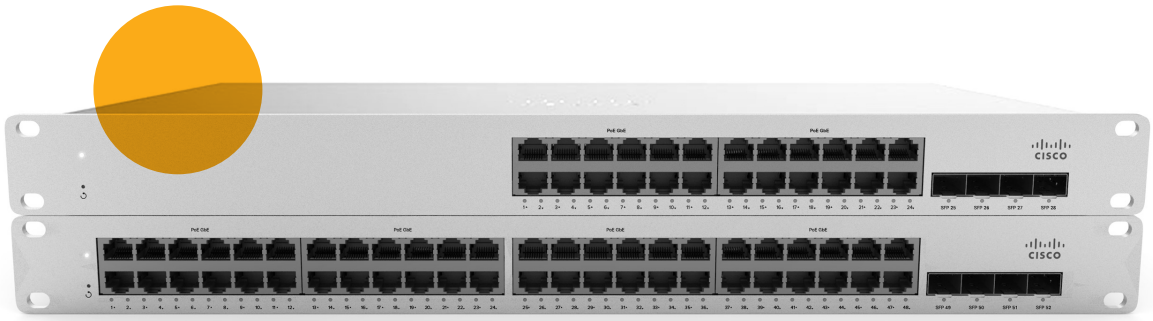
It is predictive: Cisco Umbrella learns from Internet activities to automatically identify attacker infrastructure staged for current and emergent threats. It captures and understands relationships between malware, domains, IPs, and networks across the Internet. Even if a device gets infected in other ways, Umbrella prevents connections to the attacker's server, stops data theft, and prevents any ransomware from executing encryption.

It offers visibility: You have visibility on all employees' Internet activities across all devices and over all ports, even when they are off the corporate network. And activity logs can be kept forever. It also uncovers activities across your smart devices like surveillance cameras, smart thermostats, smart TVs, etc.

Umbrella is a cybersecurity solution that recognizes a potential attack and blocks a suspicious DNS request before the browser connects to the malicious site. It is affordable too, at just US$38 per user each year. Best of all, it is the easiest cybersecurity solution you will ever deploy, because it sets up in minutes.

Cisco Meraki MX Security[6]—Unified Threat Management

Cisco Meraki® MX Security Appliances are ideal for SMBs looking for a Unified Threat Management (UTM) solution. With Meraki MX, you get a comprehensive suite of network services, which removes the need to shop for multiple appliances.



The MX is 100-percent native cloud managed, which makes installation and remote management seamless and simple. The comprehensive suite of Meraki MX network services includes:

Software-Defined WAN

Software-defined WAN (SD-WAN) is the latest WAN technology that easily overlays your company's existing WAN setup and empowers your IT staff to manage multiple types of connections through a single interface. And since it is software, it is easily and quickly configured onto your current infrastructure. SD-WAN is known for its security, reliability, ease of use (secure deployments, one dashboard, one- or two-click insertion), and network visibility, which allows for quicker and more accurate troubleshooting and problem solving. An SD-WAN architecture is especially good if your SMB is spread over a few geographies, as it increases communication and security across different networks and is easily scalable. Best of all, it is completely flexible, and you can set up the SD-WAN network in any way that suits your infrastructure.

Cloud-Managed Architecture

Built on Cisco Meraki's award-winning cloud architecture, the MX is the industry's only 100-percent cloud-managed solution for UTM and SD-WAN in a single appliance. MX appliances have a self-provision feature that automatically pulls policies and configuration settings from the cloud. Powerful remote management tools provide networkwide visibility and control and enable administration without the need for onsite networking expertise.

Ironclad Security

Layer 7 fingerprinting technology lets administrators identify unwanted content and applications and prevent recreational apps like BitTorrent from wasting precious bandwidth.

