



The MSP's Guide to a Multi-Layered Security Approach

8 steps to ensure your security practice covers the
full lifecycle of cybersecurity management.

About this guide

This guide discusses the importance of helping SMB clients secure their businesses by implementing a layered security approach with comprehensive coverage over the cybersecurity lifecycle.

- Under siege**1-2
 - Why SMB clients must secure their business 1
 - Attacked from all sides.....2

- Fortifying SMB defenses** 3-4
 - The need for a multi-layered, proactive defense3
 - Using industry standards as a guide.....4

- 8 steps to build a complete security practice**..... 5-14
 - 1. Implement identity protection policies and solutions 5-6
 - 2. Put endpoint security in place7
 - 3. Layer on additional email security.....8
 - 4. Enforce data protection and compliance..... 9-10
 - 5. Implement web and network security together 11
 - 6. Begin ongoing end user security training 12
 - 7. Add mobile security 13
 - 8. Create a disaster recovery, backup, and incident response plan 14

- Your security experts** 15
 - Putting it all together.....15

Under siege

Why SMB clients must secure their business

The threat is real. As the startling statistics below show, businesses are under siege. Cyberattacks are possible at any time and have the potential to cause irreparable damage. Small- and medium-sized businesses (SMBs) are especially vulnerable due to their lack of awareness, knowledge, and resources, which can leave them feeling overwhelmed and alone against a looming threat landscape.

68%

of SMBs experienced a serious cloud security incident in 2022.¹

61%

of SMBs felt their organization might be hit with a successful ransomware attack in the next 12 months.²

\$4.35 million

is the average total cost of a data breach in 2022.³

42%

of SMBs attribute their security issues to lack of training.²

MSPs must protect themselves before they can protect their clients

MSPs are one of the biggest threats to their downstream clients' security. By leveraging a remote monitoring and management (RMM) tool, an MSP has direct reach into each of their clients' endpoints. This is the exact access a cybercriminal wants – instead of needing to break into each business individually, an attacker can target an MSP's RMM tool to gain access to the system and push ransomware to all the MSP's clients at once.

MSPs need to protect themselves before they can protect their clients – so always follow all the same best practices that you recommend to clients.

Under siege

Attacked from all sides

What's especially daunting about modern cybersecurity is the reality that cybercrime is on the rise overall, and there are increasingly more types of threats to know about and defend against.

From barrages of brute-force style direct assaults (such as DDoS attacks on networks and algorithm-fueled password attacks) to sneakier attacks that aim to slip past system defenses and cause damage or steal sensitive information, there is both an increasing volume and variety of cyberattacks poised to breach your clients' digital infrastructure.

Cybercriminals are growing more sophisticated, making them harder to defend against.

Social engineering techniques manipulate and exploit human behavior to bait users into giving up valuable information. This is especially effective if a person's password is compromised, and the attacker can take advantage of the victim's trust in their contact list.

Phishing attempts are getting much harder to recognize – gone are rampant grammatical errors, awkward phrasing, and suspicious formatting. Phishing emails and websites have become more successful at mimicking real people and legitimate brands to convince end users to give up sensitive information.

Business email compromise (BEC) attempts can trick even savvy users who see an urgent, personalized message seemingly from their boss and rush to respond.

Spoofing techniques have been greatly enhanced, using professional graphics to mimic trusted brands and trick users into downloading malware.

Zero-day attacks and fileless executable malware that can slip past attachment scanning tools are becoming more prevalent.

Trojan horses
Imposter malware or code disguised to appear legitimate to gain backdoor system access.

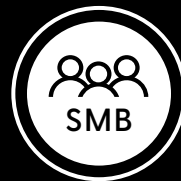


Password attacks
Hacking attacks (which can use scripts, algorithms, password sniffers, or keystroke loggers) that seek to obtain a system password for illegal access.



Spyware
Malicious software that infiltrates devices to gather information.

DDoS attacks
Distributed denial of service (DDoS) attacks that overwhelm the resources of a network.



Eavesdropping
Attempts to steal data transmitted by devices across an unsecured network.

Malware, worms, and viruses
Malicious software meant to damage or steal data from a device or network.



Phishing
Attempts to trick users into sharing sensitive info by posing as a trusted entity.











