LAYERED SECURITY STRATEGY

PROTECTION PROVIDING PEACE OF MIND

TABLE OF CONTENTS

Mirazon

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

We can offer pounds of cure too, if you need it.

Cybersecurity strategies for your business are very similar to the security measures you take for your home. With each additional layer comes more protection - and peace of mind.

Information security has never been more critical to organizations of all sizes. Bad actors are constantly attacking networks, preying on unsuspecting end users or trying to infect your systems with ransomware.

Through years of experience in configuring network security systems and remediating nasty malware attacks, Mirazon has honed a robust Layered Security Strategy for both preventing and mitigating cybersecurity breaches.

LAYERED SECURITY STRATEGY

DNS FILTERING

ASSESSMENTS & MONITORING

END USER TRAINING

MFA

EMAIL SECURITY

NEXT-GENERATION FIREWALL

ENDPOINT PROTECTION

Cybersecurity threats are ever-evolving. The only way to combat this is with the mindset of assuming it's a case of WHEN and not if -- how do you limit the scale of an attack?

With Mirazon's Layered Security Strategy, you will be able to identify, stop, and minimize cyberattacks.

LAYER 1

ENDPOINT PROTECTION

THE LOCKS AND DEADBOLTS TO YOUR BUSINESS

ENDPOINT PROTECTION
The locks and deadbolts to your business

Just like the locks/deadbolts on the doors and windows of your house, endpoint protection is the foundation for a secure environment - and is often taken for granted.

Endpoint protection refers to the measures and security solutions implemented to secure the endpoints, such as smartphones, laptops, desktops, or servers, within a network. It involves safeguarding these endpoints against malicious attacks, unauthorized access, and data breaches.

Endpoint protection consists of various security measures, including antivirus and antimalware software, firewalls, intrusion prevention systems (IPS), and data encryption. These measures aim to detect, prevent, and respond to potential threats that could compromise the integrity, confidentiality, and availability of the endpoint and network.

It plays a crucial role in ensuring the overall security posture of an organization and is an essential component of a comprehensive cybersecurity strategy.

LAYER 2

NEXT-GENERATION FIREWALL

THE SMOKE ALARMS TO YOUR BUSINESS

NEXT-GENERATION FIREWALL

The smoke alarms to your business

Similar to the way smoke alarms detects danger, a next-generation firewall (NGFW) protects your business through detecting and blocking not only malicious network packets, but also potentially harmful applications or protocols. By leveraging deep packet inspection, NGFWs can scrutinize the content of network traffic, allowing organizations to implement more granular security policies.

NGFWs also incorporate additional security functionalities such as intrusion prevention systems (IPS), antivirus, and advanced threat protection (ATP). These features help organizations defend against a wide range of threats, including malware, viruses, and zero-day attacks.

Another key aspect of NGFWs is their support for threat intelligence feeds and integration with security information and event management (SIEM) systems. By leveraging these capabilities, organizations can stay updated with the latest threat intelligence, receive alerts, and take automated remedial actions when potential security incidents occur.

Furthermore, NGFWs provide advanced visibility and control over network traffic, allowing organizations to set up policies based on specific criteria such as application, user, or device. This helps to enforce security across the entire network and implement a zero-trust approach to network security.

In conclusion, next-generation firewalls offer a comprehensive and proactive approach to network security, combining traditional firewall functionalities with advanced threat prevention capabilities. These solutions are designed to address the security challenges posed by the increasing sophistication of cyber threats, safeguarding organizations' critical assets, and ensuring a secure and resilient network infrastructure.

After all, you don't want to live somewhere that can't alert you of a fire. The same should go for your business - because where there's smoke, there's fire.

LAYER 3

EMAIL SECURITY

THE FLOODLIGHTS TO YOUR BUSINESS

EMAIL SECURITY
The floodlights to your business

Proper email security should act like the floodlights to your home - catching bad actors before they have a chance to breach the systems. It's a crucial aspect of ensuring the confidentiality, integrity, and availability of emails and the information they contain.

Email security involves implementing various measures and protocols to protect against unauthorized access, interception, and manipulation of email communications. By employing encryption, authentication, and anti-malware techniques, it aims to safeguard sensitive data from being compromised.

