Security Built for Your Business

T. Daniels Consulting

INTRODUCTION

Your day starts with a hot cup of coffee (or maybe an energy drink if coffee isn't your thing) and a long list of emails that need your immediate attention.

You do your best to get through everything you didn't get to from yesterday before everyone else gets in and you get bombarded with today's fire drills. And that project you've been trying to get to for the last 3 weeks? Well it's just going to have to wait for another day.

Security for your organization and your critical data is one of the last things on your mind but it should be of time concern in today's world. But where do you start with identifying security solutions that could keep your organization safe, provide you the visibility into your network that you need, and let you get back to the rest of your to-do list?

Take a look at some of the most common security threats you face, the best practices you can put in place to protect your organization, and how T. Daniels Consulting can help.

Weak or Re-used Passwords

81% of hacking-related breaches leveraged stolen or weak passwords.[1] The time for post-it notes on monitors and Password123 are way over.

Your employees need secure passwords that can be managed in a foolproof way. How are you ensuring that passwords aren't leaving your business vulnerable to a breach?

1 http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Password Best Practices

Be password SMART

Symbols, letters & numbers
More than 12 characters
Avoid personal information
Refuse to reuse old passwords
Trust password management tools

Multi-Factor Authentication

MFA tools provide additional proof of identity beyond simple passwords. They require a user to not only authenticate with something they know (e.g. a password), but with something they have and something they are as well. This limits a cyber criminal's ability to use stolen credentials to access accounts.

T. Daniels Consulting's SecureFactor

Our unique multi-factor authentication solution helps you to reduce the likelihood of network disruptions and data breaches arising from lost or stolen credentials. SecureFactor goes beyond traditional 2-Factor Authentication (2FA) by considering innovative ways to positively identify users – such as with our Mobile Device DNA approach. And our large ecosystem of 3rd party integrations means that customers can consistently deploy SecureFactor protection to access the network, VPNs, Cloud applications – wherever it's needed.

Happy Clickers

90% of attacks start with a phishing email.[3]

As long as organizations have happy clickers that will follow the link, hackers will continue to leverage this method for malware delivery.

Phishing education is an important way to ensure that all of your employees know the warning signs of a phish, but you need phishing protection in place as well.

Wouldn't it be great if there was a solution that provided protection AND offered an education refresh?

3 https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing

Phishing Education

Education is critical for helping users know the risks of phishing emails and the warning signs to keep watch for.

You want to ensure that your employees are prepared to defend themselves against anything that comes through their inbox.

DNS Monitoring and Blocking

But education alone can't completely protect your employees. As phishing emails become more personalized and targeted, it's just a matter of time before something gets clicked. You need to have a solution in place that monitors DNS traffic and blocks access to malicious sites.

DNSWatch

T. Daniels Consulting's DNSWatch detects malicious DNS requests and blocks access to these sites, redirecting the user to a safe page that educates them on the risk and warning signs of a phish.

These events are teaching moments for your employees and a very effective way to engage people about the risks of clicking on phishes

File Download Madness

Similarly to malicious links sent via email, sending malicious email attachments is another common way that hackers deploy their attacks.

This method requires the hackers to develop an attachment that will entice the victim to download.

Common types of attachment lures include:

- Invoices
- Scanned documents
- Delivery failure messages
- Order & payment confirmation
- Specific flight confirmations

Can you protect users from malicious download attacks?

Signature-based Threat Protection

Scanning for known malicious files before they are opened provides a necessary level of detection to prevent this method of attack.