Ransomware
Malware that locks users out of a device, system, or data until a fee is paid.

Fortifying SMB defenses

The need for a multi-layered, proactive defense

To defend against an increased rate and range of attacks, businesses need to take a multi-layered defensive approach that overlaps safeguards, limited access points, end user training, and perimeter defenses.

Essentially, modern companies need to become digital fortresses, with multiple layers of proactive protection that serve to monitor, detect, alert, and prevent the onslaught of cyberattacks.

 <p>1. Identity protection and access management</p>	 <p>2. Endpoint security</p>	 <p>3. Email security</p>	 <p>4. Data protection</p>
 <p>5. Web and network security</p>	 <p>6. End user training</p>	 <p>7. Mobile security</p>	 <p>8. Disaster recovery, backup, and incident response plan</p>

Fortifying SMB defenses

Using industry standards as a guide

The Center for Internet Security (CIS) Critical Security Controls (referred to as **CIS Controls**) are a recommended set of actions for cyber defense, providing specific and actionable ways to thwart cyberattacks. There are 18 high-priority actions – and 153 specific safeguards – that present a strong starting point for any organization looking to enhance their security framework.

A security framework is a combination of tools, policies, people, and documentation – defining policies and procedures for establishing and maintaining a set of security controls. **Implementing CIS Controls** endorsed by PCI, HIPAA, NIST, and cyber insurance agencies can keep your organization compliant and insulated from cyberthreats. This will also set you up for future success as compliance measures continue to expand. Between supply chain attacks, compliance and regulatory concerns, and subrogation from insurers, it is vital that you create a defensibility posture for your business.

18

High-priority actions

153

Specific safeguards

8 steps to build a comprehensive security practice

1. Implement identity protection policies and solutions

Passwords are the key to accessing business data, but passwords alone are becoming an increasingly simple lock for hackers to pick. In addition to implementing strong password policies, passwords should be reinforced with extra layers of security such as multi-factor authentication (MFA). However, it's also important to balance security with productivity – otherwise, users can experience “password fatigue” due to the effort of maintaining unique passwords for every account or become frustrated by completing MFA every time they want to sign in.



Enforce strong password policies

While passwords shouldn't be the only line of defense to data, make them as strong as possible by enforcing password policy best practices throughout an organization.

- Require long password strings with a mix of letters, numbers, symbols, and capitalization
- Set time limits for passwords to expire and don't allow recent passwords to be reused



Enable MFA

MFA is the best defense to reinforce passwords and strengthen access security. MFA safeguards access to apps and data by requiring a second form of authentication in addition to a password, such as time-based codes sent via text, email, app, fingerprints, or answers to personal security questions.

24%

of SMBs blame cybersecurity issues on weak passwords.²

99%

of compromised accounts didn't have MFA enabled.⁴

8 steps to build a comprehensive security practice

1. Implement identity protection policies and solutions



Combine single sign-on (SSO) with MFA where possible

Signing into an app can slow users down by 10–30 seconds, which adds up with each app used. To help users remain productive while maintaining security, enable SSO whenever possible (e.g., for all Microsoft apps) to reduce the number of credentials that users must manage and the number of sign-ins they have to complete each day. SSO also helps reduce desk tickets related to password resets.



Apply conditional access (CA) rules

To further balance security and usability, set rules to limit MFA when users are in the office but continue to enforce MFA on untrusted networks (home, airports, coffee shops, etc.). This reduces user frustration at being slowed down by the extra steps of MFA when they're at work.



Supplement SSO gaps with a password management tool

Not every app can be combined with SSO, so to further reduce the number of passwords that users have to maintain (and therefore reduce the likelihood of password reuse across apps), you should offer a password management tool that generates strong passwords, then encrypts and stores user credentials.

Only
16%

of employees use an SSO solution.⁵

24%

of SMBs say access management is a top security challenge.²

11

is the average number of passwords that small business employees must remember.⁵

2. Put endpoint security in place

The rise of wireless devices has drastically increased the number of endpoints in an organization. In addition to servers and desktops, each employee's laptop, tablet, and smartphone adds another possible vulnerability that can be exploited to give incoming malware access to the corporate network. Simply installing antivirus software is no longer enough due to the proliferation of attack vectors, including email attachments and hyperlinks, web browsing, social media, and apps.