But you should go beyond only using the tools included with your email provider, and implement additional security software, such as Proofpoint, to stay ahead of the ever-evolving threats plaguing today's digital world. These additional protocols quarantine suspicious messages, and help protect your business, employees, and IT infrastructure.
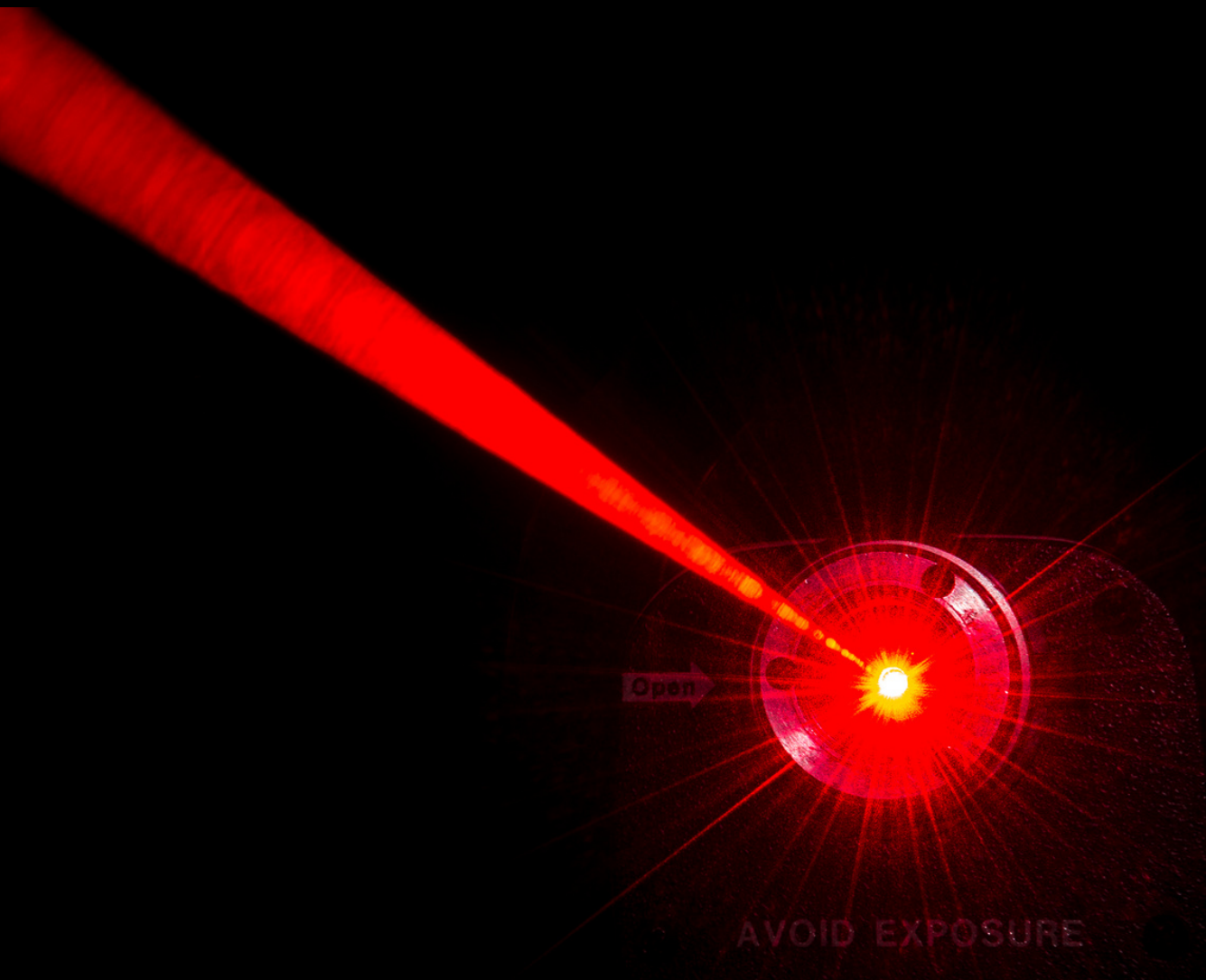
Because email is STILL the biggest delivery method for malware, as well as the most prevalent vector for fraud and scams, this layer of Mirazon's Layered Security Strategy is critically important in maintaining a good security posture.
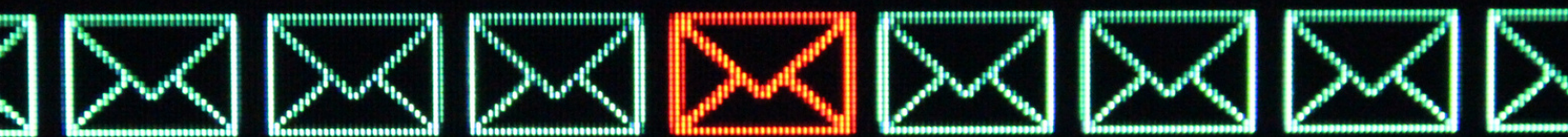
LAYER 4

