CyberLock™

INTELLIGENT ZERO-TRUST

True Local Zero-Trust
Adaptive Cybersecurity

The Problem with Cybersecurity

End-users implicitly trust cybersecurity products and believe they are protected

“I have antivirus software, how did I get a virus?”

– Every infected end-user

Traditional and next-gen Cybersecurity vendors assure their end users
“You are protected”.

Ultimately, there is a disconnect / discrepancy between cybersecurity vendors overpromising efficacies of their products and the end-user expectations of these products.

We maintain this is the primary cause of most malware infections.

End-users expect a lock, not a filter.
At a minimum, the endpoint must be locked at the point of infection.

Please keep in mind

throughout this presentation…

CyberLock's ON and OFF modes indicate whether its **LOCAL** Zero-Trust locking mechanism is ON or OFF.

Global Zero-Trust – The Industry Standard

When CyberLock's local locking mechanism is OFF, its security posture is approximately equivalent to other Zero-Trust solutions, which rely heavily on ML/Ai, global whitelisting and digital signatures, and simply is not as secure as Local Zero-Trust.

Local Zero-Trust – Unique to CyberLock

When CyberLock's local locking mechanism is ON, it provides a TRUE Zero-Trust security posture, and only allows items that are already on the tiny, customized local whitelist, and does not automatically allow by ML/Ai, global whitelisting or digital signatures, as these indicators are only utilized as file insight provided to the end-user.

How CyberLock Works

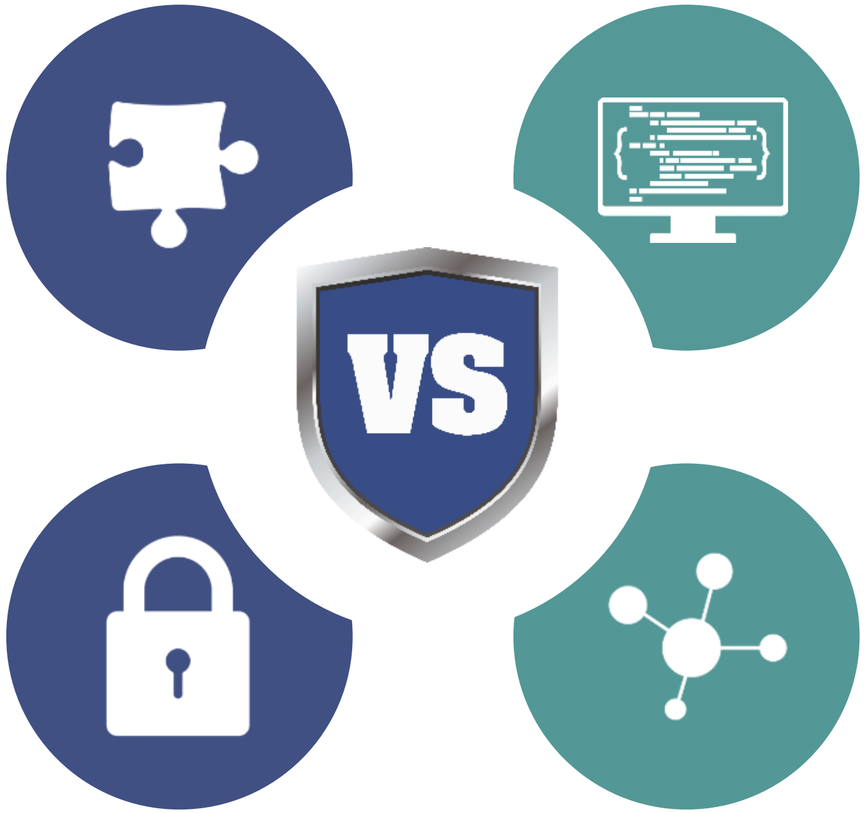
User-friendly toggling computer lock

Complementary Solution

CyberLock is designed and built to complement current traditional and next-gen antivirus solutions by adding a robust layer of user-friendly protection that effectively locks the endpoint when it is at risk.

Malware Prevention

CyberLock toggles to ON and blocks all new non-whitelisted executable code while the user's device is running a web app or email client, preventing malware from ever executing, and toggles to OFF when the device is no longer at risk, to automatically and safely build the tiny, customized local whitelist.



