Intrusion

intrusion.com | 888-637-7770

Shield Endpoint

Autonomous Zero Trust Endpoint Protection for the Modern Workforce

Protect remote users, mobile devices, and distributed workforces with autonomous network enforcement, identity-centric Zero Trust access, and reputation-driven threat prevention. Shield Endpoint extends enterprise-grade protection directly to endpoint devices wherever they operate, including remote environments, unmanaged networks, hybrid workplaces, and cloud-connected infrastructures. Available for **Windows and Android.** Combining Zero Trust networking, autonomous threat prevention, and browser isolation into a unified platform designed to reduce exposure before threats become incidents.

Prevention-First Endpoint Security

Traditional endpoint security solutions often focus on detecting compromise after malicious activity has already begun. Shield Endpoint takes a prevention-first approach by controlling communications before threats can establish persistence, retrieve payloads, exfiltrate data, or communicate externally.

Built on an identity centric Zero Trust overlay architecture powered by NetFoundry technology and enhanced by Intrusion's proprietary threat intelligence platform covering more than **8.5 billion IP addresses**, Shield Endpoint continuously evaluates outbound and inbound communications in real time. Known malicious infrastructure is blocked immediately. Unknown or suspicious destinations can be treated as untrusted by default.

Reduces exposure to:

- Ransomware communications
- Malware delivery infrastructure
- Phishing and credential harvesting
- Command-and-control callbacks
- Data exfiltration attempts
- Zero-day communication channels
- Suspicious and low-reputation infrastructure

Why Organizations Deploy Shield Endpoint

- **Identity-Centric Zero Trust Architecture:** Establishes secure, authenticated communications between devices, users, and authorized resources without exposing services directly to the public internet.
- **Autonomous Reputation-Based Enforcement:** Every communication request is evaluated against Intrusion's continuously updated global reputation intelligence platform to block malicious and untrusted destinations automatically.
- **Protection Beyond the Corporate Perimeter:** Protects users and devices regardless of location, enabling consistent enforcement across remote work environments, hybrid infrastructures, and unmanaged networks.
- **Browser Isolation and Safe Web Access:** The integrated Safe Web Sandbox enables high-risk web content to execute within isolated rendering infrastructure rather than directly on the endpoint device.
- **Outbound Communication Control:** Focuses heavily on controlling outbound communications often associated with modern attacks, including C2 activity, malware callbacks, and unauthorized data transfers.
- **Unified Visibility and Centralized Management:** Intrusion Command Hub provides centralized reporting, AI-powered insights, policy management, and operational visibility across Shield deployments.
- **Lightweight Enterprise Deployment:** Designed for scalable deployment across distributed workforces while minimizing operational overhead and endpoint performance impact.

How Shield Endpoint Works

Shield Endpoint creates a secure Zero Trust communications overlay between endpoint devices and authorized resources. Every connection is authenticated, encrypted, and continuously evaluated against Intrusion's global threat intelligence platform. Trusted communications proceed normally. Malicious, suspicious, or low-reputation destinations are blocked before communications fully establish.

This enables organizations to proactively reduce exposure to threats that rely on outbound connectivity to:

- Retrieve secondary payloads
- Establish persistence
- Communicate with command-and-control infrastructure
- Exfiltrate sensitive data
- Deliver phishing and credential theft campaigns

For high-risk web activity, Safe Web Sandbox technology isolates browsing sessions within secure cloud-rendered environments — allowing users to safely access unfamiliar or suspicious websites while active web content executes outside the local endpoint.

Who Benefits from Shield Endpoint

- **Security Operations Teams:** Reduce alert fatigue and improve operational efficiency through autonomous threat prevention and centralized endpoint visibility.
- **Remote and Hybrid Workforces:** Extend enterprise-grade protection consistently across distributed users and unmanaged network environments.
- **MSPs and MSSPs:** Deliver scalable Zero Trust endpoint protection and centralized management across multi-tenant customer environments.
- **Enterprises Modernizing Zero Trust:** Strengthen identity-centric security architectures with reputation-driven communication enforcement and outbound threat control.

ZERO TRUST. ZERO COMPROMISE.

Shield Endpoint autonomously controls every communication, blocking malicious, unknown, and untrusted destinations before threats can establish persistence or exfiltrate data.

Shield Endpoint vs. Traditional SASE and Zero Trust Clients

Capability	Shield Endpoint	Typical SASE / Zero Trust Clients
Identity-Centric Overlay Architecture	●	○
Reputation-First Autonomous Enforcement	●	○
Unknown Infrastructure Enforcement	●	○
Integrated Browser Isolation	●	○
Autonomous Outbound Communication Control	●	○
Off-Network Endpoint Protection	●	●
Centralized Visibility & Policy Management	●	●

● Native Capability ○ Partial or Policy-Dependent Capability

About INTRUSION Inc.

INTRUSION Inc. delivers advanced cyber threat intelligence and prevention technologies designed to help organizations proactively reduce risk through prevention-first security and autonomous network enforcement. Powered by decades of intelligence gathering and historical reputation analysis, the Shield platform extends protection across on-premises, cloud, and endpoint environments.

Contact Us
888-637-7770
info@intrusion.com
www.intrusion.com