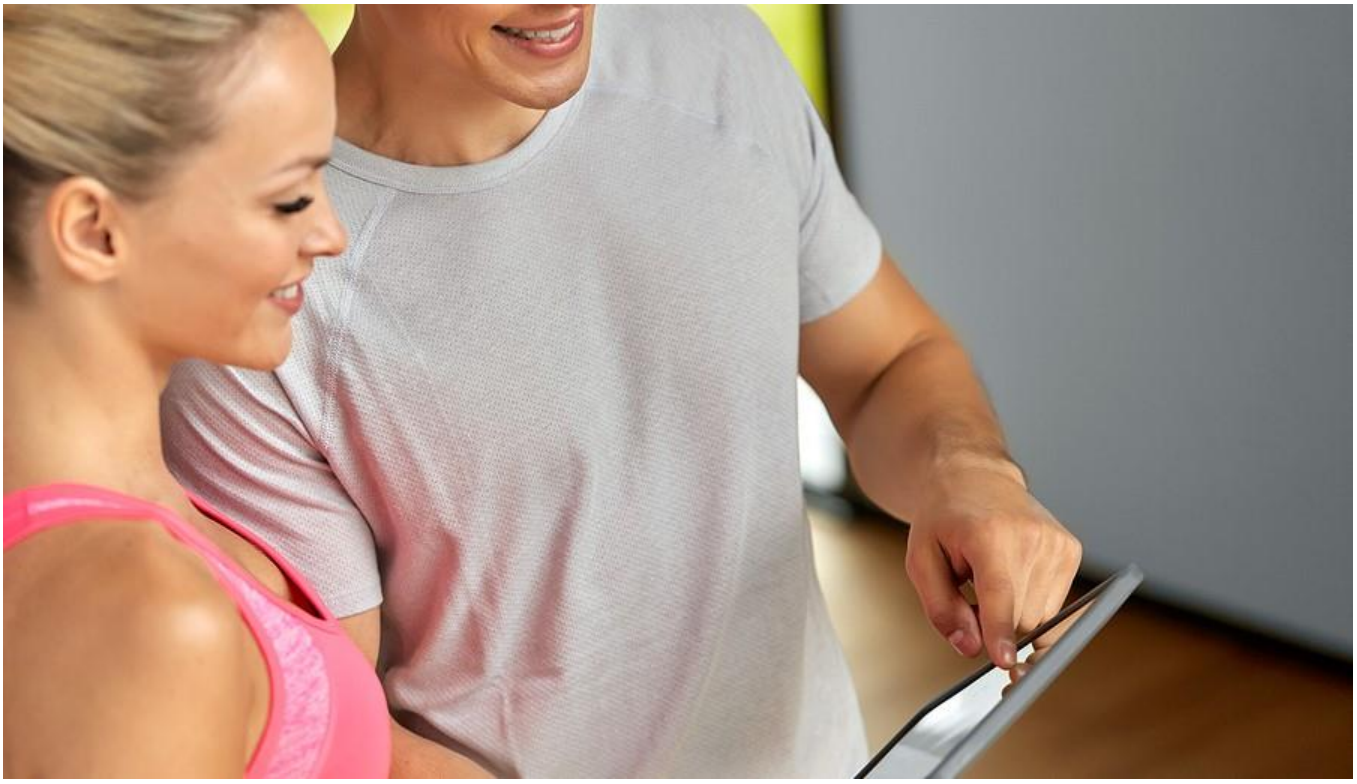
Engage a Personal Cyber Security Trainer for the New Year



In our previous post, we listed three common cyber security threats with security best practices and cyber-security solutions that simplify your life while reducing the risk of an energy-draining security breach. Again, we encourage you to engage your personal cyber security trainer to improve your security health for the new year.

Until you attend that life-changing meeting, here are three more common cyber security threats you face with security best practices and solutions to help keep you in shape.

Remote Employee Threats

As remote work multiplies employee locations, your workforce will be less and less protected by your network security bubble. Out-of-date software, browsers, and plugins, plus unpatched and unprotected home systems leave remote employees even more vulnerable to attack.

Deep Threat Analysis and Endpoint Visibility

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 the true intent of a threat can be known before it impacts users.

> *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 and Host Sensor

Threat Detection and Response (TDR), which includes Host Sensor from WatchGuard Technologies, provides detailed visibility into threat events and activity out to users' endpoints, even when they aren't network connected.

TDR also enables the detonation of suspicious threats from endpoints in a virtual environment to detect malicious intent. If the threat is discovered to be malicious it can quickly be remediated before any damage occurs.

File Download Traps

Like phishing links embedded in email, malicious email attachments provide another common vehicle for hackers to launch attacks. In this scenario, hackers develop and entice the victim to download an attachment with a benign-looking name.

Common types of attachment bait include:

- Delivery failure notifications
- Scanned documents
- Order and payment confirmations
- Specific flight arrangements
- Invoices and bills

Signature-based Threat Protection

Scanning for known malicious files before unsuspecting users open them affords the necessary detection to prevent this method of attack.