The integrated Cisco Snort® engine delivers superior intrusion prevention coverage, a key requirement for PCI 3.0 compliance. The MX also uses the Webroot BrightCloud URL categorization database for CIPA/IWF-compliant content filtering. And all this is complemented by the Cisco Advanced Malware Protection (AMP) engine for antimalware (see below), AMP Threat Grid cloud, and MaxMind for geo-IP-based security rules. Also, Meraki MX's industry-leading Layer 7 security engines and signatures are always kept up to date via the cloud, which simplifies network security management and provides peace of mind to IT administrators.

Another security feature of Cisco Meraki is its unique autoprovisioning site-to-site VPN, which connects branches securely, without tedious manual VPN configuration. Leveraging the power of the cloud, Meraki MX Security Appliances configure, monitor, and maintain your VPN, so you don't have to. Auto VPN also simplifies the process of hub configuration, eliminates risk, and minimizes network administration.

Lifetime care

Cisco Meraki MX Security Appliances include a limited lifetime hardware warranty with next-day advance hardware replacement. Cisco Meraki's simplified software and support licensing model also combines all software upgrades, centralized systems management, and phone support under a single, easy-to-understand model.

AMP[7,8]—Visibility and Control to Defeat Advanced Attacks

The AMP solution is an all-rounder, as it protects your SMB before, during, and after an attack.

Before: AMP uses global threat intelligence from Cisco Talos Security Intelligence and Research Group and Threat Grid intelligence feeds. It blocks malware trying to enter your network in real time by analyzing files at the point of entry to catch known and unknown malware. The result? Faster time to detection and automatic protection. Experts analyze millions of malware samples and terabytes of data daily and push all this to AMP. AMP then correlates files, telemetry data, and file behavior against this context-rich knowledge base to proactively defend against known and emerging threats.

During: AMP combines the above intelligence with known file signatures and Cisco Threat Grid's dynamic malware analysis technology to identify and block policy-violating file types, exploit attempts, and malicious files trying to infiltrate the network.

After: AMP moves beyond point-in-time detection and continuously monitors and analyzes all file activity and traffic and searches for any hints of malicious behavior. If an unknown file or a file previously deemed "good" starts to misbehave, AMP will detect it and instantly alert security teams to a potential compromise. It shows your IT security team where the malware originated from, which systems are affected, and what the malware is doing. It also provides the controls to rapidly respond and neutralize it with a few clicks.

With so many cybersecurity threats to defend against, along with a limited IT budget, shopping for a cybersecurity solution can be challenging.

With the comprehensive and affordable range of Cisco Start security solutions, you don't need to delay making the right choices.

Talk to our Cisco Start team today and let our experts advise you on how Cisco products can better secure your SMB against cyber attacks, starting with Umbrella, Meraki MX, and AMP.

1. *2017 Cost of Data Breach Study*, Ponemon, 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

2. Gary Miller, "60% of Small Companies That Suffer a Cyber Attack Are Out of Business Within Six Months," The Denver Post, Mar. 24, 2017. http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

3. Natalie Walsh, "14 Questions to Ask Yourself Before Committing to a Cybersecurity Vendor," Threat Stack, June 14, 2017. https://www.threatstack.com/blog/14-questions-to-ask-yourself-before-committing-to-a-cybersecurity-vendor/

4. "Cisco Leads Again in NSS Test," Cisco. https://www.cisco.com/c/m/en_sg/offers/sc07/amp-analyst-report/index.html
Note: requires registration to access report. NSS Labs is the global leader in operational cybersecurity testing. https://www.nsslabs.com/company/about-nss/

5. https://umbrella.cisco.com/products/features

6. https://meraki.cisco.com/solutions/mobile-device-management

7. "Visibility and control to defeat advanced attacks," Cisco AMP. https://www.cisco.com/c/en_au/products/security/advanced-malware-protection/index.html#~stickynav=1

8. *Cisco Advanced Malware Protection: Breach Prevention, Detection, Response, and Remediation for the Real World*, Cisco, 2016. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware protection/solution-overview-c22-734228.pdf