BUILDING A FIRST-CLASS CYBERSECURITY STRATEGY

A comprehensive cybersecurity plan can be visualized as an equilateral triangle. Just like the equilateral triangle is constructed of three sides identical in length, each of the three walls of the security triangle represent equally important pieces of the puzzle. Much like eating a well-balanced diet requires incorporating items from all areas of the food pyramid, building a robust cybersecurity strategy requires implementing products from each of the three sides of the security triangle. Adding multiple products from one side and none from another will result in gaps within your security approach.

On the right side of the security triangle sit the *control tools.* These are the Zero Trust tools that provide proactive protection. Based on the rules you set, tools on this side of the triangle stop unwanted behavior instead of relying on machine intelligence to recognize and react to it. Firewalls control access to your network. Application Allowlisting dictates which applications can run in your environment. Ringfencing™ restricts what those permitted applications can access and interact with once they are running. Privileged access management (PAM) regulates the use of admin privileges. While proactive control tools provide effective protection, a robust cybersecurity approach will never solely rely on controls from a single side of the security triangle.

On the left side of the security triangle, you have *detection tools.* Antivirus tools scan the endpoint for known destructive files and bad behavior so they can detect an impending threat and respond by quarantining the suspicious files. NextGen AVs and EDRs use heuristics, machine learning, and artificial intelligence to detect and respond to behavior the tool judges as harmful or unwanted. Instruments on this side of the triangle rely on the tool to see an issue, decide if it's good or bad, and then respond. Detection tools provide great reinforcement for tools that provide control. The most vigorous security plans utilize instruments from all three sides of the triangle, minimizing potential cyber vulnerabilities

At the bottom of the security triangle is the *human firewall.* End users stand between your endpoints and the adversaries trying to access them. They are the gateway into your organization. Strong security strategies must incorporate information security training for all users. However, even the most cyber-savvy users aren't immune to human error and can fall victim to phishing attacks. That is why a robust security plan can't rely on user training alone.

TERMINOLOGY

- **Application Whitelisting** - The approach of restricting the usage of any tools or applications only to those that are vetted and approved.
- **Anti Phishing** - Applications that monitor all incoming emails, downloads, URLs, and hyperlinks to check them for any possible viruses or phishing scams.
- **Anti Spam** - Solutions that focus on blocking and mitigating the effects of illegal emails – or spam – on email users.
- **Anti Virus** - A software designed to hunt and remove viruses from your device(s) or block viruses from entering in the first place.
- **Dual Factor Authentication** - A security process in which users provide two different authentication factors to verify themselves.
- **EDR** - Endpoint Detection and Response tools monitor and record activities and workloads taking place on a device to detect and respond to malicious behaviors and files.
- **Elevation Control** - Enables users to run specific applications as a local administrator, even when they do not have local admin privileges.
- **Firewall** - A security program or software that controls network traffic and prevents outsiders, including threat actors, from entering your organization.

THREATLOCKER®

TERMINOLOGY CONT.

- **IDS** - Intrusion detection system is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered.
- **Network Control** - An endpoint firewall enabling you to control inbound network traffic, using dynamic ACLs, all managed from a central location.
- **Ringfencing™** - An endpoint security tool unique to ThreatLocker® that blocks your applications from interacting with other applications, files, and the internet, proactively defending against the spreading of malicious instructions.
- **Storage Control** - A ThreatLocker® tool that provides protection for your internal and external data and information storage.
- **ThreatLocker® Ops** - Monitors behavior patterns of software and users with the addition of detection, alerts, and automated responses.
- **Threat Hunting** - A proactive approach to identifying previously unknown or ongoing non-remediated threats within an organization's network.

CONSTRUCTING A CYBERSECURITY TRIANGLE

With your new knowledge, fill in the blanks in the chart below.