THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

NETWORK CONTROL

Zero Trust host-based firewall with dynamic ACLs

Introduction

Discover how ThreatLocker® Network Control fortifies your network security while seamlessly integrating with the full ThreatLocker® Zero Trust Endpoint Protection Platform. ThreatLocker® Network Control delivers:

- **Full visibility and control.**

Monitor and manage inbound and outbound traffic with a centrally managed host-based firewall. Deny all unwanted network connections by default, allow by exception—core to Zero Trust.

- **Granular control.**

Create policies at the computer, group, or organization level.

- **Dynamic protection.**

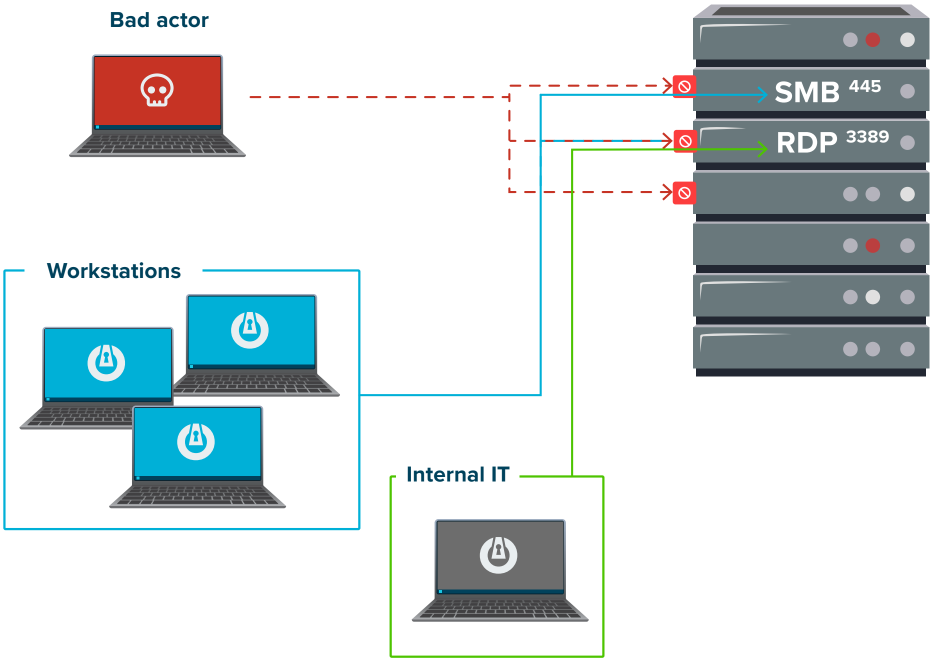
Secure ports with a default-deny policy and traditional static rules for IP addresses and ranges. Then use dynamic Access Control Lists (ACLs) to automatically open and close ports, ensuring only secured and authorized ThreatLocker® devices interact with network resources—a critical step in stopping breaches from unmanaged or unmanageable devices.

- **Advanced filtering.**

Block unwanted outbound traffic by IP, domain, or category—like social media or cloud storage.

- **Seamless integration:**

- Use the ThreatLocker® Access mobile application to automatically update your M365 named locations for use in Conditional Access policies.
- Pair with ThreatLocker® Ringfencing™ for granular application-level network restrictions.
- Enable ThreatLocker® Detect for real-time alerts and actions.



Network Control dynamic ACLs

Dynamic Access Control Lists (ACLs) in ThreatLocker® Network Control enable ports to open and close automatically, allowing only specific permitted devices to access network resources. This blocks unapproved east-west traffic and prevents unauthorized devices from even seeing any open ports during a network scan.