MULTI-FACTOR AUTHENTICATION

THE MOTION SENSORS TO YOUR BUSINESS

MULTI-FACTOR AUTHENTICATION
The motion sensors to your business

Just like motion sensors alert you of movement outside of your home, multi-factor authentication (MFA) alerts you of suspicious activity regarding accounts, passwords, and attempted breaches.

MFA adds an extra layer of protection to your online accounts and requires users to provide multiple factors of identity verification to gain access to their accounts - typically something they know (such as a password), something they have (such as a one-time password from a mobile device or a physical token), or something they are (such as a fingerprint or facial recognition).

By combining these different factors, MFA significantly enhances the security of user and business accounts and helps prevent unauthorized access - because even if one factor is compromised, the attacker would still need the additional factor(s) to gain entry.

However, there is a new phenomenon referred to as "MFA fatigue," which is when users get used to the verification process and develop habits of clicking "accept" without actually paying attention to what's being asked. Because of this, it's important to stay on top of employee cybersecurity education... Which leads us to the next layer involving end-user training.

LAYER 5

END-USER TRAINING

THE GLASS-BREAK SENSORS TO YOUR BUSINESS
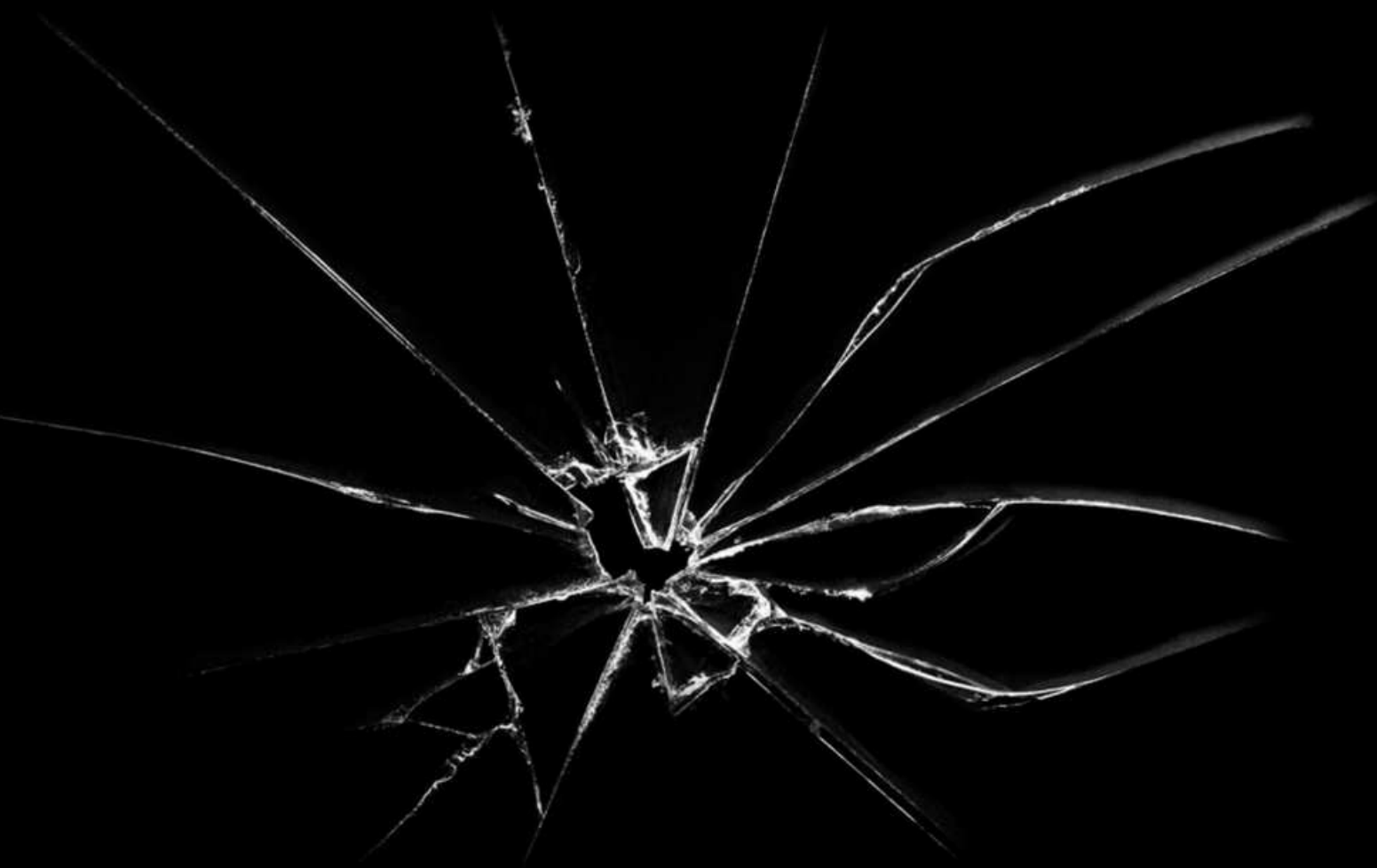
# END-USER TRAINING
The glass-break sensors to your business