Cloud Sandboxing for File Detonation

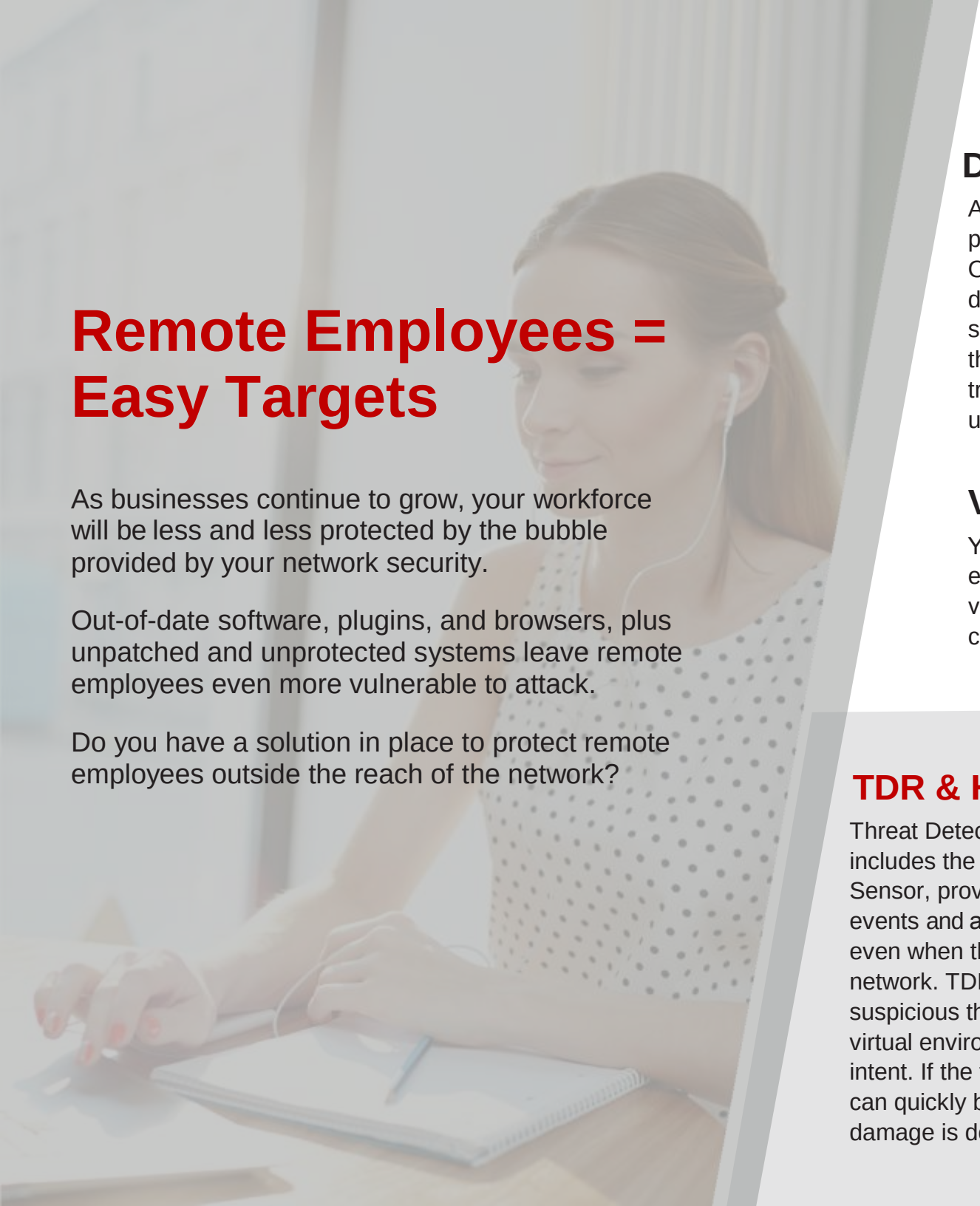
Cloud sandboxing is a safe way to open threats and detonate potentially malicious files. By opening them in a virtual environment that mirrors your system is every way, you can get a clear picture of any malicious intent, without putting your actual device at risk.

GAV and APT Blocker

Included with T. Daniels Consulting's Total Security Suite, Gateway AntiVirus (GAV) and APT Blocker provide layered defenses against malicious file attachments in phishing attacks.

GAV leverages a continuous updated database of signatures to block known malicious file extensions from being opened.

Unknown threats and zero day malware attacks prevent a whole new set of challenges in defending your organization. But with T. Daniels Consulting APT Blocker, you're able to detonate these files in a safe, virtual environment to determine if they have malicious intent. If it does, the file will be quarantined to ensure that it isn't opened.



