Layered Cybersecurity: A Comprehensive Guide for Effective Defense

Protecting your organization from cyber threats can seem overwhelming. It is often confusing to know where to start and how to make incremental improvements. Providing answers to senior management, customers, and auditors regarding the organization's security profile and priorities frequently challenges even seasoned security professionals.

Poor security can be devastating to any organization, but small and medium-size businesses can be particularly hard hit. IBM estimates the average cost of a data breach in 2023 was $4.45 million, up 15% over 3 years. The effects of a breach can include lost revenue from operational downtime, expansive fees for remediation, escalating cyber insurance premiums, reputational damage that can last for years, and even bankruptcy.

Managing a cybersecurity program is particularly hard in small and midsize organizations increasingly targeted by hackers. The 2023 DBIR reported that organizations with fewer than 1,000 employees experienced over 67 percent more breaches than those with more than 1,000 employees (381 v. 227). These organizations have the same legal and regulatory responsibilities of larger companies, but usually without the resources to adequately staff a security team or purchase costly solutions.

We designed this ebook to help individuals and teams understand, plan, and prioritize their security goals. Whether you are starting a new cybersecurity program or working to mature an existing one, you can use this resource to steer your program. The ebook will help you ask the right questions of your organization and vendors to ensure you are maximizing your security spend.

Please note: While we always recommend that organizations start with a cybersecurity assessment, every organization is unique with different priorities, capabilities, and risk profiles. Focus on the security activities below in an order that fits your needs, budgets, and skills.

Where to Start

Unfortunately, there is no such thing as a perfectly prescribed program, or a silver bullet to cybersecurity (despite what some vendors may tell you). Just like one's health, achieving a good cybersecurity posture is an ongoing process. The program will vary a bit between organizations based on their employee count, IT infrastructure, regulatory demands, resources, and skill sets. At a high level, securing your organization requires understanding where weaknesses exist and applying multiple layers of defense, with each layer supporting the others. This ebook summarizes those activities into three layers:

LAYER

Assessments & Testing

Identify existing weaknesses and vulnerabilities and prioritize remediation actions.

LAYER

Detection & Response

Monitor your environment for attempts by cybercriminals to penetrate your networks and applications. Take action to minimize the impact of those attacks.

LAYER

Policies & Training

Educate your team to identify and defend against cyber-threats. Establish expectations for how employees should handle data and organizational resources.

Let's drill down on each layer.

Security Layers

Assessments & Testing

Most organizations have some level of security implemented, usually starting with antivirus solutions on endpoints (computers, servers, mobile devices) and network firewalls. However, before you start buying and deploying additional solutions, there are fundamental activities that should occur, including an overarching review of all aspects of your cybersecurity posture obtained through a thorough cybersecurity assessment.

Cybersecurity Assessments

Identify the Unknowns

Recommended Frequency

At least semi-annually. Remember to reassess when you make major changes to the network, environment, and/or IT infrastructure.

Peter Drucker, the legendary management consultant and so-called "father of modern management", famously said, "You can't improve what you don't measure." The same is true in cybersecurity. Most organizations starting a security program lack an understanding of their weaknesses, as well as their strengths. A cybersecurity assessment identifies these unknown weaknesses and provides you with a baseline against which you can measure progress.

Most cybersecurity risk assessments will follow a questionnaire process based on a standardized checklist of controls. You can choose one of the international standards, such as the NIST Cybersecurity Framework, Center for Internet Security (CIS) Critical Security Controls, or ISO 27001. You may also have regulatory, compliance, and/or insurance requirements your customers, partners, or vendors demand you follow. You can perform a cybersecurity risk assessment on your own or hire an outside company to conduct one for you. The result should be a report that outlines your organization's strengths and weaknesses.

A good assessment report should also include prioritization and remediation steps that provide guidance on how to begin resolving weaknesses. Providing a transparent scoring system and an overall score or grade provides a measurable baseline. For example, if your initial score is a "C", you can identify steps and focus areas to move to achieve a "B" or better. In short, your baseline allows you to know where you stand and identify where to begin, where to first allocate budget, and which activities can provide the biggest impact.