ThreatLocker® dynamic ACLs are authenticated and updated through three main methods. The first two are used when a ThreatLocker® object is used, the last being when a keyword is used.
They are:

- Local challenge
- Cloud-based challenge
- Authorization host

1. Local challenge

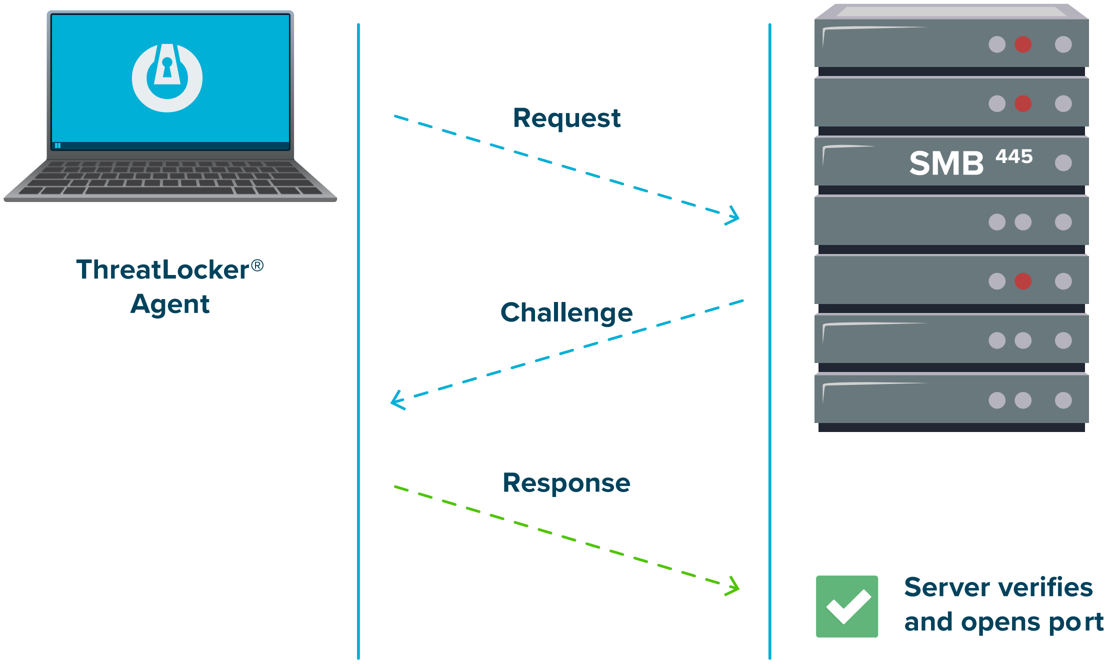
Best for devices on the same network.

I. The computer sends a request to access a port on the server.

II. The server sends a challenge to the computer's challenge port.

III. The computer responds with a valid answer.

IV. The server verifies that the response is correct and opens the port for the computer.



2. Cloud-based challenge:

Ideal for remote work scenarios.

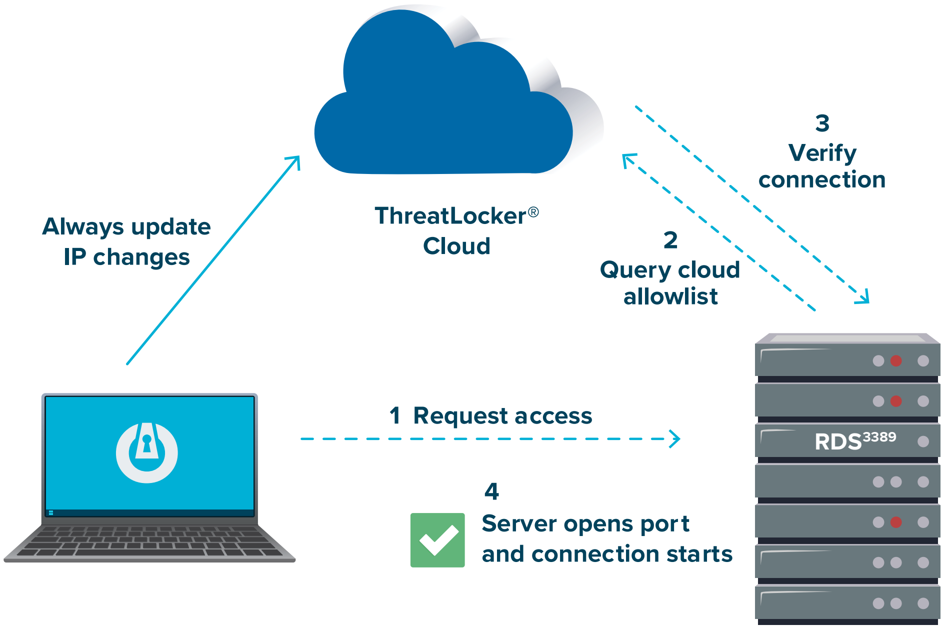
The ThreatLocker®-protected computer informs ThreatLocker® cloud of any IP address changes.

