# WHAT ALL SMALL BUSINESS OWNERS NEED TO KNOW ABOUT CYBERSECURITY

UNDERSTANDING MODERN THREAT PROTECTION

Salvus TG

# THE PROBLEM

Small businesses are adopting new workflows, policies, and procedures to remain productive and competitive in their spaces. With this rapid transformation comes an increase in **cybersecurity risks**. These new attack vectors can render traditional solutions such as antivirus and firewalls powerless against these modern threats.

**Over 60% of cyberattacks are aimed at small business** and that number is predicted to steadily increase. Laptops, desktops, mobile devices and the employees using them inside & outside of the office are all major vulnerabilities.

These changes in how we work have shifted a focus to the development of enhanced security concepts and tools designed to protect the small business sector.

# THE SOLUTION

Small businesses must begin combining modern security tools with ongoing cybersecurity training and testing of their employees. By focusing on the two largest risks factors, **employees** and **endpoints**, you will improve your organization's overall cybersecurity posture and culture and limit the risk of a breach.

# Upgrade Your Antivirus:

**ENDPOINT DETECTION AND RESPONSE**

It all starts with securing your endpoints. Laptops, desktops, servers and other devices must be secured in and out of the office.

An **Endpoint Detection & Response Protection Platform,** or EDR, unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

TO PUT IT SIMPLY, THINK OF EDR AS A MUCH BETTER ANTIVIRUS.

EDR is designed to actively detect and respond to intelligent and advanced cyberattacks. These solutions are capable of detecting patterns and can recognize suspicious activity on a workstation or server. An EDR solution understands how cyberattacks behave, and can mitigate threats before they have the chance to do damage, protecting your data and assets.

# Strengthen Your Staff:

**SECURITY AWARENESS TRAINING**

One of the most effective ways to strengthen your cybersecurity posture is by eliminating as much **Human Error** as possible.

Studies have shown that human error could account for 90% of all data breaches. A number that has consistently risen over the last 3 years. Today, your employees are constantly exposed to sophisticated phishing and social engineering attacks. In order to prevent these attacks from becoming breaches, your employees must know how to spot and how to respond to these threats.

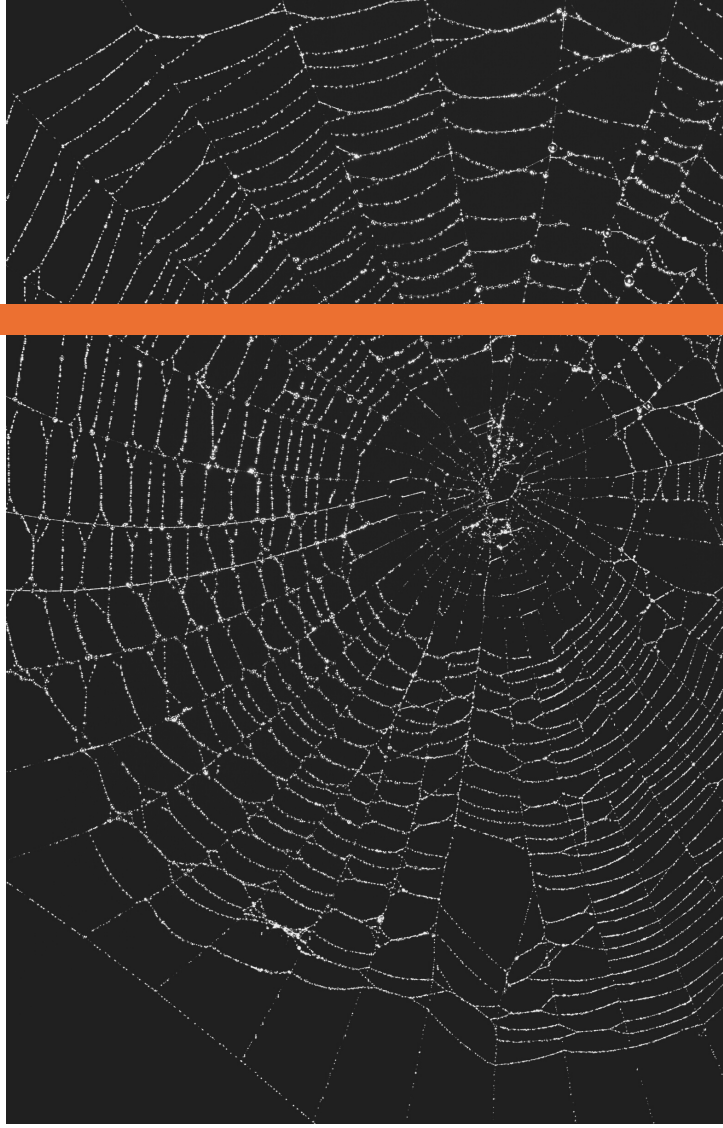
## EMPLOYEE AWARENESS TRAINING WILL TEACH YOUR EMPLOYEES HOW TO SPOT A CYBERATTACK AND HOW TO PROPERLY RESPOND

Ongoing training and testing of your employees will provide detailed insights into their cybersecurity behaviors and habits. To determine these behaviors, simulated phishing emails campaigns can be sent to your employees and report if they are prone to clicking where they shouldn't.

By analyzing these behaviors you can strategically provide additional training to mitigate the risks of malware, data loss and cybertheft. This approach to employee training and testing has shown significant results across all industries and sizes of organization. **On average, companies that implement ongoing awareness training reduce their "phish-prone" percentage from 40% down to just 5% within 12 months.**

# Protect Your Credentials:

**DARK WEB MONITORING**



Digital credentials, such as usernames and passwords, connect you and your employees to your network, critical business applications, as well as online services. Unfortunately, criminals know this —and that's why digital credentials are among the most valuable targets. **Once stolen, your company's credentials are then bought and sold on the Dark Web.**

Compromised credentials are then used to conduct further criminal activity. And since employees often use the same password for multiple services, the potential damage from a single compromised credential is increased exponentially. Over 75% of credentials compromised are not discovered by the victims organization, but by law enforcement or a public announcement of a data breach. This lack of visibility increases the amount of time a cybercriminal can use those credentials for nefarious means.

Dark Web Monitoring can identify, analyze and proactively monitor for your organization's compromised or stolen employee data and mitigate the risks associated.

## Key Takeaways

- When compared to traditional security solutions, EDR provides enhanced visibility into your endpoints and allows for faster response time. EDR can protect your organization from advanced forms of malware, phishing and other modern threats.
- Your employees are your weakest link when it comes to cybersecurity. One of the most prolific hackers of all time, Kevin Mitnick, has stated **"It takes one to catch one, and the best way to catch one is through awareness training."**
- Monitoring the Dark Web reduces the amount of time between the occurrence of a data breach and when it is discovered, limiting the window of opportunity criminals have to take advantage.

**For more information on how Salvus TG can improve your cybersecurity, please reach out to us at 816-222-1115 or info@salvustg.com**