The Benefits of a Cybersecurity Risk Assessment

- Identify & prioritize areas for improvement
- Meet requirements, faster
- Align to key frameworks

Vulnerability Scanning

Practice Ongoing Hygiene

Recommended Frequency

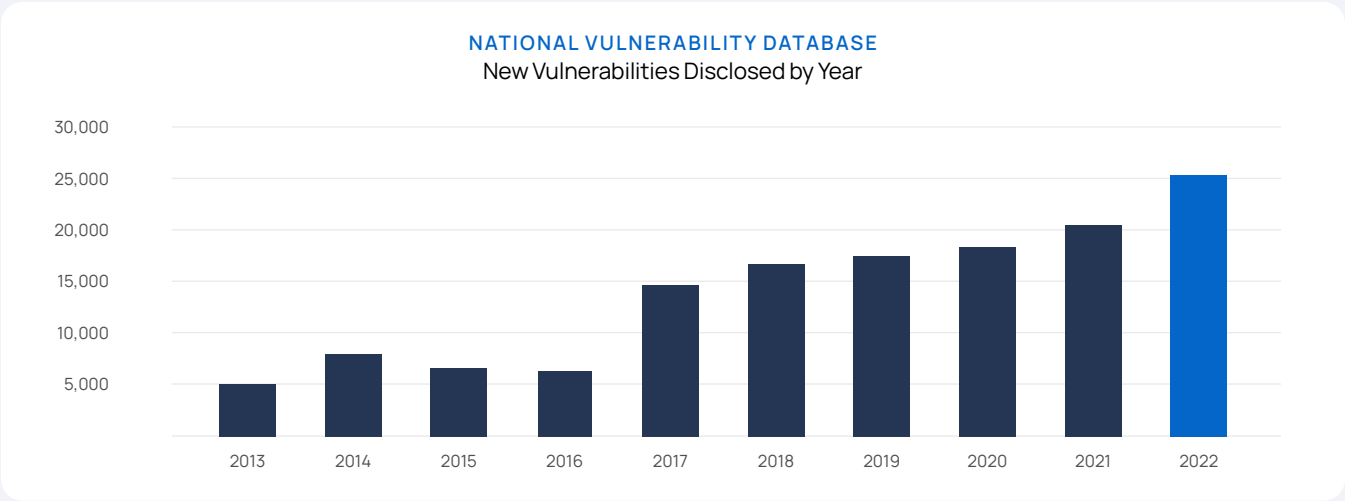
Vulnerability testing is recommended as an always-on solution with a minimum cadence of monthly reporting.

IT security is ephemeral. Yesterday's secure environment can present high risk today if vendors or researchers disclose new vulnerabilities in the hardware and software you run. These vulnerabilities might exist on your computers, printers, security cameras, or software applications used by your teams.

Keeping abreast of these is good cybersecurity hygiene. Unfortunately, researchers and vendors identify and disclose new issues every day. As shown in the graph, NIST's National Vulnerability Database tracks thousands every year. Each time a new vulnerability is disclosed, a race begins between hackers and defenders.

A good vulnerability management program will include the use of a vulnerability scanner. You can run these yourself or have a vendor perform this task on your behalf. These tools scan internal and external networks actively hunting for security vulnerabilities on websites, web and mobile applications, and devices like routers, servers, and switches. Once detected, you can prioritize remediation based on severity (tools will often group findings for you).

There may be many issues to resolve, particularly when you first start, and you may not be able to remediate them all quickly. Don't be discouraged. This is common, especially for organizations with larger teams and IT infrastructure. Start with the critical issues first, then move through high, medium, and ultimately lower severity level issues. If you are working with a security partner, they should provide remediation recommendations and can often suggest compensating controls to mitigate risks while you work your way through the list.



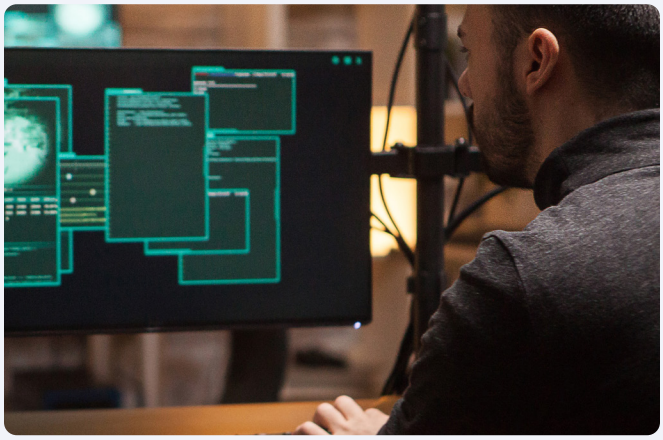
Penetration Testing

Think Like a Hacker

Recommended Frequency

Semi-annually is a best practice, but at least annually. It's also important to consider retesting after making major changes to the network, environment, and/or IT infrastructure.

