THREATLOCKER

Stop Adding the Wrong Layers to Your Security Stack!

Revisit the Basics to Learn How A Different Approach Can Prevent More Attacks

To IT professionals and business leaders trying to keep their systems secure,

I've been in the cyber security business for over 20 years, serving in roles from security analyst to CTO and now CEO of a cyber security software vendor. Throughout my career, the most common question I am asked has been, "What should I invest in to give me the best protection for the cost?"

While the question remains the same, my answer has changed over the years as technology has evolved. Antivirus (AV) software used to help, but never did the job sufficiently. As attackers evolved, security solutions like AV have had difficulty keeping up with malware and the various methods of entry that have been devised. Companies have responded to this by continually adding layers to their security stack and creating entire departments of resources dedicated to finding threats.

For most companies, this level of investment just isn't feasible. Continuing to add technologies for detection (such as anti-phishing, MDR, IPS, IDS, AV, anti-spam, and EDR) is overlooking a basic premise. Specifically, why are we investing in more layers of detection when the best security investment we can make is to stop the threat from ever entering our systems?

Today, my answer to the question of what to invest in for the best protection and value is—better controls. We need to block anything from executing that isn't approved as safe to execute. This used to be highly manual and a poor end-user experience, but technology for controls has also evolved. There are IT-friendly and user-friendly ways to have usable controls for applications and storage that can make securing your systems much more simple and effective for a much smaller investment.

I wrote this paper to help explain why the current approach to security isn't working for most companies and how getting back to the basics is the best way forward. I hope you find it helpful for your research. I also welcome any questions that may arise and encourage you to reach out to me on LinkedIn.

Best,

Danny Jenkins
CEO, ThreatLocker

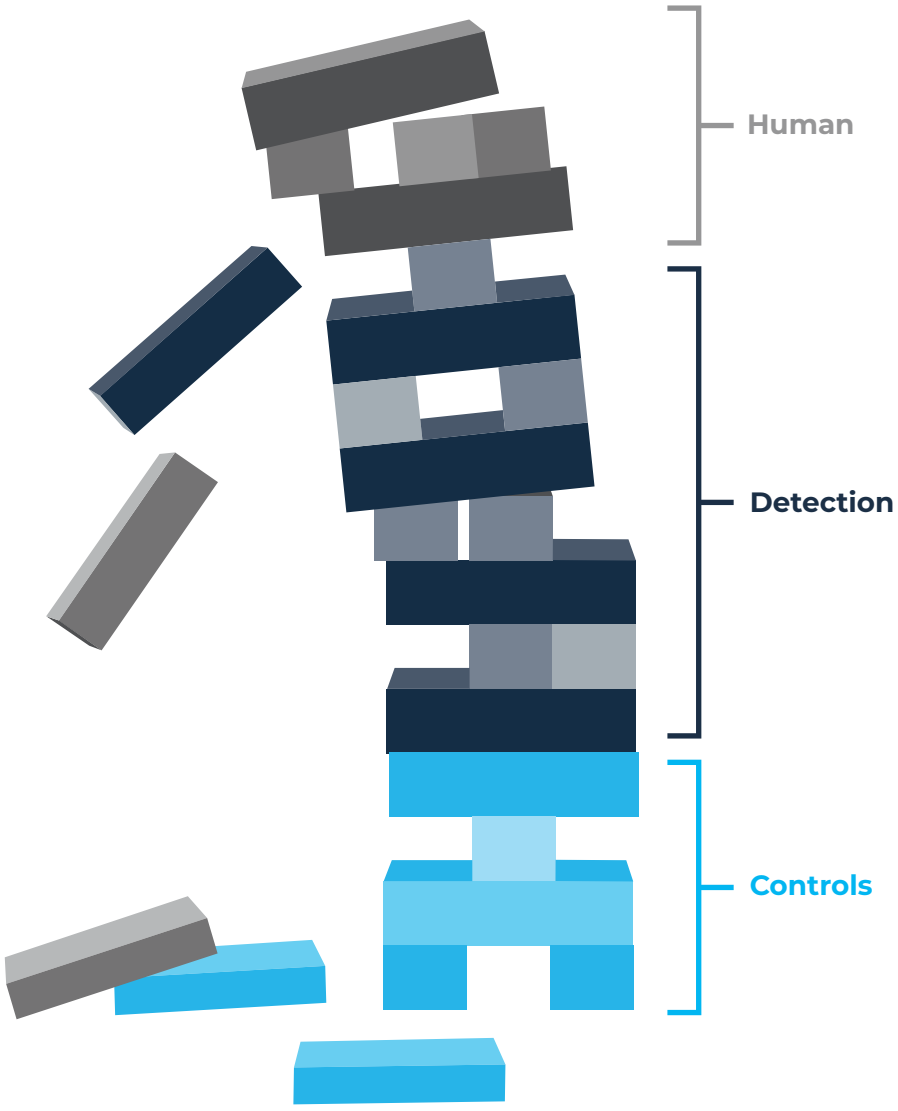
Why Adding More Detection Layers Isn't Working

