

Cyber Security Monitoring for Small & Medium Businesses

# Four Things to Consider when Protecting Your Small Business from Cyber Threats

# Who Should Read This?

This guide is essential reading for owners and executives of Small and Medium-sized Businesses (SMBs) who are concerned about the increasing threat of cyber-attacks.

It is specifically aimed at CEOs, CTOs, CIOs, IT Managers, and Security Officers of Small and Medium Businesses (SMBs) who want to safeguard their businesses against cyber threats. If you are concerned about securing your business data, network, or customer information, this document is for you.

Within this document, we discuss the critical cybersecurity challenges faced by SMBs today and specifically focus on the:

- Alarming frequency of cyber-attacks and the specific vulnerability of SMBs.
- Ongoing need to proactively monitor SMB environments against cyber threats.
- Importance of affordability without compromising on essential security features.

Security platforms are purpose built to identify and alert you on evolving cyber threats. In this document, we examine the key features that an effective security platform for SMBs should include, such as fake domain detection, zero-day visibility, AI-powered cyber threat analysis, and ransomware alerts. We highlight the significance of having a security platform that provides clear, actionable insights without the complexity typically associated with enterprise-level tools.

Finally, we emphasize the necessity of choosing a security platform that fits the budget of an SMB while offering the best value in terms of price and performance.

This document is not only a guide, but a call to action for SMBs to take proactive steps in securing their digital assets, ensuring business continuity, and maintaining customer trust. If protecting your business from cyber threats is a priority, this article will provide you with the knowledge and direction you need.

# Is there a Problem?

“Hackers aren't waiting for you to catch up. They're **already inside** your network.”

Many business owners don't believe they are a target. Yet **43% of attacks target SMBs**—attackers expect them to have less protection.

Ransomware attacks **increased by 148%** last year. Are you next?

**60%** of SMBs are **out of business** within 6 months after a cyber-attack.

**39**  
seconds

Every 39 seconds,  
a cyber-attack  
strikes.



## So what can you do?

With the current cybersecurity landscape, as an SMB, you need to identify cyber issues and prioritize which ones need immediate attention. When investigating cyber security offerings, you need to consider the following variables.

**1**

### **Strong Detection Engine.**

Regardless of your size, you need a powerful security detection engine. You must know if there is a problem.

**2**

### **Made for Enterprise—not SMB.**

Most robust platforms are built for enterprise, so they include detection, alerts and enterprise-level tools necessary to FIX the problems. Their price reflects it. However, as an SMB you only need to know if there is a problem (quickly)—since most small businesses rely on MSPs to fix them.

**3**

### **Too Hard to Use.**

Most full-featured detection tools are ridiculously hard to use. They hide the information you need among layers of menus, reports, and other complex functions—fine for an IT team, but useless for you.

**4**

### **Too expensive.**

Most effective alternatives are WAY too expensive for SMBs (you won't buy a \$20k application). It must fit your budget.

So, where do you find a powerful security offering, with the right features for SMBs, that is super easy to use, and priced within reach? That is the question.





# 4 Things to Consider


**1** You need Powerful Cyber Security Monitoring

**2** The RIGHT Fit for SMBs

**3** MUST be easy to use

**4** Affordable

Now let's consider each of these in detail.



# 1 You Need Powerful Cyber Security Monitoring

Ongoing monitoring proactively protects your business. It must include security features critical for SMBs:

## ■ Fake Domains.

Identifies potential imposter domains to prevent phishing attacks and protect your brand, ensuring your business stays safe from deceptive practices.

## ■ AI Powered.

Uses machine learning to quantify current and future risks. Provides intelligent, adaptive protection that evolves with emerging threats.

## ■ Adversarial Insights.

Provides insights into potential attackers, helping you stay informed and prepared to defend against threats.

## ■ Historical Trends and Analysis.

Offers critical details to help you make informed security decisions, improving your overall risk management.

## ■ Zero-Day Visibility.

Quickly detects unknown threats before they can cause damage, keeping your business secure from new and emerging risks.

## ■ Ransomware Alerts.

Identifies known ransomware to provide early warnings, allowing you to take preventative measures before an attack occurs.

## ■ Recursive Assessment.

Continuously updates your security insights, adapting to new threats and ensuring ongoing protection.

# 2 The **RIGHT** Fit for SMBs

Most SMBs don't have on-site security specialists—so they can't fix what they find. However, all SMBs need to be alerted to problems and get help. TARA CTA concentrates on SMBs and their unique needs.

- **External Weaknesses.**

Identifies external, Internet-facing risks (email, firewalls, website, and imposter domains) and highlights security gaps. Ensures all external entry points are monitored and secured, reducing the risk of outside attacks.

- **Monitoring and Alerting.**

Quickly identifies issues without needing deep security expertise, making it easier for SMBs to manage security and respond to threats efficiently. Sends email alerts to designated support resources for rapid response.

- **Red / Green Light Indicators.**

Simple indicators provide at-a-glance security status, perfect for non-technical users to easily understand and act upon.

- **Team Collaboration.**

You can visually mark items as fixed or accepted making it easy to track the status of security issues and resolutions.



# 3 **MUST** be Easy to Use

It can contain much of what is found in enterprise cybersecurity systems, but it should be tailored to the specific needs of SMBs, focusing on what is needed 100% of the time.

## ■ Overall Risk Score.

Shows an overall risk score and highlights risk findings in each security category. Understand what's at risk, delegate getting it fixed, and get back to running your business.

