THREATLOCKER

Protecting From the Endpoint Outwards When the Traditional Perimeter Has Vanished

In 2021, the perimeter as we know it has disappeared. We witnessed the acceleration of this process in 2020 as the shift to remote work exploded.

The Disappearance of the Traditional Perimeter

The traditional perimeter operated within a “trusted zone” which relied on firewalls, web filtering, and network filtering for protection.

With devices frequently roaming in and out of the corporate network and connecting to remote environments, businesses must develop a flexible security plan to protect increasingly mobile users.

The Weaponization of Legitimate Software

When an application runs on the endpoint, it has access to all data and information the user can access. Regardless of whether a user is a local administrator or not, applications are given too much privilege.

We have observed a significant increase in malware, ransomware, and the weaponization of legitimate software used in cyber attacks. With the increased risk of exposure at the endpoint, organizations must prioritize better security and **control** at the endpoint.

Organizations commonly adopt basic tools like antivirus and EDR to detect malicious activity. The problem is, threat detection can't distinguish between Dropbox and a piece of malware disguising itself as genuine software. In fact, by the time an attack is discovered, it's usually too late, as the damage has already occurred and data has been compromised.

> **Relying on threat detection to protect against malicious software is like adding multiple smoke alarms and saying we don't need to worry about fire.**
>
> - ThreatLocker CEO, Danny Jenkins

Approach Security with a Zero Trust Default-Deny Mindset

Change the paradigm from trying to block threats with detection to denying all software that isn't explicitly trusted. There are several benefits to this approach, including the mitigation of risks associated with unknown or zero-day malware. Organizations that adopt a default-deny approach don't need to rely on known patterns and definitions, therefore removing the risk of false negatives. Another benefit to this approach is the prevention of shadow-IT which creates a potential back door into a company.

In February of 2021, a water treatment plant in Oldsmar, Florida was hit with a cyberattack. It turns out the cybercriminal weaponized TeamViewer after gaining access to shared credentials to carry out the attack. Once the criminal gained access, they increased the sodium hydroxide levels from 100 parts per million to 11,000 parts per million.

This occurred two days before the Super Bowl which was hosted about 15 miles from the location of the treatment plant. If successful, the cyber attack would have increased the amount of sodium hydroxide to dangerous levels in the local water supply. Ultimately, if TeamViewer hadn't been running on this device, the attack could have been prevented.

Limit What Applications Can Do

All applications have potential vulnerabilities. Between 2020 and 2021, we observed Microsoft Exchange, SolarWinds Orion, Internet Explorer, Zoom, and several other widely used applications hit with a zero-day exploit.

The takeaway is, not only should you control what applications can run, but you should also limit what applications can do once they're running. ThreatLocker gives you the ability to Ringfence™ applications, creating policies around their behavior.

By adding controlled firewall-like boundaries, you effectively stop your applications from interacting with other applications, network resources, registry keys, files, and more. This approach ensures your software cannot step out of its lane and steal your data through malicious behavior.

Ringfencing™ Can Prevent:

- PowerShell gaining untethered access to your files
- Microsoft Exchange communicating with PowerShell
- SolarWinds Orion accessing the internet

Ringfencing™ your applications significantly mitigates the severity of exploits by placing restrictions around how applications can interact with the least privileged at both the user and application level.

Limit Administrator Permissions

While malware doesn't require administrative privileges to swallow your data, encrypt your files, and spread across your network, limiting administrative permissions should play a key role in your cybersecurity risk mitigation plan.

ThreatLocker gives you the ability to control administrative permissions and grant privileges for specific applications, either temporarily or permanently.

This solution provides a simple process of approving, elevating, and controlling applications. The management overhead often associated with application updates is removed since ThreatLocker provides predefined application definitions, preventing any interruptions in day-to-day business.

Adopt a Zero Trust Approach

Zero Trust is a security framework that was developed by Forrester analyst John Kindervagin 2010. This approach has grown to become one of the most popular frameworks in cybersecurity today.

The way in which users operate in the complex IT world is paving the way for zero trust. The traditional security model is no longer compatible in protecting against modern threats.

To adapt, organizations must operate within the framework that no user, network, or device can be trusted by default until proven otherwise. When trust is given, granular policy controls should be enforced.

To learn more about how ThreatLocker helps organizations achieve a Zero Trust strategy, visit www.threatlocker.com

THREATLOCKER