Each time a new attack is found, we add ways to detect and prevent that attack. This strategy worked well for a time. In the 1990's security measures were focused on controls such as firewalls and internal policies. By the early 2000's, antivirus protection was a must. A new worm or Trojan arose and antivirus professionals quickly developed and sent us a method to detect it and stop it before it damaged our systems. But by 2005, attacks shifted from causing chaos to data theft and ransom. Additionally, the volume of attacks grew substantially. Over 5 million new malware samples were being found annually.

So what did companies do? They added so called NextGen endpoint protection because legacy antivirus wasn't keeping up. Unfortunately, by 2010 it was clear that cyber attacks were becoming a business model. Keyloggers were running rampant getting bank information. Fileless malware and more targeted attacks became the norm. So technologies like endpoint detection and response (EDR) were developed and added to the security stack.

By 2015, IT teams were buried in alerts and security operations centers (SOC) were formed to manage alerts. SOC analysts were reactionary and trying their best to find issues and stop invaders before they caused irreparable damage. The most sophisticated SOC teams are now using security tools in the cloud and training their people to threat hunt and proactively seek out vulnerabilities and attackers in order to defend against them.

The end result is a teetering tower of protection. Many disparate systems that are still leaving entry points vulnerable. If you look at the bulk of security investments in the past 20 years, they have been in detection layers. This is because the assumption is that the controls are not strong enough to keep attackers from getting into our systems, so we need ways to quickly detect them once they are inside.



Florida cities pay $2M in ransom to get systems back online

Local steel company crumbles when attacker steals data

Spanish shoe shop used as entry point for huge bank data breach

Hundreds of dental offices crippled by ransomware

22 Texas cities forced back to paper after ransomware attack

Medical debt collection agency connected to 750 hospitals got phished

University of Utah pays $457K ransom for just 0.02% of data

UCSF pays $1.14M ransom to recover encrypted data

Entertainment law firm victim of data theft of celebrity info with $21M price tag

Travelex money-exchange goes offline for a month to recover from cyber attack

Malicious infection locked down Communications & Power Industries—including naval weapons information

Cognizant servers encrypted by Maze malware costing upwards of $70M

Yet Attackers Are Still Getting In

Looking back, this has been a logical evolution. Except for one problem—**attackers are still getting through.**

Just in the first half of 2020, the 11 biggest ransomware attacks hit municipal governments, universities and private businesses. And combined they have spent more than $144 million on everything from rebuilding networks and restoring backups to paying the hackers ransom. The largest breaches and payouts are what the media picks up, but countless small companies are also being attacked—often leading to closing of their doors.

What Happens When Attackers Get In

The short term results of a cyber attack are often stolen data or a ransomware lock on systems. I've talked with so many business leaders who swore they would never pay a ransom, but when it happens to them they desperately want to do whatever they can to get back their data. Unfortunately, in both 2018 and 2019 only 26% of organizations that paid ransoms got all of their data back. That leaves 74% that are not able to return back to normal operations.

Less obvious than ransomware, but potentially even more damaging is data theft. Organizations can be completely unaware that data has been copied and removed from the system because they still have their data. Yet it can be sold multiple times before anyone identifies the source of the breach. When the data stolen is customer information, this can be even more costly to attempt to repair the damage.

Size Doesn't Matter

Small companies are just as attractive (if not more so) to cyber attackers as large companies. Smaller companies in a supply chain are being targeted as an entry point to then hop to larger prey. This means smaller companies can not only lose important partners and suppliers if not protected, but also be held responsible for mega-breaches.

What most companies don't realize is that attackers today don't just enter, steal and leave your systems. Instead, they bring you 7 years of bad luck. They study you, learn your business, your customers, your suppliers and they use that information to social architect future attacks.

> **"I'll never forget my first call in cyber security where a CEO was crying because his business was gone. I've seen it so many times now where you leave work on Friday and you wake up on Monday morning, turn on your PC and have a red screen."**

Resolving the Attack Doesn't Absolve Your Record

What many companies don't realize until they get into a breach situation is that there are now agencies in place in many countries that are evaluating your breach. They are looking at how the breach happened and determining how easy or difficult it was to get into your systems.