I. The computer sends a request to access a port on the server.

II. The server checks with the ThreatLocker® cloud to see if that IP should be allowed to connect.

III. The ThreatLocker® cloud verifies that the computer's IP address is on the allowlist to connect.

IV. The server opens the requested port for the inbound IP address.



3. Authorization host:

Designed for devices across unconnected ThreatLocker® organizations or if the IP address differs when checking into ThreatLocker® and when connecting to the network resource, such as with a split tunnel VPN.

I. The computer periodically initiates an authentication handshake with each destination server (authorization host) that applies to it.

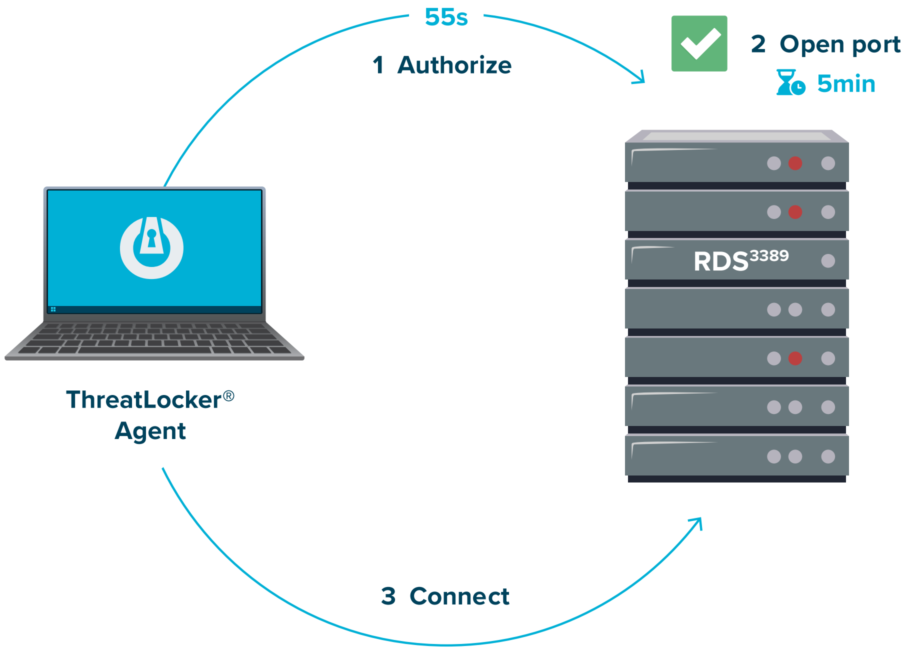
II. Each authorization host responds with a challenge.

III. The computer responds with a pre-shared key (keyword) and the challenge.

IV. The authorization host verifies the response and adds the inbound computer IP address to policies with the pre-shared key.

V. The server opens the authorized port(s) for the IP address with a 5-minute expiration.

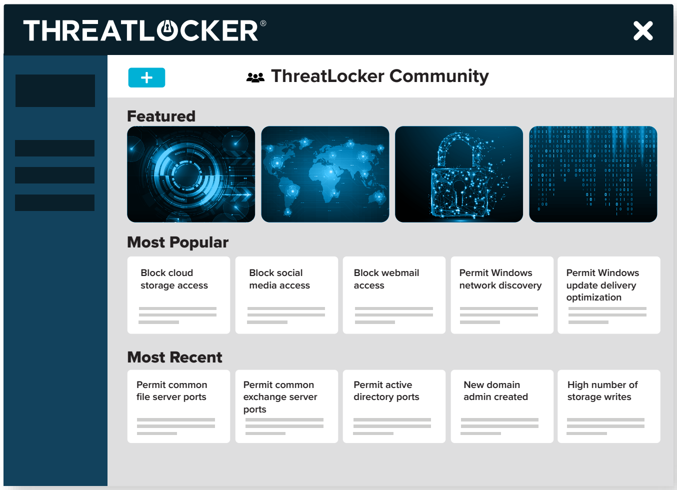
VI. The computer can connect to any server resources that it is pre-authorized to connect to.