Glass-break sensors alert you of an intruder in your home, and end-user training does the same thing. Cybersecurity Awareness Training allows you to see if an employee is capable of overlooking warning signs and clicking malicious links or files - and helps you see where proper education is needed to maintain a secure environment, which is more important now than ever.

Technology alone cannot protect your business from everything. Attackers go where security is at its weakest – and that weak link is your employees.
Your staff are the first line of defense against cybersecurity threats – not the last. It is crucial to educate employees on the existing threats they will be exposed to, how to recognize those threats, what to do if they encounter one, and best practices to mitigate threats and potential risks.

Cybersecurity Awareness Training is the best way to ensure that employees are aware of the threats they face in their jobs and personal lives. Mirazon is here to provide the customized, hands-on training your business needs to maintain a high level of security. Using a platform called Proofpoint, we will provide the knowledge, resources, and training materials to protect your people, data, company, and reputation against cyber threats.

Training should include the following elements:

Evaluate - Knowing what is/is not being implemented is critical to creating a customized training program specific to your employees and business model.
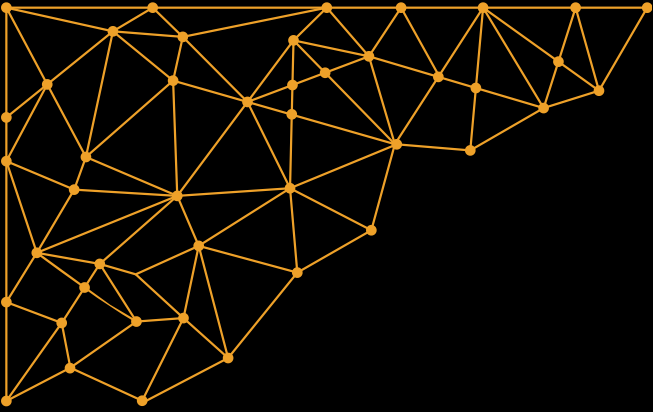
Train - Through our engaging content, we will educate your employees using personalized, evolving, interactive modules that can be taken anytime and anywhere, and can be altered for different departments and the types of threats each could become exposed to.

Test - This includes simulation attacks sent to your employees that attempt to bait them into a falling for fake cybersecurity attack. The content changes and is relevant to what employees may legitimately be exposed to.