While an assessment will help you determine what you should be doing, and a vulnerability scan will help identify unpatched systems, one of the best ways to understand if you have adequate controls is to "think like a hacker." This means attempting to find and exploit security weaknesses using the same tactics and techniques as a criminal would.



In security, this involves employing "white hat" or "ethical" hackers to attempt to penetrate your systems. A "pen test" is an approved, standardized, and non-destructive test of your defenses. The findings will vary based on the time allowed for the testing and the skills of the ethical hacker. In other words, ask an ethical hacker to try and get to the crown jewels, then report back on how far they got (and how they did it) so you can focus on closing those gaps.

The first step with penetration testing is scoping the work. Since some organizations have never done one before, it often starts with an external network test. An external penetration test is an "outside-in" view of your network intended to identify any exploitable points of entry. A more advanced pen test can focus inside the network to explore what assets an attacker can reach. For example, if the pen tester can reach file systems and elevate their privileges to write to those systems, that would indicate vulnerability to a ransomware attack.

A pen test starts by providing your IP address. The ethical hackers use commercial and proprietary tools and techniques in an attempt to penetrate your systems. A pen test goes well beyond what you might see with automated vulnerability scanning. The result is a professionally prepared report demonstrating what a malicious hacker could accomplish, supported by prioritized findings, risk ratings, and remediation recommendations.

Website Scanning

Keep Your House in Order

Recommended Frequency

Ongoing, monthly at minimum.

An often-overlooked weakness in an organization's cybersecurity posture can be its public facing marketing websites and web applications. Both of which are often maintained and updated outside of IT's control.

Configuration issues, surface vulnerabilities, scripting attacks, and planted malware can lead to infections for site visitors and users, deface your brand, image, or products, damage your organization's reputation, or even result in your website or application being blacklisted by the likes of Google and other leading search engines and ISPs.

Automatic website scans look for potential threats on your public facing website(s) and web applications including, compromised hosting and IP information, spam and injected malware, outdated software or vulnerable plug-ins and extensions, server errors, blacklist status, and more. Reports provide risk scoring, vulnerabilities found, and recommendations for improvement.

Potential Website Threats

Compromised hosting	Server errors
Compromised IP information	Blacklist status
Spam & injected malware	Vulnerable plug-ins & extensions
Outdated software	and more...

Compromised Credential Monitoring

Scan the Dark Web

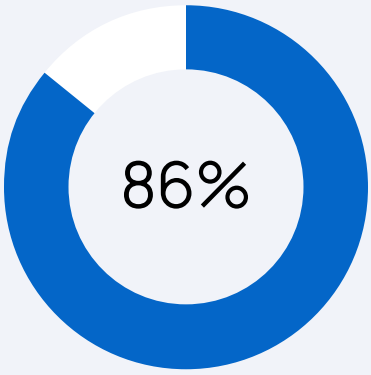
Recommended Frequency

Ongoing, monthly at minimum.

An organization is only as secure as its weakest link. Often, that is a user error that results in a stolen password. Unfortunately, it is not just your internal passwords you need to worry about; a 2021 study found that 70 percent of people reuse passwords across personal and business sites.

Stolen credentials can provide criminals substantial financial incentive and, according to the 2023 Verizon Data Breach Investigations Report, are used in 86 percent of attacks on web applications. They sell them on the dark web to buyers who then use them for "account takeovers": simply logging into an organization's systems rather than hacking applications and networks to steal data, spread malware, or conduct fraud. Remember, since one user's passwords might open many website doors (such as your financial system or your document storage solution), these passwords can have a significant value in the criminal marketplace.

Monitoring for stolen credentials gives you the ability to identify any compromised employee passwords available on the clear, deep, and dark web. Once found, it is critical that users immediately change their password on all accounts.



Use of Stolen Credentials

9%
Exploit Vulnerability

8%
Brute Force

6%
Other

Security Layers

Detection & Response

No organization is immune to cyberattacks. This makes it critically important to employ proactive measures to find, stop, and eliminate attacks as they occur before attackers can steal confidential information and damage your data and networks. The best approach is to monitor systems to identify activities used during the “reconnaissance” phase of an attack, when criminals are familiarizing themselves with your systems and regular IT activities. If you assume an attacker will inevitably be successful (and you should), you also need a plan for responding to those attacks. Finally, teams require a mechanism for staying alert to emerging threats and containing them as quickly as possible.

