CLOUDFLARE

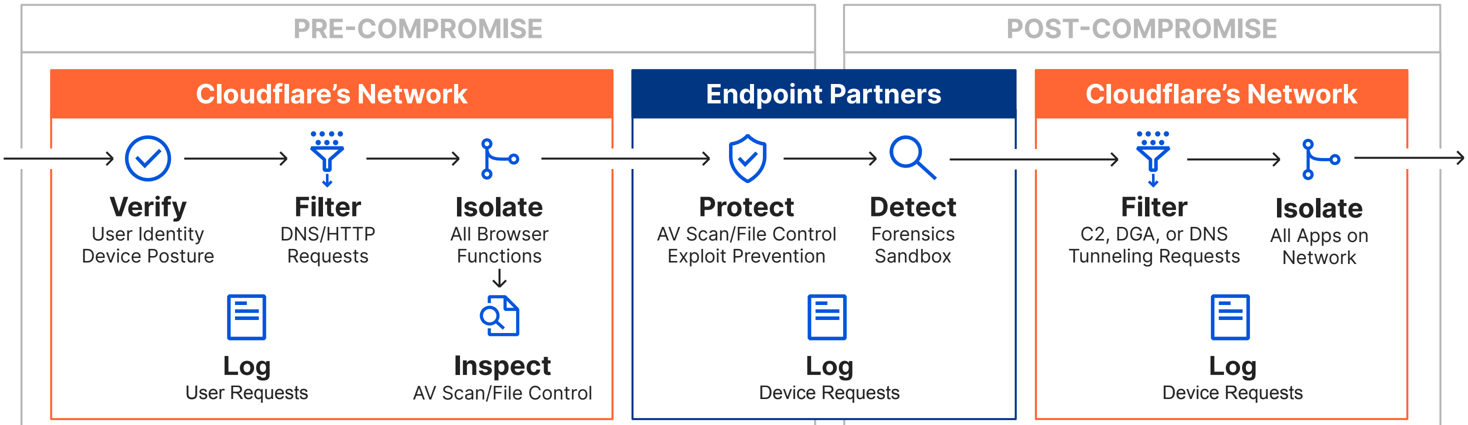
Simpler, more effective threat defense

Malware, phishing, cryptomining, and more attacks will strike. Mitigate the impact.

To keep up with the ever-shifting threat landscape, layering defenses is a best practice, but using too many distinct tools to improve security is not only costly and complex, it trades off performance. Smaller orgs want simpler ways to reduce risk, mid-sized orgs also need more effective responses, and larger orgs also require visibility in one place.

Cloudflare unites many once-distinct security services — even shifting all the endpoint compute that takes place within browsers — into one Zero Trust platform that runs on a massive Anycast edge network. Better threat defense starts with Zero Trust — verifying devices are safely managed before they can connect to corporate resources.

The solution: Integrated threat defense across network and endpoint security



PRE-COMPROMISE

Cloudflare's Network

Verify User Identity Device Posture → **Filter** DNS/HTTP Requests → **Isolate** All Browser Functions ↓ **Inspect** AV Scan/File Control