Contextual Engine

Our unique Antimalware Contextual Engine is a sophisticated algorithm that examines the context of every possible attack chain event, so that benign events are automatically allowed and potentially malicious events are automatically blocked.

Machine Learning & Ai

CyberLock's automated whitelisting functionality utilizes Machine Learning and Artificial Intelligence as well as an advanced file reputation service (WhitelistCloud) that provides invaluable file insight to the end-user.

How CyberLock Is Different

Adaptive Cybersecurity and Antimalware Contextual Engine

Dynamic Security Postures

The Achilles' heel of all cybersecurity products is that they are only able to offer a single static level of protection, so at any given time their security posture is likely either too aggressive or too relaxed, resulting in false positives and breaches. CyberLock solves this issue by dynamically adjusting its security posture on the fly, based on the end-user's current activity and behavior. Because of our dynamic security postures feature, CyberLock is able to offer a tighter and more robust lock than is possible with any other product.

Cybersecurity experts agree that application whitelisting is by far the most effective security mechanism on the market, but no one ever bothered to make this technology user-friendly enough for all users, until we created CyberLock. Before CyberLock, all application whitelisting products were active full-time, often when it did not make sense to be active, which most users and Administrators found to be annoying and untenable, so they would choose to forgo application whitelisting altogether. Our patented snapshot technology automatically builds the tiny, customized local whitelist for the end-user, resulting in the smallest possible whitelist and attack surface in the industry.

Antimalware Contextual Engine

Our unique Antimalware Contextual Engine considers the entire attack chain in the parent / child process creation relationship. Not only does this make CyberLock more secure, our mechanism is flexible so that blacklisting vulnerable items globally is not required. For example, CyberLock is not required to blacklist PowerShell globally in order to protect against PowerShell attacks. In other words, CyberLock considers the entire attack chain so that benign scripts that need to execute are able to do so, while blocking malicious PowerShell attacks.

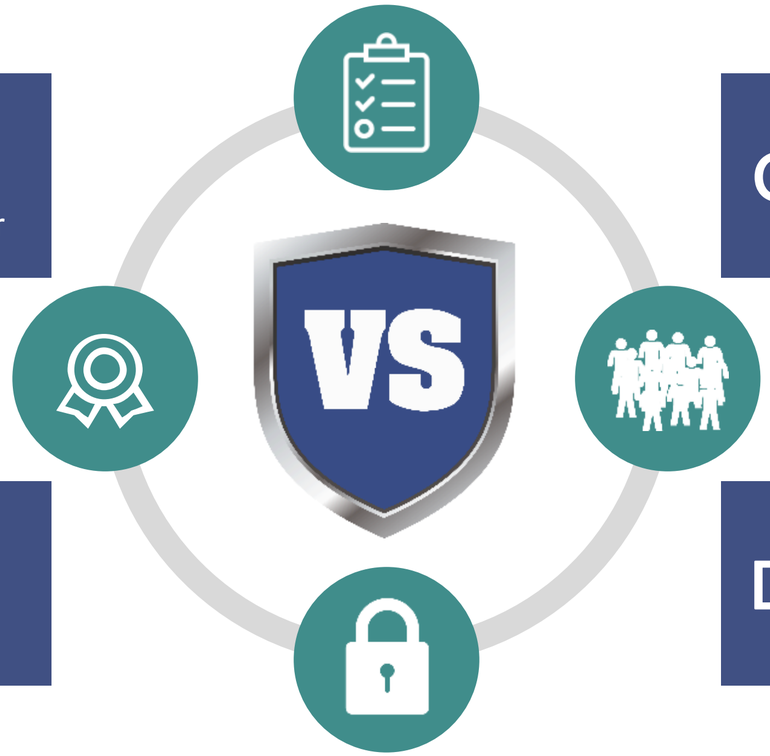
CyberLock includes extremely robust ransomware, script, LOLBins and fileless malware protection capabilities. LOLBins (Living Off the Land Binaries) have become an increasingly common attack vector in the cybersecurity landscape. Other endpoint protection products typically only protect 5-50 vulnerable processes (for example, powershell, cmd, cscript, regsvr32, forfiles, scheduled tasks, bcedit), while CyberLock protects 1,000's of vulnerable processes system wide, all automatically, all with zero configuration.