While traditional antivirus solutions simply try to prevent attacks, modern endpoint detection and response (EDR) solutions actively discover and remediate threats across devices, desktops, and servers. Advanced endpoint protection solutions use automation, machine learning, and behavioral monitoring to detect, respond to, and eliminate a diverse range of threat vectors, including executable or fileless malware, document and browser exploits, malicious scripts, and credential scraping. Features to look for include:

- Visibility into endpoints, apps, running processes, and encrypted traffic
- Threat forensics
- Ability to isolate and disconnect infected endpoints from the network
- File recovery and device rollback

68%

of organizations experienced one or more endpoint attacks that successfully compromised their data and IT infrastructure.⁶

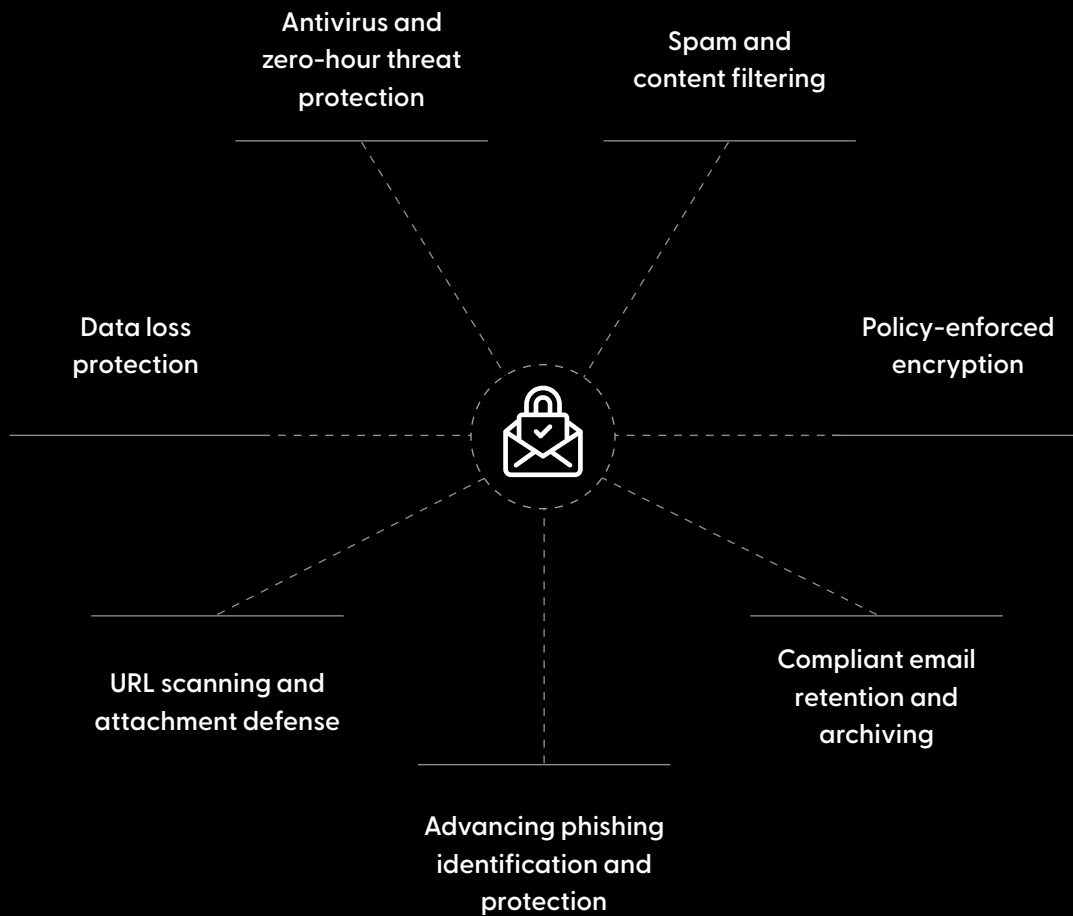
70%

of successful breaches begin on endpoint devices.⁶

8 steps to build a comprehensive security practice

3. Layer on additional email security

Because email is the #1 vulnerability for phishing, ransomware, spam, and malware, it is critical to protect sensitive data from leaving the organization and stop threats before they can enter your network through this method. The native security features of most email solutions, including Microsoft 365, don't offer enough built-in protection to combat today's threats – you should layer on a third-party solution that can provide advanced security features.