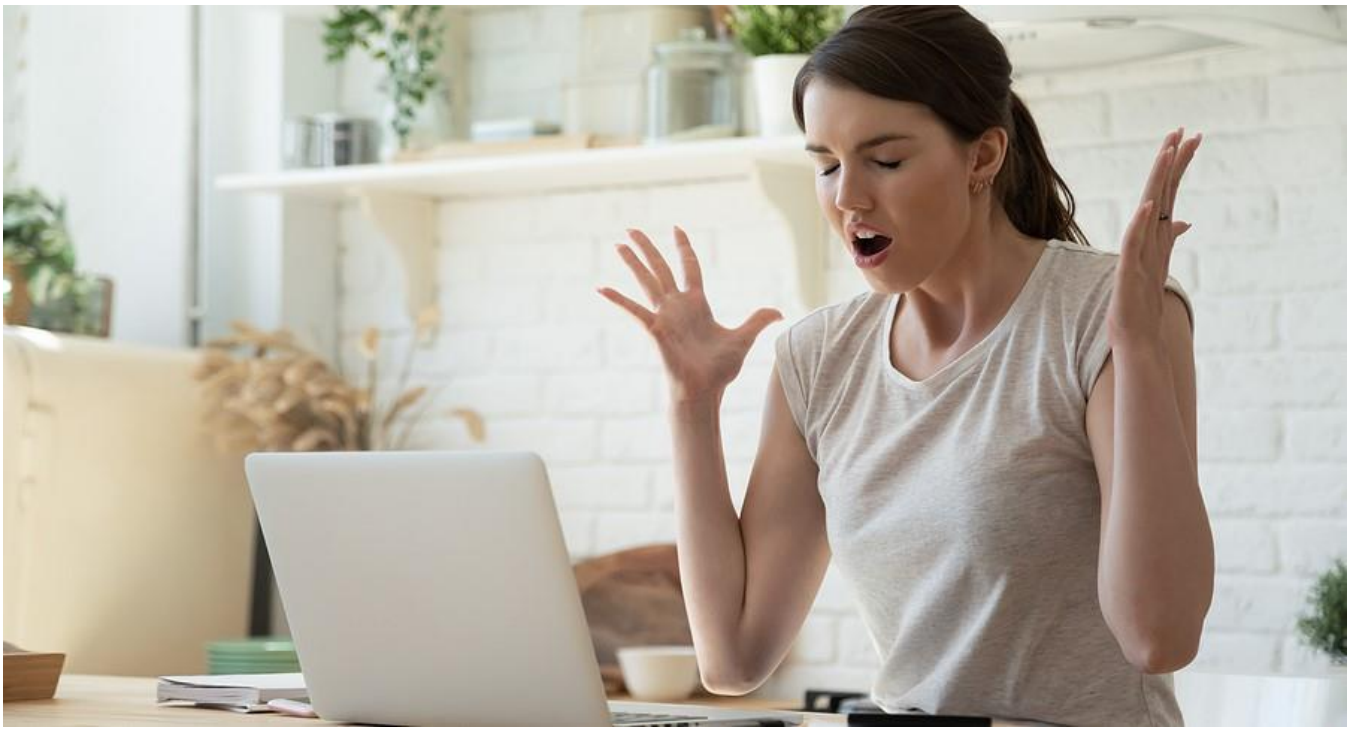
Cloud sandboxing provides a safe way to open threats and detonate potentially malicious files.

By opening files in a virtual environment that mirrors your system in detail, you get a clear indication of malicious intent, without putting your device at risk.

GAV and APT Blocker

WatchGuard's Gateway AntiVirus (GAV) and APT Blocker provide layered defenses against known malicious file attachments. GAV leverages a continuous updated database of signatures to block malicious file extensions from being opened.

With WatchGuard APT Blocker, you're able to detonate unknown threats and zero-day malware attack files in a safe, virtual environment. If malicious intent is detected, it quarantines the files to prevent opening.



Slow Throughput from Uncontrolled Surfing

The common practice of employees visiting time-wasting or inappropriate websites exacts a huge toll on business productivity. According to the New York Post, the average employee wastes more than eight hours per week on activities unrelated to their job!

> *Your employees need access to the Internet to do their jobs, but you need visibility into users' web surfing to determine how it impacts performance.*

Slow throughput can reduce work at your office to a snail's pace. Is it Bob in marketing watching too many music videos on YouTube? Or maybe Tiffany in HR watching the event she couldn't attend?

URL filtering

You need tools to guard your network against risky web content, malicious activity, and time-wasting sites. Web filtering enables you to enforce company policy by monitoring access to any of these sites.

WebBlocker

WatchGuard WebBlocker provides a powerful and easy-to-use solution for controlling and monitoring web activity across the organization. Moreover, you can easily block or limit non-work-related web activity to ensure adequate bandwidth is always available.

Dimension

With WatchGuard Dimension, you see network activity in real time displayed in intuitive and interactive dashboards and reports. You quickly see who is consuming the most bandwidth, unusual traffic patterns, and the most visited websites.

Engage a Personal Cyber Security Trainer

The attacks of today and the threats of tomorrow require a layered approach to security solutions. Engage a certified and experienced business cyber-security trainer from eMazzanti Technologies to design a cyber-security program for your business. As a 5X WatchGuard Partner of the Year, they work to quickly get your business cyber security into shape.

Call today to schedule a free consultation.