How CyberLock Is Different

CyberLock is the only solution that…

A Offers dynamic security postures that automatically and safely builds the tiny, customized local whitelist for the end-user

B Automatically creates the smallest, most secure attack surface in the industry



C Is the only deny-by-default product that is user-friendly enough to be adopted by all users

D Keeps the end-user vigilant and aware of emerging threats, makes them feel safe, and provides easy access to the lock

CyberLock's only direct competitors are a class of security products known as "deny-by-default". While there are a handful of deny-by-default products, CyberLock is the only deny-by-default product on the market that was designed and built from the ground up with usability and the user experience in mind.

A Simple Analogy

Nuclear Power Facility

Here is a simple analogy to further explain the significance of Dynamic Security Postures.

When designing physical security, a nuclear power plant will utilize dynamic security postures to properly protect the facility. That is, a high security posture cannot be utilized fulltime because it is too costly and daunting. Likewise, a low security posture cannot be utilized fulltime, as this will result in breaches.

Cybersecurity is no different from physical security in this regard. If a single static security posture is utilized, the system is not optimally protected.

In short, the security posture should match the present threat.

User Experience

User-friendliness is key

We discovered early on, if you are going to lock an endpoint, you have to make the lock user-friendly. That is, you cannot simply lock an endpoint and call it a day, without regard for usability.

One example is Microsoft's User Account Control. Even though end-users quickly adapted to UAC when it was introduced in 2007, it remains difficult for many end-users to utilize PROPERLY. CyberLock is significantly more secure and user-friendly than UAC, and also provides invaluable file insight and user recommendations when blocking a file and displaying a user prompt. In short, if end-users can handle UAC, they can certainly handle CyberLock.

In addition, CyberLock does not force the end-user to respond to dangerous affirmative user prompts, simply because the end-user might inevitably click "Yes". This eliminates the possibility the end-user inadvertently allows an unknown or malicious item.

Instead, CyberLock displays an auto-closing mini prompt before requiring the end-user to make a decision on whether to allow or block a new item, and also provides file insight and user recommendations when asking the end-user to make an Allow or Block decision.

The One Rule of CyberLock

For end-users

When instructing a new user on how to properly use CyberLock, simply explain that CyberLock is a toggling computer lock that automatically locks their computer when they are engaging in risky activities like browsing the web and checking email.

And then explain to the end-user, there is only one rule when using CyberLock…

If CyberLock blocks something you intended to run, you can click Allow if the CyberLock user prompt is blue.

Otherwise, if CyberLock blocks something unexpectedly, simply ignore or close the mini prompt and assume CyberLock was blocking malware.

The Future of Cybersecurity

Adaptive Cybersecurity through Dynamic Security Postures

Cybersecurity has three paths moving forward…

1. Do nothing, maintain the status quo, and continue to rely solely on ineffective allow-by-default technologies. This path will ensure that infection rates continue to rise.

2. Lock the endpoint fulltime with traditional centrally managed application whitelisting. This path has proven time and again to not be a viable option because it is entirely too daunting for end-users and administrators alike.

3. Implement Adaptive Cybersecurity through Dynamic Security Postures with CyberLock and lock the endpoint when the user is engaging in risky activities.

The Future of Cybersecurity

Adaptive Cybersecurity through Dynamic Security Postures

There has been a dangerous trend the last few years in cybersecurity to make endpoint protection as silent as possible to end-users. We believe end-users should become active participants in the fight against malware, and CyberLock is designed to help end-users remain continually aware and vigilant.

ML/Ai, global whitelists and digital signatures are amazing file insight tools to provide to the end-user, but they are not true zero-trust indicators.

Ultimately, the only way to achieve true zero-trust is with a tiny, customized local whitelist that creates the smallest possible attack surface.

Now, just imagine if your favorite traditional or next-gen antivirus / EPP included Dynamic Security Postures that automatically locked the endpoint when it was at risk.