8 steps to build a comprehensive security practice

4. Enforce data protection and compliance

34% of SMBs say they use the CIS Framework and **22%** say they use the NIST Framework.²

Protecting a company's most sensitive and proprietary information through data loss prevention and email/file encryption helps avert data breaches and the potential costs of litigation, penalties, fines, and settlements. This is especially essential for organizations that must comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), and Payment Card Industry (PCI) standards.

Millions of healthcare records are wrongly exposed or breached each year due to failed HIPAA compliance. However, despite the massive importance of securing patient data (and the potential impact of settlements and fines due to violations), HIPAA compliance can feel overwhelmingly complex to organizations starting their compliance journey, which is where compliance software can help.

Malicious attacks

are the most common and most expensive root cause of data breaches.

Small businesses

face disproportionately larger data breach costs relative to larger organizations.

8 steps to build a comprehensive security practice

4. Enforce data protection and compliance



Data loss prevention (DLP)

Protect confidential and critical information from being accidentally shared, lost, leaked, or stolen through rule-based monitoring and alerts (e.g., “no number formats that indicate Social Security Numbers are allowed to be sent in outbound emails”).



Email encryption

Encrypt inbound and outbound emails based on policies to ensure that sensitive information can be safely shared inside and outside the organization.



Whole disk encryption

Implement whole disk encryption on every laptop to protect business data in the event of device loss or theft.



App blacklisting and web security

To ensure that business data can't be sent via unmonitored and unprotected channels, you can disallow users from using their personal email or apps such as Dropbox on work devices.



USB device control

In highly secure environments, lock down user USB ports to prevent employees from walking out with sensitive, proprietary, or confidential data on a thumb drive.



HIPAA compliance software

HIPAA compliance solutions provide structured guidance to help organizations achieve and maintain compliance with assessments, training, incident management, business associate management, and breach support staff.

5. Implement network and web security together

It is critical for businesses to fortify connections to protect and control access to their environment's entrances and exits. To secure incoming and outgoing network traffic, network and web security must work hand-in-glove. Network security helps protect network systems and data from unauthorized or malicious access, while web security protects users from accessing malicious websites.

Network security

1. Install a reputable next generation firewall that can provide intrusion prevention and detection, URL filtering, and data loss protection.
2. Disable unnecessary ports to narrow the attack surface and provide cybercriminals with fewer vulnerabilities to exploit. For example, remote desktop protocol (RDP) provides admins with powerful capabilities but also opens up an endpoint to attacks. Restricting access or enforcing proper authentication is critical.
3. Segment a network for guests and even employees' personal devices to keep unauthorized users from accessing resources they shouldn't, as well as creating a defined line of work and personal web surfing habits.

47% of SMBs plan to invest heavily in network security in 2023.²

Web security

1. Whether users are simply web surfing or are tricked into clicking a malicious link in a phishing email, protect users by blocking them from visiting malicious websites.
2. Prevent users from visiting inappropriate websites, such as pornographic, gambling, or gaming sites.
3. Preserve bandwidth consumption by blocking users from streaming services, such as Netflix, that use up precious bandwidth.

27% of SMBs say malicious websites/web ads are a main reason they've had a security issue.²

8 steps to build a comprehensive security practice

6. Begin ongoing end user security training

A company's security posture is only as strong as its least secure employee. And with phishing attempts growing more sophisticated, even savvy users can find themselves accidentally clicking malicious links, opening risky attachments, or mistaking a spoofed URL for a familiar website and offering up sensitive information. Empower end users by engaging them with ongoing security training to teach them how to spot and respond to various types of threats.

Phishing simulation training

Phishing simulation tools are a great way to teach employees to be alert for, identify, and report suspected phishing attempts in their inbox.

Only 35% of businesses conduct phishing simulation training.⁷

Ongoing micro training

As cybercriminals continue to innovate, continual education is important so that users stay up to date on the latest threats. Security awareness training solutions use microcontent and quizzes to build security scores and track progress company-wide.