Policies

1. Community policies

ThreatLocker® offers pre-configured community policies to quickly secure your environment while permitting necessary connections. These policies allow essential connections, such as common ports for Active Directory (AD) or SQL servers, while blocking access to high-risk websites like file-sharing platforms, social media, and email services.



ThreatLocker Community

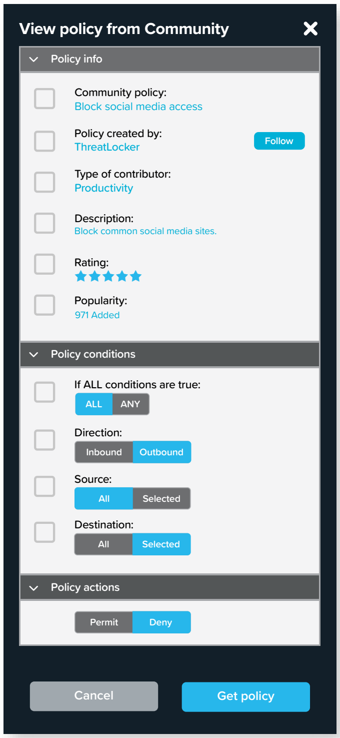
Featured

Most Popular

- Block cloud storage access
- Block social media access
- Block webmail access
- Permit Windows network discovery
- Permit Windows update delivery optimization

Most Recent

- Permit common file server ports
- Permit common exchange server ports
- Permit active directory ports
- New domain admin created
- High number of storage writes



View policy from Community

Policy info

□ Community policy: Block social media access

□ Policy created by: ThreatLocker

□ Type of contributor: Productivity

□ Description: Block common social media sites.

□ Rating: ★★★★★

□ Popularity: 971 Added

Policy conditions

□ If ALL conditions are true: [✓ ALL] ANY

□ Direction: Inbound [✓ Outbound]

□ Source: [✓ All] Selected

□ Destination: All [✓ Selected]

Policy actions

Permit [✓ Deny]

2. Custom policies

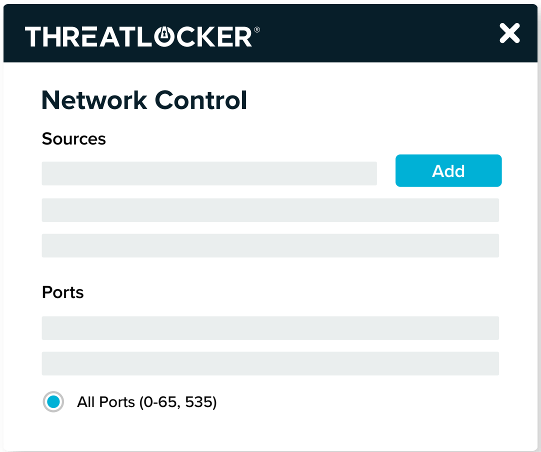
For more precise, granular control, custom policies let you permit specific network connections and enforce a default-deny rule to block unwanted traffic. You can tailor policies for inbound and outbound traffic to apply to objects, keywords, IP addresses (IPv4/IPv6), ports, and tags. You can even restrict outbound connections based on URL content, blocking domains or specific websites.

Object

Objects are items within the ThreatLocker® environment that can be added to a policy for more targeted control. This includes Computers, Groups, or Organizations.

Keyword (pre-shared key)

Keywords act as unique identifiers for authenticating (forward) connections. Like a password, ensure keywords are secure and distinctive to prevent unauthorized access.



● All Ports (0-65, 535)

IPv4

Single IPv4 addresses and CIDR notation IP ranges are accepted.

IPv6

Full and shortened IPv6 addresses, and CIDR notation IP ranges are accepted.

Port(s)

ThreatLocker® has pre-built suggested ports, but you can enter any port(s) for a policy to apply to.

Tag

Tags simplify policy management by grouping multiple items, like IP addresses and domains, under a single identifier. When a tag is updated, all related policies automatically reflect the changes without needing to deploy policies. For example, you can use tags to efficiently manage access to printers or other network resources.

Implementing network microsegmentation

Network microsegmentation divides the network into smaller, controlled sections, limiting access to only what's necessary—Zero Trust for the network. In case of a breach, damage is contained to the affected device, preventing wider exposure.