Managed Detection & Response

Detect and Block Attacks

Recommended Frequency

24/7/365. Include regularly scheduled reviews to gauge and improve cyber hygiene.

Hackers work around the clock, so defenders need to match those hours. Staffing an inhouse Security Operations Center (SOC) 24/7/365 is not financially feasible for many organizations. Enter Managed Detection and Response (MDR), an outsourced service that actively collects and correlates data from traditionally siloed systems (endpoints, mobile devices, network, perimeter, cloud, and applications) and analyzes the signals for malicious activity. MDR providers offer trained security experts to monitor your systems and alert you to potential attacks. These cyber specialists monitor for reconnaissance activity such as failed login attempts, port scans, and "indicators of compromise" (e.g., malware signatures and unusual network requests). Their services can range from anomaly detection and communicating simple alerts to remediation guidance and real time mitigation (i.e., stop an attack as it's happening).

When looking at service providers, make sure they can cover all your assets, including endpoints (computers, services, mobile devices, networks) and email and other cloud applications. Some service providers limit their coverage solely to endpoint-based cybersecurity with varying response levels or may only provide an alert or recommendations for remediation and not contain a breach or act on your organization's behalf. Others can actively identify and contain developing attacks in real-time and provide guidance and recommendations to improve your security posture.

Choose a provider and service level that addresses your security needs and budget. And when thinking about budget, while MDR can seem expensive, remember to consider ROI. Building your own SOC can cost millions, as can falling victim to a significant cyberattack such as ransomware or a data breach.

Incident Response Plan

Be Prepared for Attacks

Recommended Frequency

Review and update at least annually and always when there are infrastructure/system changes or key personnel changes to anyone enlisted in the plan.

Successful attacks are rampant, whether it is through stolen credentials, unpatched vulnerabilities, or user error. Proactive organizations prepare for this reality with incident response plans. An incident response plan is a structured approach that organizations use to manage and respond effectively to cybersecurity incidents. Having a vetted plan ready to go can save significant time, effort, and money.

Your plan should indicate how to handle incidents like a breach of sensitive data, ransomware, and even a lost company computer. It should also include procedures for promptly assessing and triaging incidents to determine their severity, scope, and potential impact. Ensure your incident response plan contains a clear, step-by-step approach to rectifying the situation, detailing who will conduct specific tasks as needed. That means defining names, roles, and responsibilities so you can act quickly and effectively in the event of an incident. It's helpful to also consider regulatory and legal requirements, such as data breach notification laws, industry-specific regulations, and contractual obligations.

Remember to review the plan as a team to ensure everyone knows their roles and responsibilities in the unfortunate case of a cyber incident.

Your plan should

- Indicate how to handle incidents like a breach of sensitive data, ransomware, and even a lost company computer.
- Include procedures for promptly assessing and triaging incidents to determine their severity, scope, and potential impact.
- Contain a clear, step-by-step approach to rectifying the situation.

Cybersecurity Threat Alerts

Stay Aware

Recommended Frequency

Ongoing, with frequent updates for relevant alerts.

Maintaining awareness of new and evolving threats, recent breaches, and a rapidly changing cybersecurity landscape is important. However, there are hundreds of sources that publish breach announcements, emerging threats, and new vulnerability warnings every day. Busy IT professionals have many responsibilities and cannot make this a full-time job.

A curated security feed makes it possible to maintain awareness without overwhelming teams with noise. Look for a vendor that provides strategically selected content. This will save you time by consolidating information and presenting only relevant and meaningful cybersecurity stories, news, alerts, and events.

Security Layers

Policies & Training

While lacking the glamour of blocking an attack or implementing new solutions, documented policies and frequent training are a critical part of any cybersecurity program. Unsafe user practices are often the weak link in a cybersecurity program. According to one report, human errors account for 95 percent of cybersecurity incidents. Policy and training activities ensure that users understand how they can help improve the organization's cybersecurity hygiene – including password management, authorized application and device use, and using organizational assets appropriately. Making sure these policies comply with legal and regulatory requirements demands expertise.

Technology Acceptable Use Policy

Practice Good Cybersecurity Hygiene

Recommended Frequency

Review, update, and train users at least annually and remember to train every new employee who joins the team.

