# Triple Protection of User-Controlled Devices from Malicious Actors Through Applied Threat Intelligence

Powered by our Global Threat Engine and integrated with Safe Web Sandbox, **Shield Endpoint** provides zero trust security that enables secured communications with devices in a trusted network and provides safe web browsing and communications with devices that are outside of a trusted network.

## What is Shield Endpoint?

Shield Endpoint is a zero-trust system available for Windows and Android devices that enables enterprises to extend network security and threat protection to users wherever they may be. Shield Endpoint ensures devices only communicate with services in the zero-trust system or services on the Internet, thus stopping ransomware, phishing, malware downloads, command and control, zero-day attacks, data exfiltration, and other elusive threats. The Safe Web Sandbox allows safe web browsing to high-risk websites without fear of bringing malware onto your device.

## Shield Endpoint Differentiators

Shield Endpoint avoids alert fatigue by automatically blocking communications from threats that elude prevention layers, and enables threat hunting and network forensics by logging all communication attempts. It also allows the use of your own cloud-based endpoints while still providing full protection.

Shield Endpoint for Windows offers a browser isolation environment add-on, which allows for the safe viewing of sites that would normally have been blocked. The add-on renders the webpage in a browser in our cloud and displays the contents on the screen, allowing you to interact with it, but without letting any harmful elements touch your computer.

## Unique Value

- Stay ahead of advanced threats with Intrusion's Applied Threat Intelligence that uses over 30 years of internet cataloging and a threat catalog including millions of known malicious domains and IPs
- Verify every device to ensure your network stays protected with a zero-trust network overlay powered by Netfoundry
- Automate onboarding and revocation of authorized users with our Azure Active Directory integration
- Enable threat hunting and forensics with full logging of outbound requests, both blocked and allowed
- Correlate events across devices with reporting for all endpoints on the network through the optional Central Dashboard
- Deploy across thousands of devices with a simplified installation process

**Shield Endpoint** offers advanced features, like dual device and user authentication, to keep your network more secure than other endpoint solutions. Shield will firmly protect your user-controlled devices and can seamlessly be added to an existing security stack.

| Features | Shield Endpoint | Zscaler | Cloudflare ZT |
|---|---|---|---|
| Endpoint Device Protection | ● | ○ | ○ |
| Authenticated Access | ● | ◑ | ◑ |
| Secure Communications | ● | ◑ | ◑ |
| Safe Browsing | ● | ◑ | ◑ |
| Domain Filtering | ● | ◑ | ◑ |
| Phishing Protection | ● | ◑ | ◑ |
| Zero-Day Protection | ◑ | ◑ | ◑ |
| Command & Control Protection | ● | ○ | ○ |
| Anti-Bot Protection | ◑ | ◑ | ◑ |
| Data Exfiltration Protection | ● | ◑ | ◑ |
| Anti-Virus/Malware Protection | ◑ | ○ | ○ |
| On-Device Reconnaissance Protection | ● | ○ | ○ |
| Threat Hunting & Forensics Support | ● | ◑ | ◑ |
| Zero Trust Network Overlay | ● | ● | ● |
| Machine Learning | ● | ● | ● |
| Applied Threat Intelligence | ● | ○ | ○ |

● Full Capability ◑ Some Capability ○ No Capability

## About Intrusion

Leveraging 30 years of expertise, we are committed to protecting companies from digital threats. Our vision is a future where security and connectivity peacefully coexist, leading to a world free from digital harm.

☎ 888-637-7770 intrusion.com