WHAT IS ZERO TRUST?

Zero Trust is a cybersecurity model based on the principle of "never trust, always verify." Unlike traditional security models that assume internal networks are trusted, Zero Trust treats all users, devices, and network traffic as potentially untrusted, regardless of their location within or outside the corporate network. This approach emphasizes strict identity verification, continuous monitoring, and least-privilege access controls. Every request, whether from an internal or external source, is thoroughly authenticated and authorized before being allowed access to any resource. By eliminating implicit trust, Zero Trust helps organizations reduce the risk of data breaches, minimize insider threats, and improve overall security posture. Implementing Zero Trust involves technologies like Multi-Factor Authentication (MFA), micro-segmentation, encryption, and robust access controls to enforce security policies and ensure that only authorized users and devices can access critical data and systems.

RINGFENCING™

Controlling what software can run should be the first line of defense when it comes to better protecting yourself against malicious software. Ringfencing adds a second line of defense for applications that are permitted. First, by defining how applications can interact with each other, and secondly, by controlling what resources applications can access, such as networks, files, and registries. Ringfencing is an invaluable tool in the fight against fileless malware and software exploits.

Protect your data from malicious behavior

- Stop fileless malware and limit damage from application exploits
- Define how applications integrate with other applications
- Stop applications from interacting with other applications, network resources, registry keys, files, and more
- Stop applications from interacting with built-in tools such as PowerShell, Command Prompt and RunDLL
- Stop built-in tools from accessing your file shares

WHAT IS ZERO TRUST?

APPLICATION ALLOWLISTING

Allowlisting has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, Allowlisting puts you in control over what software, scripts, executables, and libraries can run on your endpoints and servers.

This approach not only stops malicious software, but it also stops other unpermitted applications from running. This approach greatly minimizes cyber threats by stopping rogue applications from running on your network.

Block unnecessary executions

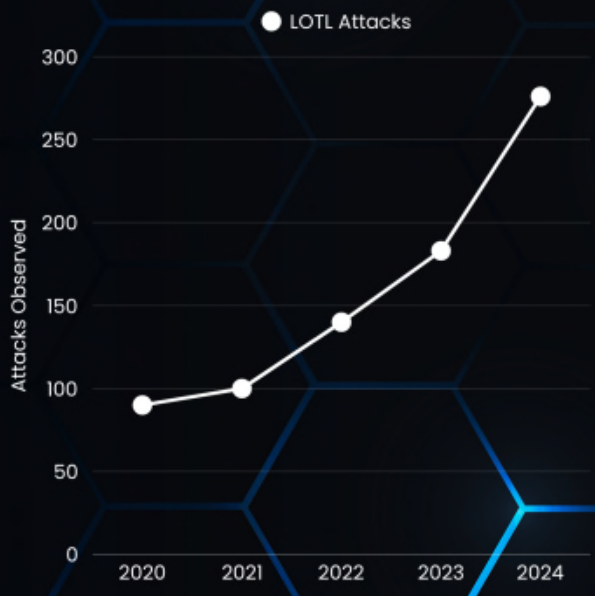
1. Stop any application from running on your machine that is not a part of the allow list.
2. Add firewall-like application policies
3. Add Time-Based Policies
4. Keep up to date with Built-In Applications

WHAT IS ZERO TRUST?

APPLICATION ALLOWLISTING

LOTL Method

In general, it found that attackers are leveraging trusted applications and tools on Windows – a technique commonly known "living off the land" binaries – to conduct discovery on systems and maintain persistence. **Compared to 2023, Sophos observed a 51 percent increase in this tactic, or 83 percent increase over 2021**



WHAT IS ZERO TRUST?

SHADOW IT

Employees introduce new security holes when they download unapproved applications

WHAT IS ZERO TRUST?

Bad Excuses for Allowing Shadow IT

"Employees can use the best tools for their jobs."

"Shadow IT reduces costs when employees use their own tools."

"Business operations streamlined when users implement their own tools instead of waiting for approvals."

STORAGE CONTROL

Storage Control is an advanced storage control solution that protects information. We give you the tools to control the flow and access of data. You can choose what data can be accessed, or copied, and the applications, users, and computers that can access said data. By using storage controls, you are in control of your file servers, USB drives, and your data. Most data protection programs on the market are butcher knife solutions to a problem that requires a scalpel. Blocking USB drives and encrypting data-storage servers can help secure your organization's private data, but these tools don't take into account that this data still needs to be quickly accessible. Waiting for approval or trying to find a device that's allowed to access the needed files can drain hours of productivity.

Choose how your data is accessed

- A full audit of all file access on USB, network, and local hard drives
- Restrict or deny access to external storage, including USB drives, network shares, or other devices
- Approve access for a limited amount of time or permanently
- Restrict access to specific file types, for example only permit access to jpeg files from a camera
- Limit access to a device or file share based on the application
- Enforce or audit the encryption status of USB hard drives and other external storage

WHAT IS ZERO TRUST?

ELEVATION CONTROL

When it comes to adding extra layers of security to your cybersecurity stack, it's important to always add a human layer. Users with admin access are often the weakest link across your network, so their movements must be monitored and tracked. Elevation Controls provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their users, whilst allowing them to run individual applications as an administrator.

Key capabilities of Elevation Control

Complete visibility of administrative rights
- Gives you the ability to approve or deny an individual's administrator access to specific applications within an organization even if the user is not a local administrator

Streamlined permission requests
- Users can request permission to elevate applications and add notes to support their requests

Varied levels of elevation
- Enables you to set durations for how long users are allowed access to specific applications by granting either temporary or permanent access

Secure application integration
- Ensures that once applications are elevated, users cannot jump to infiltrate connected applications within the network

WHAT IS ZERO TRUST?

NETWORK CONTROL

Network Control allows for total control of inbound traffic to your protected devices. Using custom-built policies, you can allow granular access based on IP address or even specific keywords. Unlike a VPN that needs to connect through a central point,

Network Control is a simple connection between server and client. Network Control is built in a way that creates a seamless experience, enabling users to work as normal while eliminating the need for a solution, such as a VPN.

Key capabilities of Network Control

Configurable
- Network Control gives users the ability to configure network access to endpoints using global and granular policies.

Cloud-Based
- The cloud-managed solution provides customers with a centralized view of endpoint policies across your customers.

Dynamic
- Network Control enables users to deny all traffic to published servers while only allowing a single IP address dynamically or even a keyword. This is great for users who travel often.

WHAT IS ZERO TRUST?

NETWORK CONTROL

RDP

Network Encryption

SMB

WHAT IS ZERO TRUST?

GET IN TOUCH

Scott Peterson
Chief Information Security Officer
speterson@cybsolutions.com