Remote Employees = Easy Targets

As businesses continue to grow, your workforce will be less and less protected by the bubble provided by your network security.

Out-of-date software, plugins, and browsers, plus unpatched and unprotected systems leave remote employees even more vulnerable to attack.

Do you have a solution in place to protect remote employees outside the reach of the network?

Deep threat analysis

Advanced and evasive threats need strong protective solutions in place to defend against them. One way to protect against these threats is with deep threat analysis tools like network and host sandboxing. By detonating malicious and suspicious threats in safe, virtual environments you can see the true intent of a threat before it can impact your users.

Visibility to the endpoint

You can't stop what you can't see. So for remote employees, you need to make sure you have visibility into the endpoints, even when they aren't connected to the network.

TDR & Host Sensor

Threat Detection & Response (TDR), which includes the T. Daniels Consulting Host Sensor, provides detailed visibility into threat events and activity to your users' endpoints, even when they aren't connected to the network. TDR also enables the detonation of suspicious threats from the endpoint in a virtual environment to determine malicious intent. If the threat is deemed malicious it can quickly be remediated before any damage is done.

Surfing Employees & Slow Throughput

Visiting time-wasting or even inappropriate sites can have a huge impact on business productivity.

In fact, the average employee could be wasting more than 8 hours per week on activities unrelated to their job. That's an entire work day![4]

Slow throughput can have your bustling office moving at a snail's pace. Is it Karen in accounting watching too many cat videos on YouTube? Or maybe Patrick in sales watching the game he couldn't get tickets to?

How can you ensure that employees are maximizing their productivity while at work, and more important, that they aren't visiting dangerous or inappropriate websites on the job?

4 https://nypost.com/2017/07/29/this-is-how-much-time-employees-spend-slacking-off/

Visibility into web activity

Your employees need access to the web to do their jobs, but this can also cause strain on your network performance. You need visibility into users' web surfing to determine if access to time-wasting sites is what's causing the issue.

URL filtering

You need the ability to guard your network against risky web content, malicious activity and even time-wasting sites. Web filtering enables you to enforce corporate policy to ensure that access to any of these sites is monitored and approved.

WebBlocker

T. Daniels Consulting's WebBlocker provides a powerful and easy-to-use solution for controlling and monitoring web activity across your entire organization. Further more, you can easily block or limit non-work related web activity to ensure adequate bandwidth is available at all times.

Dimension

T. Daniels Consulting Dimension enables you to see network activity in real time presented in intuitive and interactive dashboards and reports. This enables you to quickly see who is consuming the most bandwidth, if there are unusual traffic patterns, and the most visited websites.

What's the Next Big Threat?

You don't have the time (or maybe just not the energy) to keep up with threat trends and today's latest malware attack.

But threats continue to evolve, and hackers are attacking your business from every angle.

Do you have a solution in place to protect against known, unknown and evasive malware threats?

Access to threat research in an easy-to-consume way

Even when time doesn't permit, you still need a way to stay up to date on threat trends and predications. If you don't have the bandwidth to do it yourself, make sure you're working with teams that can provide this insight to you.