They will also look at whether or not you had the means to safeguard your systems properly—but didn't. If this is their finding, they can fine you heavily and even stop you from running your business.

A New Approach is Needed

The entry points into our systems are continually growing. Our applications continue to update and change. Our perimeter is expanding with more employees working from home. The volume and breadth of threats continue to increase as the business model for cyber attacks continues to earn money. So where can IT departments invest their security budgets that will provide the most security?

Instead of continuing to invest in more detection layers, we need to go back to basics and keep attackers from entering our systems in the first place. The technology is available to do this without hurting the end user experience, but people need to change their approach.

Having a stronger foundation of security controls will indeed stop more attacks from reaching our entry points and allow us to treat detection as a back-up measure. Here's what we need.

> **"With Covid and remote work the rules of the game have changed. We can't say we have smoke alarms therefore we don't need to worry about fire."**

Step 1: Block Unapproved Executions

The first tactic we need to take is to block anything from executing that isn't on an approved list (also called a whitelist). This functionality is called Application Control or Whitelisting. However, traditional methods of doing this are challenged by application updates - which now happen frequently. For example, Zoom came out with seven updates in two months. Each time an update occurs, traditional whitelisting technology sees this as unapproved and blocks its execution.

What is needed is usable whitelisting that can easily handle updates with a logical and fast workflow. It needs to be simple for IT to handle while not restricting the end user experience.

Step 2: Add Ringfencing

ThreatLocker's proprietary Ringfencing solution goes beyond blocking untrusted applications and controls how applications can behave after they have been opened. This solution adds controlled, firewall-like boundaries around your applications, stopping them from interacting with other applications, accessing network resources, registry keys, and even your files. This approach is extremely effective at stopping fileless malware and exploits, and makes sure software does not step out of its lane and steal your data.

By using Ringfencing, you can stop applications like Zoom from accessing your files and launching other applications that could be used against you - even if it isn't on your whitelist, even it's a trusted application, and even if it's malware. For instance, does Zoom really need access to all of your file shares? Or does Powershell need uncontrolled access to the internet? Applications like Microsoft Word should never be executing PowerShell, yet attackers are exploiting the fact that most companies don't have controls for this. They are using fileless malware that antivirus software can't detect and whitelisting alone can't prevent.

Whitelisting blocks all untrusted applications, however, it will not stop an attacker from weaponizing tools and applications against you. That's why Ringfencing is critical when blocking these attacks. We highly recommend you combine Ringfencing with Whitelisting. By combining these techniques, untrusted applications are not going to be permitted, regardless of how the payload is delivered to you.

> **"Ringfencing applications is what really stops your allowed applications from being weaponized. This should be the de facto standard in how people protect their business now."**

Step 3: Strengthen Storage Controls and Policies

While Whitelisting and Ringfencing protect your applications from being used in attacks, you also need to control access to your data storage. Your storage control should allow you to determine what kinds of files can be saved to, copied from, or deleted off your systems.

You should also be able to set individual policies for file types like text and video, as well as unique policies for storage devices like hard drives or servers.

> **"CISOs need to ensure that this set of controls is a baseline of their security posture. This is so doable and easy. There are no excuses not to do this. It is risk management in spades."**

Strengthening Security Controls Shuts Down Entry Points

With these three control solutions, you've effectively blocked the majority of entry points into your system. With the addition of auditing file and application access for both remote and local users, your IT team can hold a strong security posture with a unified audit.

ThreatLocker Was Designed to Ensure

All Companies Could Secure Their Systems

Most companies will never have the resources for a SecOps team with threat hunters working to prevent attacks. But that doesn't mean that they can't have powerful controls to prevent threats from doing damage. That's precisely why ThreatLocker was built. We believe every organization deserves to have the capabilities needed to defend their data and systems.

We provide usable application whitelisting with ringfencing to better control what is running on your systems. And remember, Ringfencing not only stops what other applications it can call, but also what the application can access. Additionally, the ThreatLocker 24-hour operations center continuously monitors for application and operating system updates, so you don't have to worry about adding a new file to the application whitelist every time Microsoft, Google, or another vendor releases an update. In summary, ThreatLocker is the easiest way for IT to manage a default deny policy.

ThreatLocker also provides the storage controls and policies you need to protect your data. We've also layered on top of that the ability to see in real time your application and file access from both local and remote users. All of this is in an easy-to-use interface that doesn't require cybersecurity training to use. ThreatLocker is the simplest and most effective way to lockdown your systems.

Want to see ThreatLocker in action? Click here to watch a recorded demonstration.

Whitelisting

Ringfencing

Storage control

Real time access

Intuitive interface

24hr Support