74% of businesses have formal security training programs.⁷

7. Add mobile security

Prior to the COVID-19 pandemic, many companies were already beginning to embrace remote work and bring-your-own-device (BYOD) policies in support of mobility. The pandemic rapidly accelerated that shift and now, the modern workforce expects the convenience and flexibility to work where they want. However, this means that the network security perimeter is no longer enough to protect company resources. Mobile devices are now one of the most targeted entry points for incoming malware through malicious wireless networks, application vulnerabilities, and lost or stolen devices.

Mobile security solutions help businesses manage and protect mobile smartphones, tablets, laptops, and IoT devices on the corporate network, adding an extra layer of security to mobile endpoints. Features commonly include:

- **Device management** provides device administration, including enrollment, configuration, policy management, BYOD privacy setting management, and remote wipe.
- **Mobile application management** provides the ability to distribute apps to devices, push notifications for needed updates, and prevent users from downloading disreputable apps.
- **Content management** allows users to securely access and share company documents on mobile devices via encryption and authorization.
- **Network access control** enables authorized devices to securely access the corporate network and internal resources.
- **Isolation** separates a user's work apps from their personal apps, so that business data can be wiped if needed without interfering with a user's personal information.

45%

of businesses suffered a compromise involving a mobile device in 2022.⁸

53%

of mobile devices have access to more sensitive data than in 2021.⁸

8 steps to build a comprehensive security practice

8. Create a disaster recovery and response plan

Only **29%** of SMBs say they have a strong disaster recovery policy.²

From malicious threats and user error to physical disasters and hardware failure, there are countless ways for a business to lose valuable data or experience downtime, which can have a huge impact on productivity, lead to mounting IT costs, and damage the company's brand.

Businesses of every size need to plan ahead to know how to respond in case of a data breach, outage, or cyberattack in order to safeguard data and stay operational. This is increasingly important for businesses in compliance-regulated industries, such as healthcare and finance.

An effective backup and disaster recovery plan should:

- Identify the main threats to data and operations, as well as their likelihood
- Define the company's tolerance for downtime and data loss
- Inventory all hardware, software, apps, and data, then prioritize what is critical
- Outline a data restoration and recovery strategy, including service/solution, storage location, and processes, and prioritize what needs to go back online first
- Build processes to re-establish access to critical IT resources, apps, and data
- Establish roles and responsibilities within the action plan
- Create a communication plan for both internal and external communications in the event of downtime
- Institute an employee training and awareness program

It can be eye-opening for Microsoft clients to learn that Microsoft themselves recommend third-party backup solutions.

[The Service Availability section of the Microsoft Services Agreement](#) states:

"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve the content or data that you've stored. We recommend you regularly backup your content and data that you store on the services or store using third-party apps and services."

Your security experts

Putting it all together

The layered security approach outlined in this guide can seem complicated and daunting to an SMB with limited IT resources – especially when the stakes are so high due to the potential cost of damage from a breach. In fact, three out of four SMBs say they don't have sufficient personnel to address IT security.

With SMBs feeling overwhelmed and under-prepared for the increasing volume and variety of cyberattacks, MSPs like you are vitally important to guide your clients towards modern, proactive defensive practices.

And you're not alone either – Pax8 is here to help you identify gaps in your clients' technology stacks and easily deploy the cloud security solutions they need to combat today's advanced cyberthreats.

Other resources

Explore:

NIST Framework

Read:

CIS Controls Guide

Read:

Pax8 Security blog

Explore:

Pax8 Security Hub



Want to discuss security solutions you can offer as additional layers of defense?

Schedule a call

Sources

1. Snyk, The State of Cloud Security Report 2022, 2022
2. Datto, 2022 SMB Cybersecurity Report for MSPs, 2023
3. IBM and Ponemon Institute, 2022 Cost of a Data Breach Report, 2022
4. Microsoft, 2023 Identity Security Trends and Solutions from Microsoft, 2023
5. Specops Software, The 2022 Weak Password Report, 2022
6. PurpleSec, Cyber Security Stats for 2023, 2023
7. Proofpoint, 2023 State of the Phish Report, 2023
8. Verizon, 2022 Mobile Security Index, 2022