A Technology Acceptable Use Policy is a set of guidelines and rules that outline the acceptable and unacceptable uses of an organization's systems and resources. This policy should explain in detail to the employee how they may use company devices, passwords, and technology, including best practices such as how to store and share files. This can extend to include treatment of personal devices on company networks, also known as BYOD ("Bring Your Own Device").

It is important that your policy uses simple and clear terms so everyone can easily understand and follow expectations. Once developed, every employee should receive training on the policies and acknowledge in writing their understanding and acceptance.

Deliver Tailored Cybersecurity Policies

- Set expectations with a clear and strong baseline for how technology and data should be used and protected, remotely or in-office.
- Mitigate insider threats and reduce the change of human error by communicating and training on cybersecurity best practices.
- Prepare for compliance with documents that support legal, industry, HR, and other regulatory requirements.

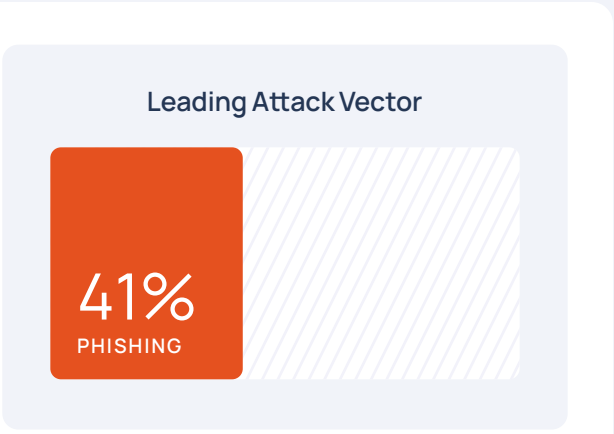
Phishing Simulations

Replicate Attacks

Recommended Frequency

Ongoing. Monthly is a best practice.

Phishing emails are an easy, effective method for hackers to trick unsuspecting recipients into clicking links, opening files, and other activities that allow the hacker to steal credentials or commit financial fraud. Email filters cannot stop all malicious emails. According to the 2023 IBM X-Force Threat Intelligence Index, phishing is the leading attack vector, used in 41 percent of incidents to gain initial access.



Phishing emails are increasingly sophisticated with files or malicious links built into them. Others leverage pretexting. In a pretexting attack, the hacker gathers information, fabricates stories, and leverages social engineering to impersonate the company CEO or other executive, then ask an employee to send a file, purchase something quickly, or pay an invoice, for example.

With the average employee receiving hundreds of emails each day, defending against phishing emails is difficult. Training your employees to identify email-based attacks is an essential preventative measure that everyone must undertake. Phishing simulation tools enable you to send carefully crafted phishing emails to your employees and observe their actions. Do they click the email links? Do they mark them as junk or report the emails to IT?

Phishing simulations mimic real attacks without damaging the organization. Email messages are designed and distributed to attempt to trick users into revealing sensitive information or taking actions that may compromise their security, such as clicking on a malicious link, entering credentials on a fake website, or downloading a malicious attachment. Good solutions include automated options to simplify deployments and track performance, including reminders and built-in reporting.

After the simulation, the organization provides feedback and training to the targets who fell for the phishing attempt. This may include explanations of what they did wrong, the risks and consequences of falling for phishing attacks, and best practices for identifying and responding to phishing attempts.

Cybersecurity Awareness Training

Build a Security Culture

Recommended Frequency

Ongoing, awareness training at least annually and anytime a new team member joins your organization. Video reinforcement continuously.

Cybersecurity awareness training covers the ABCs of security. It helps technical and non-technical employees understand basic principles of protecting themselves and the organization against cyberattacks.

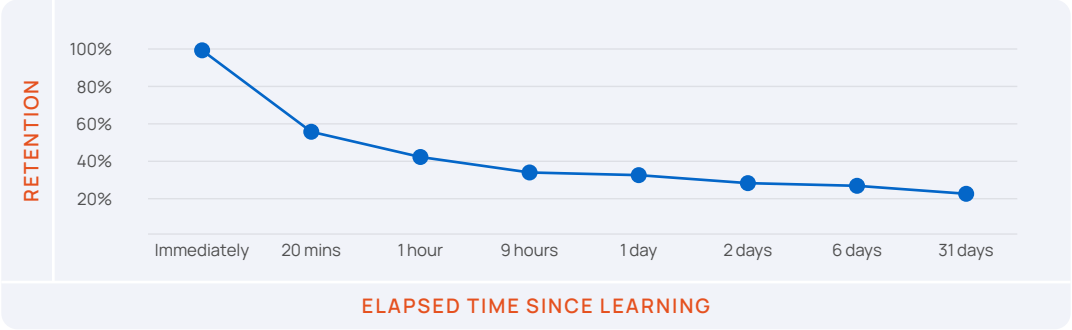
Many companies make cybersecurity training an annual requirement. While a step in the right direction, it is important to remember that learning is a process, not an event. This includes cybersecurity awareness. When training sessions are events only held once or twice each year to meet compliance requirements, students do not retain knowledge. A study represented by the famous Ebbinghaus Forgetting Curve showed that students forget over 75% of a lesson in the first week alone.