## ■ Industry Peer Comparisons.

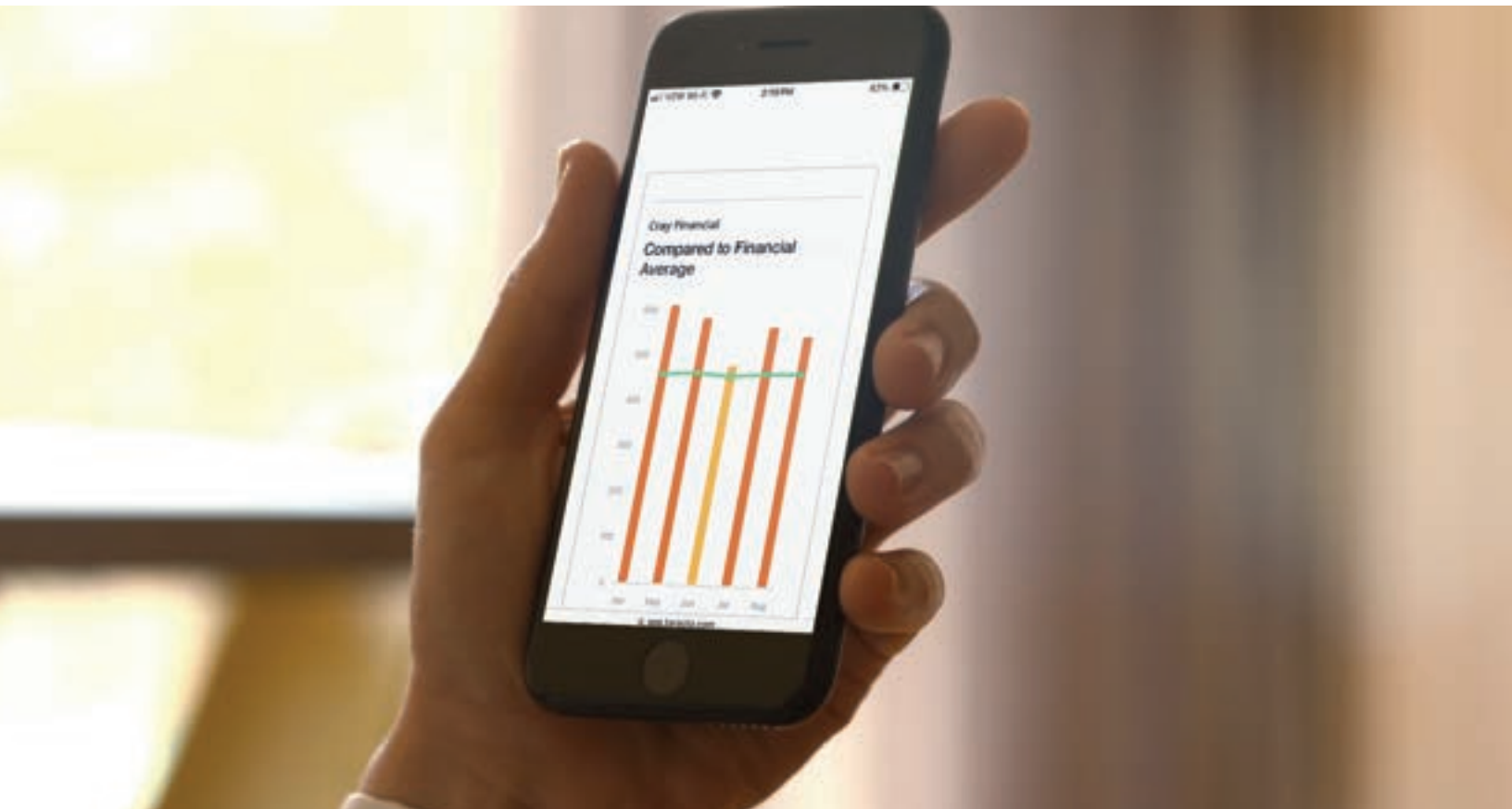
Benchmarks against other organizations in the same industry. Helps you understand how your security stacks up against peers, guiding improvements and justifying security investments.

## ■ Detailed Data Breach Analytics.

Lists any data breach that involves organization employees including which ones were exposed. Provides transparency and accountability, enabling you to address breaches swiftly and mitigate damage.

## ■ Easy Data Export.

Includes visual analytics for common issues and the ability to export findings to other tools if additional analysis is desired.







# 4 Affordable

SMBs don't have the budgets of a large enterprise, so the price has to be easy-on-the-pocket or they won't purchase it. They should look for:

- **Absolute Best Value.**

Single/fixed price model and a small percentage of the cost of enterprise alternatives, catering to the smaller budget available at SMBs.

- **Affordable Monthly or Annual-Prepaid Options.**

Should include a payment plan that fits a limited budget.

- **Cancel Anytime.**

Avoid long-term contracts. The program should prove its value each month.

# Conclusion

The simple truth is...the cyber security needs for an SMB are very similar to that of a larger company. But in many cases, SMBs need to be even more diligent since they are often considered an easy target of opportunity for hackers. However, most SMBs do not have IT security specialists in-house, and often rely on Managed Service Providers (MSPs) to protect their business.

As such, they don't need a cyber security utility to fix the problems—but they must be able to DETECT them quickly and easily. Ideally, they should predict where cyber risks are evolving into problems—so their MSPs can fix the issues and ensure they are always up and running.

We've identified the type of cyber security system and features to consider when evaluating your options. Hopefully, this will help you stay protected, avoid being one of the attack statistics, and concentrate on running a successful business.



Brought to you by  
TARA CTA  
(248) 793-8660  
[www.taracta.com](http://www.taracta.com)