

# Shield OnPremise

Autonomous Network Enforcement for Modern Enterprise Protection

Protect every device on your network with autonomous, reputation-driven enforcement designed to stop malicious and untrusted communications before they become incidents. Shield OnPremise is a transparent inline security platform that protects workstations, servers, IoT devices, OT environments, unmanaged assets, and legacy infrastructure **without requiring software installation on endpoints**. Positioned alongside your existing firewall infrastructure, Shield strengthens organizational security posture by reducing exposure to known and unknown threats across the network.

## Prevention-First Security Built for Modern Threats

Traditional security tools detect threats after activity begins. Shield takes a different approach. Powered by Intrusion's proprietary intelligence platform covering more than **8.5 billion IP addresses**, it continuously evaluates communications in real time using decades of behavioral intelligence.

Known malicious infrastructure is blocked immediately. Unknown and low-reputation destinations are denied by default, reducing exposure to zero-day attacks, ransomware, phishing, C2 activity, and data exfiltration. This prevention-first model extends Zero Trust principles beyond identity and access management directly into network communications.

## Why Organizations Deploy Shield OnPremise

- ◆ **Autonomous Network Enforcement:** Continuously evaluates and blocks malicious or untrusted traffic without manual rule creation or analyst intervention.
- ◆ **Protection Beyond the Firewall:** Reduces malicious traffic before downstream EDR, SIEM, and XDR tools are forced to investigate or respond.
- ◆ **Reputation-Driven Threat Prevention:** Built on 30+ years of intelligence gathering, identifying risky communications rule-based systems frequently miss.
- ◆ **Blocks Unknowns by Default:** Treats unknown destinations as untrusted, closing the gap exploited by newly created attack infrastructure.
- ◆ **Enterprise-Wide Coverage Without Agents:** Protects unmanaged devices, IoT, OT, medical equipment, and legacy infrastructure without endpoint software.
- ◆ **Visibility, Logging & Threat Hunting:** Comprehensive logging of allowed and blocked communications for forensics, compliance, and threat hunting.
- ◆ **Centralized Management & Intelligence:** Intrusion Command Hub delivers centralized reporting, policy management, and AI-powered insights.

## How Shield OnPremise Works

Shield operates transparently inline, continuously evaluating communications against Intrusion's global reputation intelligence platform. Trusted communications proceed normally. Malicious or suspicious communications are blocked before connections establish.

### Blocked communication types include:

- ◆ Command-and-control callbacks
- ◆ Malware downloads

- ◆ Ransomware communications
- ◆ Phishing infrastructure access
- ◆ Data exfiltration attempts
- ◆ Connections to unknown or low-reputation infrastructure

Threat intelligence updates continuously through Intrusion's Global Threat Engine, no constant rule tuning or manual feed management required.

## VERIFY BEFORE TRUST

Shield's zero trust enforcement model protects modern enterprises by controlling every communication — known, unknown, and untrusted.

### Shield OnPremise vs. Traditional Security Approaches

| Capability                                | Shield OnPremise | Traditional IDPS | Next-Gen Firewall |
|---|------------------|------------------|-------------------|
| Autonomous Threat Prevention              | ●                | ○                | ○                 |
| Reputation-Based Enforcement              | ●                | ○                | ○                 |
| Blocks Unknown Infrastructure by Default  | ●                | —                | —                 |
| Zero-Day Communication Prevention         | ●                | —                | —                 |
| Command-and-Control Blocking              | ●                | ○                | ○                 |
| Data Exfiltration Prevention              | ●                | ○                | ○                 |
| Protection for Unmanaged & Legacy Devices | ●                | ○                | ○                 |
| Zero Trust Network Enforcement            | ●                | —                | —                 |
| Continuous Global Reputation Intelligence | ●                | —                | —                 |

● Native Capability ○ Limited Capability — Not Typically Supported

#### About INTRUSION Inc.

INTRUSION Inc. has delivered advanced cyber threat intelligence and prevention technologies for more than 30 years. Leveraging proprietary reputation intelligence built through decades of research and government experience, the Shield platform helps organizations proactively reduce risk through prevention-first security and autonomous network enforcement.

#### Contact Us

888-637-7770

[info@intrusion.com](mailto:info@intrusion.com)

[www.intrusion.com](http://www.intrusion.com)