Teams can reduce knowledge loss with regular reinforcement of the lessons. These reinforcements need not include all the information from the lesson. The goal is to keep the learner thinking about the material and putting it to practical use. That's why markets like the construction industry do regular "toolbox safety talks" throughout the year to keep safety top of mind. You can follow a similar cadence for your cyber training.

Short and timely cybersecurity topical training videos are a good way to reinforce more formal training. Our advice is to keep lessons frequent, relevant, and brief. Nobody wants to sit through hour-long training sessions every month. But they might be ok with smaller doses of timely education. Include quizzes to confirm knowledge transfer and track students' scores for internal and regulatory compliance purposes.

Training posters and graphics can help keep security awareness top-of-mind on a daily basis. These should be memorable and include digital formats that can be shared with remote employees and through messaging channels like Slack. Don't be afraid to employ humor as part of the campaign.

Ebbinghaus Forgetting Curve



Rewards & Recognition

Tie it All Together

Recommended Frequency

This one is up to you; be sure to tie it back to the cadence of your other activities.

Embracing security takes effort. Senior leadership support is critical, making certain to all users why the programs are in place, how they help improve cybersecurity, and what it means to protect an organization from the potentially irreparable damage of a cyber incident.

Recognizing those efforts is helpful. Have some fun with your program. More and more organizations now implement recognition programs. For example, employees who pass phishing simulation testing and complete their monthly video training can win gift cards, prizes, or security "swag." Other organizations maintain a scoreboard to build friendly departmental competition. Gamification, rewards, and recognition are small steps that can help your program create a buzz and support a better, more approachable security culture.

Ways to Recognize Employee Efforts

- Win gift card(s)
- Win prizes
- Win security "swag"
- Office scoreboard(s)
- Gamification
- and more...

How to Get Started

Building a strong cybersecurity posture requires time (including across the whole team), budget, and other resources. That's why it's key to have all relevant stakeholders aligned and on board before rolling out your cybersecurity program.

Here are some tips for gaining buy-in from executive leadership and other stakeholders:

Number One

Clearly articulate the benefits of the security program to stakeholders.

Highlight how it will protect the organization from potential threats, mitigate risks, safeguard sensitive data, and contribute to regulatory compliance. Examples of the types of risks and potential damages can go a long way in helping others to prioritize the need.

Number Two

Understand the concerns and priorities of different stakeholders.

Involve them early in the process to gain their input and address any concerns or objections.

Number Three

Demonstrate success through pilot projects.

An external assessment with a limited scope can demonstrate weaknesses that require mitigation and provide a roadmap for incremental improvements. A quick scan showing vulnerabilities on a network, issues with a website, or compromised employee credentials can make things more real.

Number Four

Look for a security partner that has worked with organizations like yours.

...especially if, like most small and midsize organizations, you have limited internal security resources. A good partner will provide a breadth of products and services to help you reduce vendor sprawl, take a collaborative approach, and help you become stronger and more self-sufficient over time.

We hope this guide provides you with some helpful advice on starting or advancing your cybersecurity program and posture.

You do not need a large team to get started and making iterative progress need not be overwhelming. Understanding where risk exists through assessments, scanning, and testing can provide a roadmap for incremental improvements. Bringing in a trusted partner to deploy and manage detection and response capabilities provides enhanced, continuous security without adding internal headcount. Creating policies and training everyone from the intern to the CEO creates a "human firewall" against cyberattacks.

We are here to help. Defendify provides an award-winning All-In-One Cybersecurity® solution that streamlines and consolidates tools across assessment, testing, policies, training, detection, and response. Defendify delivers multiple layers of protection across the core pillars of cybersecurity: people, process, and technology, backed by industry leading cybersecurity support and expertise—you're never in this alone.

Defendify All-In-One Cybersecurity®

Get Started

Take your next step toward comprehensive cybersecurity.