Log User Requests

Endpoint Partners

Protect AV Scan/File Control Exploit Prevention → **Detect** Forensics Sandbox

Log Device Requests

POST-COMPROMISE

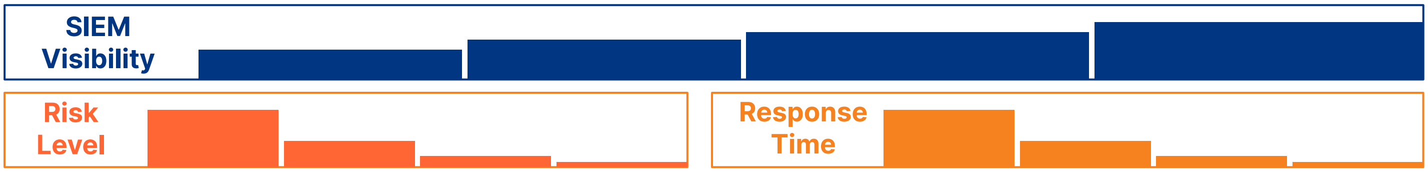
Cloudflare's Network

Filter C2, DGA, or DNS Tunneling Requests → **Isolate** All Apps on Network

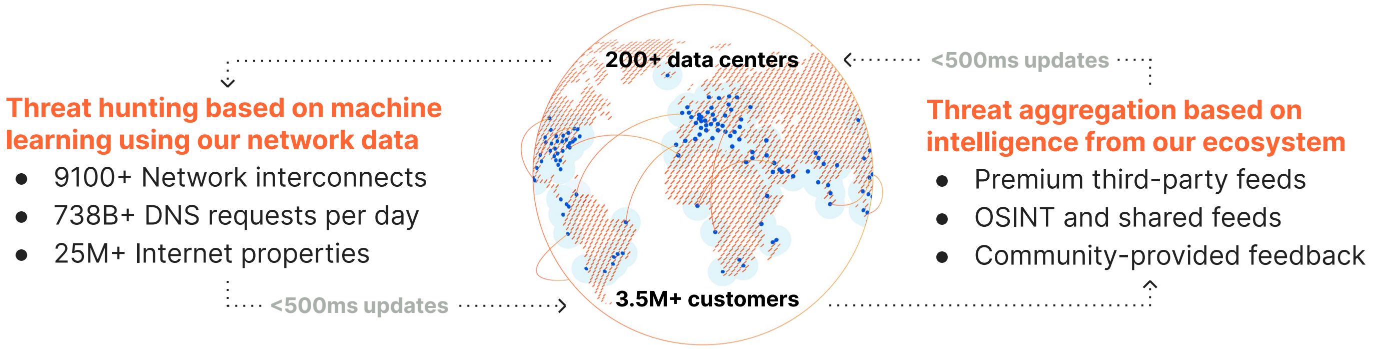
Log Device Requests

Cloudflare filters requests based on our categorization and your lists. Your policy rules will block the traffic over any port and protocol, or isolate browser functions to keep untrusted code away from your devices. Our Zero Trust browser isolation further inspects traffic and user interactions, controlling the types of files that can be accessed with AV scanning when downloads occur. It's easy to push logs into a cloud storage or SIEM platform.

Yet, breaches happen. To contain damage, Cloudflare effectively responds by blocking C2 and other device requests that would exfiltrate data, download a secondary payload, or activate a ransom. Our Zero Trust network access mitigates lateral movement by isolating applications from compromised devices within the network.



Cloudflare One Intel Platform



Threat hunting based on machine learning using our network data

- 9100+ Network interconnects
- 738B+ DNS requests per day
- 25M+ Internet properties

Threat aggregation based on intelligence from our ecosystem

- Premium third-party feeds
- OSINT and shared feeds
- Community-provided feedback

Security risk categories to block or isolate per policy rule	Malware Phishing Cryptomining	Newly seen domains New domains Unreachable domains	C2 & botnet DGA domains DNS tunneling	Spyware Spam Anonymizer

Cloudflare's intel effectively blocks known and emerging threats due to our network data and ecosystem.

Yet, no matter how ...

- many threat hunters or threat feeds a vendor has,
- much data or machine learning is used, and
- often intelligence is updated or fast it is enforced

... filters and inspections fail to block 100% of threats.

And your security teams cannot block all sites that pose some risk to your org without disrupting employees, which may cost more in lost in productivity and IT ticket handling than the resulting damage from a threat.

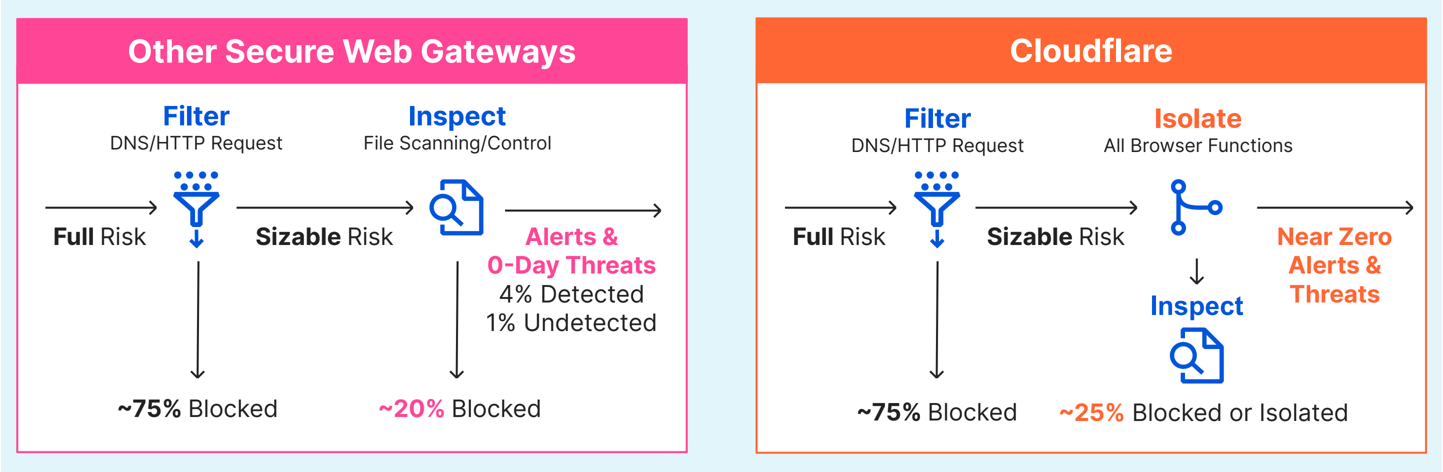
That is why you need a Zero Trust approach to Internet browsing. Cloudflare Browser Isolation is ...

- **Lightning-fast with a flawless user experience,**
- **and cost-effective to use for all unblocked sites:**

Uncategorized	Risky	Low-Risk

Coming soon:

- Inspect and control data in use, not just in transit.
- Specify where to store downloaded files.
- Prevent credentials from being entered into forms.



Contact us today to request access to an enterprise plan account of Cloudflare for Teams.