THREATLOCKER®
ZERO TRUST PLATFORM

INTRODUCING THREATLOCKER

# ZERO TRUST NETWORK AND CLOUD ACCESS

# See what ThreatLocker® could do for you

> ThreatLocker was the most intuitive solution we tested. And the responsiveness of the organization—the willingness to engage with us, set up a demo, and work with us on weekly audit reviews—was very good. It's great to have an ongoing relationship with a company that's so responsive to our requests.

**Rob Thackeray, End User Technical Architect**
**Heathrow Airport**

> What we liked about ThreatLocker was how each tool built on the last, allowing us to control exactly how granular we wanted to get with locking down our environment. We had explored other options, but achieving the same level of control would have meant piecing together solutions from multiple vendors. With ThreatLocker, we were able to get everything we needed from one place.

**Jeff Lutes, Executive Vice President of Technology**
**Orlando Magic**

> Before we had ThreatLocker, we had a lot of risk that we just couldn't control. And with ThreatLocker, I think we're doing a much better job of providing a more secure environment for our patients, our doctors, and our manufacturers.

**Greg Gootee, CISO / SVP of Information Security**
**Asembia**

# Secure your network with ThreatLocker®

Confidently ensure that users have access to a consistent and safe network connection.

You can enforce Zero Trust across your entire environment with ThreatLocker.

Offices, remote users, internal servers, and critical services can maintain smooth operations without the need to open inbound ports or deploy traditional VPN solutions.

Your end-users will get the secure and reliable internal system access they need, while avoiding any complex infrastructure changes.

# A streamlined path to network security

With ThreatLocker, you'll have the capability to implement controls that match your users' access requirements safely, with many of them operating beyond traditional perimeters.

Seamlessly shift enforcement to the device-level, cataloging them and setting access parameters to filter through a securely managed server. Without the corresponding IP address, connections will not be made. **Now you will have consistent control across:**

- Office environments
- Remote and traveling users
- Data centers
- Cloud-hosted workloads

Unnecessary network complexity will be avoided while clearly defined access policies are enforced at every endpoint to stop the risks around exposed services. **You define:**

- Which users can connect
- Which approved devices they must use
- Which internal resources are accessible
- Which ports and protocols are permitted
- Optional time-based restrictions
- Device posture

Your approved users will have the capability to work without any day-to-day interruption, but your network stays secure. **Access is now intentional and controlled.**

# How to secure your network with ThreatLocker®

Implementing access policy is straightforward and fully managed from the ThreatLocker portal.

1. **Apply deny-by-default protection**
   You can keep necessary operations unaffected whilst endpoints and servers become enforcement points. Network traffic is allowed only when it matches your defined policies, reducing unnecessary exposure automatically.

2. **Define authorized access pathways**
   Create policies that specify approved users devices or groups and their required internal resources (including Remote Desktop services or internal applications), as well as setting approved ports and time-based access rules.

   Access is then granted only when the user and endpoint are authorized with an access request that matches policy, and the device meets defined security requirements. If a user and device are trusted, access will not be impacted. If not, even correct entry credentials won't matter.

3. **Enable seamless secure remote access**
   When users connect to internal resources, both the endpoint and the server establish secure outbound connections. There is no need to open inbound firewall ports or deploy and maintain a VPN infrastructure.

   Your users can connect as expected, whether they're operating from within the office or remote, while policies ensure access remains controlled and secure.

# Why it matters

**Consistent control across locations**
Security policies follow devices wherever they operate.

**Granular access enforcement**
Define the exact conditions for access and the users that meet them.

**Centralized visibility**
Monitor connections and policy activity across your entire organization from one console.

**Device-level Zero Trust**
Access is granted based on verified devices and defined policies.

## Set the terms for secured access within your network

Ensure policies are enforced, consistently and seamlessly, across your entire organization. With ThreatLocker, you'll have the visibility and control needed to define how your network can safely operate.

# Maintain safe SaaS access across your organization

Deploy ThreatLocker® to ensure access pathways to SaaS resources are kept airtight against phishing attempts.

Keep access to important third-party SaaS services like Salesforce, Asana, and Microsoft 365 running smoothly, but safely, across your organization with ThreatLocker Zero Trust access. You can now enforce a Zero Trust pathway that attackers can't bypass even with the correct credentials.

## Render phishing useless

Ensure valid credentials aren't enough for attackers to steal critical data from your organization. Make informed decisions at the administrative level to tie the pathway between operationally important SaaS resources and authorized devices through a secure, ThreatLocker-managed broker.

With ThreatLocker Zero Trust access, you can contain the impact of attacks like phishing scams and token theft that continue to bypass traditional defenses. Even if correct credentials are intercepted, attackers would still need to use a device that's been cataloged and given permission to use a specific resource to gain access.

## Extend Zero Trust to third-party resources

ThreatLocker enables you to extend Zero Trust beyond applications and into third-party SaaS services by defining which resources are available to user-assigned devices.

Only approved endpoints and mobile devices will be able to use authorized services through a secure broker, managed by ThreatLocker. Explicitly trusted users will have a seamless and consistent user experience and access resources without delay.

While on the attacker side of things, those using an external device will be frustrated in their attempts. **Even if:**

- Credentials are valid
- Multi-factor Authentication (MFA) steps were approved
- A legitimate token was intercepted

# How to apply Zero Trust access across your environment

Implementing secure SaaS access is straightforward and controlled by your IT team.

1. **Broker access through ThreatLocker®**
   All approved devices are configured to connect to designated SaaS services through a secure, ThreatLocker-managed broker.

   This ensures connections originate from a trusted path.

2. **Define authorized devices**
   Your IT team catalogs and identifies which endpoints and mobile devices require access to specific third-party resources.

   Access is granted only when:

- The device is approved through a simple process
- The connection originates from an authorized device
- The request matches defined policy

   You've now defined the secured pathway a user must take to connect, regardless of their credential validity. Once deployed, which takes less than an hour to do, your SaaS applications can be locked down to only your organization's approved secured devices.

3. **Enforce device-level approval**
   New devices must be approved before they can use a specified SaaS resource. Unauthorized hardware cannot silently join your environment or inherit SaaS access.

# Enhanced control and compliance

You will have additional capabilities to strengthen governance and regulatory posture with ThreatLocker:

- **Tag-based policy controls**
  Apply tags directly within policies for granular access enforcement to specific web addresses and services.
- **Portal-approved device registration**
  Require administrator approval before new computers or mobile devices gain access.
- **FIPS-approved routing option**
  Support Federal Information Processing Standards (FIPS) routing for organizations with federal or regulatory requirements.

# Why it matters

**Stop token theft in its tracks**
Even stolen tokens won't give attackers authentication capabilities, so long as their device was not filtered through the ThreatLocker-managed broker.

**Greatly constrict the blast radius from phishing impact**
If a user falls victim to phishing, access attempts from unknown hardware are automatically blocked.

**Set granular device-level permissions**
Define exactly which endpoints and mobile devices can access organizational resources.

**Strengthen compliance posture**
Support regulatory standards while maintaining secure connectivity.

# Secured SaaS access is now in your hands

You define access permission through a secure broker. ThreatLocker empowers your team to maintain key SaaS access for users across your organization, reducing the risks of compromise through stolen or intercepted authentication material.

**About ThreatLocker®**

ThreatLocker is a comprehensive Zero Trust platform that delivers robust cybersecurity for enterprise environments, combining granular policy controls to secure servers and endpoints from unauthorized access.

threatlocker.com