Report - We will provide you with reports that contain analyzed results showing exactly how each employee interacted with the training assignments, simulations/simulated attacks, and assessments. These reports are detailed and easy to read, allowing you to evaluate progress and identify what areas need improvement or which employees need specialized attention.

Repeat - Our targeting training is a continuous cycle that will evolve with your business, employees, and existing threats. This is not a "one and done" approach, and we will continue to educate your employees on areas where it's needed most. Using the phishing test results, we will design and adapt recurring trainings to keep security on the top of everyone's minds, making the front-line of your business very strong.

Our Cybersecurity Awareness Training services teaches practical skills through a variety of course topics and security tools that include phishing campaigns, social engineering, emerging threats, and more – all at your own pace. The weakest link in the cybersecurity chain will always be the human aspect, and educating your employees about the importance of cybersecurity will help you create a culture of security and compliance.

LAYER 6

ASSESSMENTS & MONITORING

THE SECURITY CAMERAS TO YOUR BUSINESS

ASSESSMENTS & MONITORING
The security cameras to your business

The security cameras around your home help to keep you informed of what's happening inside and outside your perimeter - which is exactly what assessments and monitoring do for your business.

IT assessments are a systematic analysis of an organization's IT infrastructure, including its hardware, software, network, systems, and applications. It helps to identify the strengths and weaknesses of the organization's IT environment and suggests areas that need improvement.

The results can be used to improve the performance of your organization by identifying what is working well and what needs improving. This information can help you to make strategic IT decisions that improve your productivity and ensure the security of your data. Mirazon offers the following IT assessments:

- Backup Security Assessment
- Active Directory Assessment
- Office 365 Assessment
- Firewall Assessment
- IT Health Assessment

Monitoring and reporting systems provide real-time visibility into the performance of your network infrastructure, applications, and endpoints. The goal of an IT monitoring system is to provide information about trends over time so that you can identify any unusual activity or potential problems before they become serious issues.

IT assessments and monitoring services are the most important parts of an IT service management system. They help companies keep track of how their IT infrastructure is performing, and make sure that the company's technology is functioning as expected - giving your business the competitive advantage it's been looking for.

LAYER 7

DNS
FILTERING

24/7 SECURITY MONITORING FOR YOUR BUSINESS

DNS FILTERING

24/7 Security monitoring for your business

DNS Filtering is similar to a 24/7 professional monitoring service for your home. After all, you can't be everywhere all of the time making sure your employees aren't access harmful sites or clicking on malicious links. DNS filtering does that for you.

It's one of the most important security protocols that you can use to protect your network, and it's one of the first things you'll want to enable on any new router. DNS stands for Domain Name System, and it's responsible for translating domain names into IP addresses. This is important because it allows users to access websites without having to remember the IP addresses—they just type in the domain name instead.

So what does this have to do with protecting your network?

Well, if a hacker wants to break into your network and steal data or take control of your devices, they might try to do it by sending some kind of malware through a link or attachment. You can protect yourself from these threats by blocking them at the DNS level—by blocking their access to your network altogether before they get anywhere near any of your devices.

This way, even if a hacker does manage to break through all other layers of security on one machine (which is unlikely), they won't be able to do anything since there will be no way for them to reach that machine in the first place.

The way it works is that instead of going directly to the website's IP address, your computer sends its request through an intermediate device called a proxy server that checks whether or not it should be allowed. The proxy server then sends back either an unencrypted message saying "yes" or one saying "no." If it says no, then your computer won't be able to access anything on that site.

DNS filtering is frequently overlooked, and it shouldn't be. By filtering malicious domains and securing your public DNS, you can play key role in the fight against cybersecurity attacks.

CONCLUSION

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

Each element of our Layered Security Strategy has a distinctive purpose in helping you maintain a secure business and IT infrastructure, and are meant to used in tandem.

The seven layers intertwine with one another, providing a robust cybersecurity initiative.

After all, just because you have security cameras doesn't mean you shouldn't have locks and deadbolts on your house. The same goes for your business's cybersecurity strategy.

Have questions? We can help. Contact us using the information below!

1640 Lyndon Farm Court, Suite 102
Louisville, KY 40223

www.mirazon.com

(502) 240-0404

info@mirazon.com