Layered security to protect at every layer

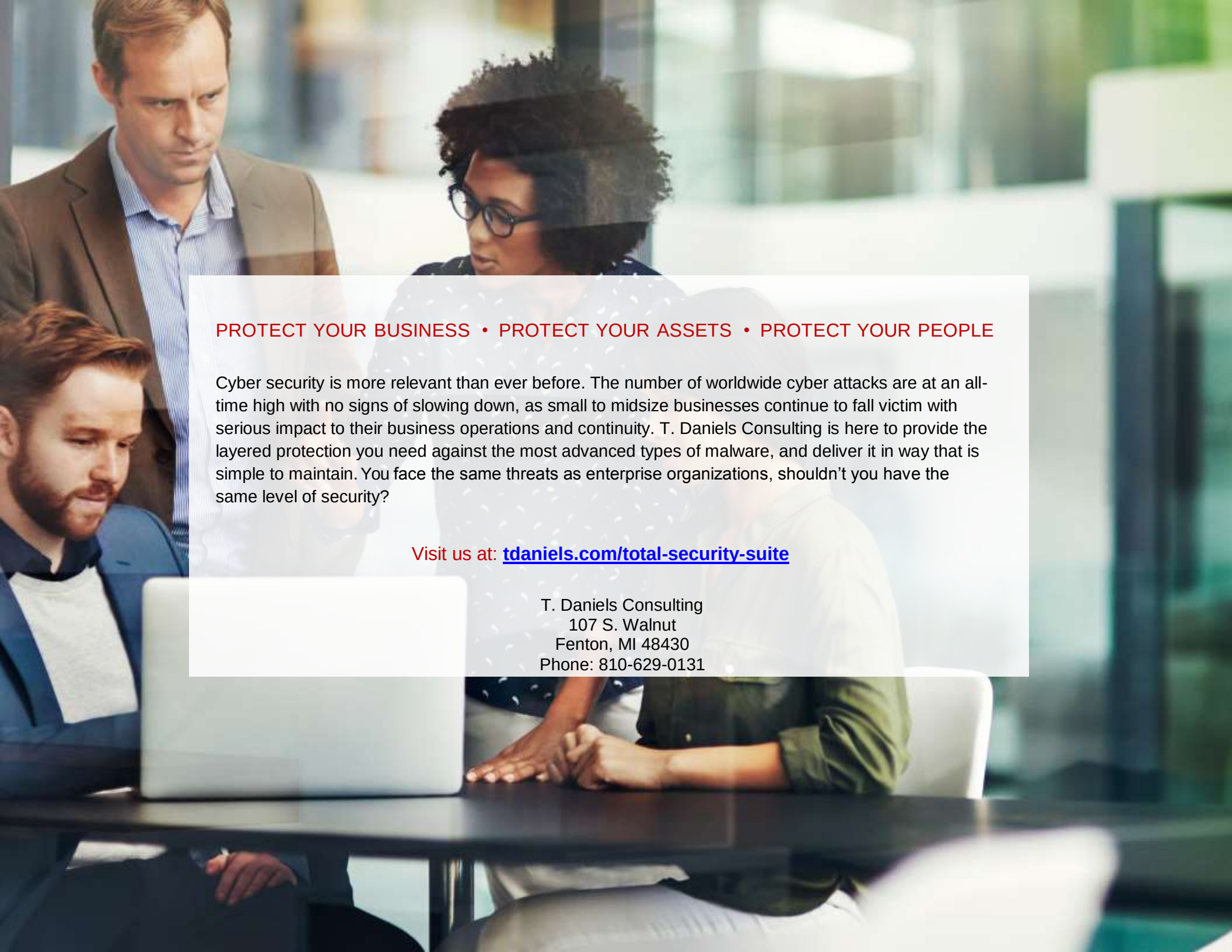
The attacks of today and the threats of tomorrow require a layered approach to your security solutions. You need the capabilities to defend against every type of attack at every layer.

Total Security Suite

T. Daniels Consulting's Total Security Suite provides protection against advanced threats at every layer. Offering fundamental services like Gateway AntiVirus and Intrusion Prevention Service to more advanced services like Cloud sandboxing and data loss prevention, T. Daniels Consulting has solutions to protect against known, unknown and even evasive attacks.

Threat Landscape

Our team has one key objective – to stay up to date on threat trends and the latest attacks so you don't have to. We strive to provide you the trends and tips to keep you secure from the latest threats.



PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

Cyber security is more relevant than ever before. The number of worldwide cyber attacks are at an all-time high with no signs of slowing down, as small to midsize businesses continue to fall victim with serious impact to their business operations and continuity. T. Daniels Consulting is here to provide the layered protection you need against the most advanced types of malware, and deliver it in way that is simple to maintain. You face the same threats as enterprise organizations, shouldn't you have the same level of security?

Visit us at: **tdaniels.com/total-security-suite**

T. Daniels Consulting
107 S. Walnut
Fenton, MI 48430
Phone: 810-629-0131