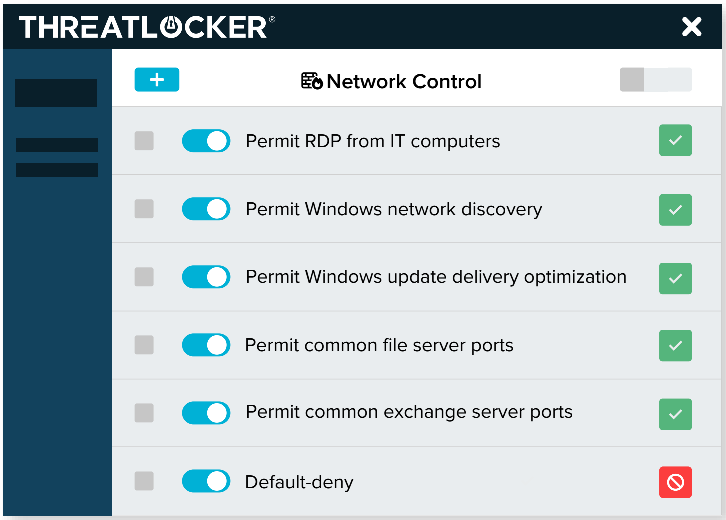
Below is an example of microsegmentation with ThreatLocker® Network Control.

1. Workstation

- Allow inbound RDP access from computers in the IT department.
- Block social media and cloud storage websites with a Community policy.
- Default–deny all other inbound connections.

2. IT administrator

- Block social media and cloud storage websites with a Community policy.
- Default-deny inbound connections.



- Permit RDP from IT computers ✓
- Permit Windows network discovery ✓
- Permit Windows update delivery optimization ✓
- Permit common file server ports ✓
- Permit common exchange server ports ✓
- Default-deny 🚫

3. File server

- Allow inbound SMB access from ThreatLocker®-protected devices in the organization.
- Allow inbound RDP access from computers in the IT department.
- Default-deny all other inbound connections.
- Default-deny outbound connections.

4. Dynamic ACL for Microsoft 365

- Set Conditional Access policies to allow access from named locations only.
- Use the ThreatLocker® Access mobile application to dynamically update named locations by user IP to reduce the dangers of credential theft.

ThreatLocker® platform integration

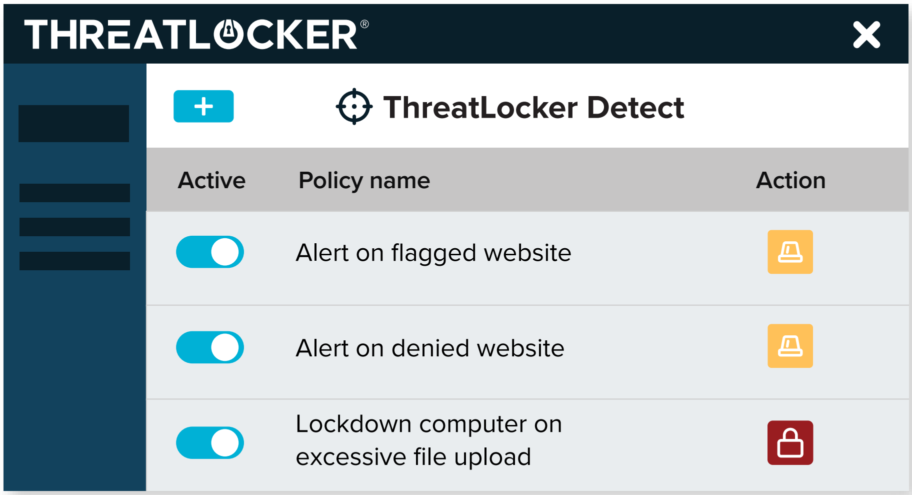
1. ThreatLocker® Detect

- Alert on Network Control policies.

  Example: Get an alert if a user attempts to access a blocked website.

2. ThreatLocker® Ringfencing™

- Apply Application Control with ThreatLocker® Ringfencing™ to limit network access for specific applications. Combined, Network Control and Ringfencing™ ensure only authorized computers and applications can access specific network resources.



Active	Policy name	Action
●	Alert on flagged website	🔔
●	Alert on denied website	🔔
●	Lockdown computer on excessive file upload	🔒