

//adamnet.works

reflex AI

adaptive AI

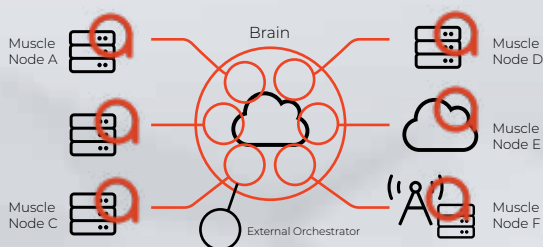
DTS  
don't talk to strangers

# adam:ONE®

Next Generation **ZTc** SASE

**Proactively deny connections of all potential threats while intelligently remaining connected to all that is good and necessary.**

- **Neutralize Ransomware, Zero Days & Evasion Threats** BEFORE detection.
- **Exfiltration of Classified Data & IP theft stopped** BEFORE attacks can execute.
- **Phishing Vector Closed by default.** Effectively mitigate the Human Factor.
- **IoT | IIoT | MIoT | OT | ICS | CI protected.** No agent required.
- **Sovereign Data Custody.** Decentralized resilience.
- **Resolve Shadow IT.** Automatic Device Quarantine. Full Layer2 Visibility.
- **M-22-09 easily fulfilled** across all devices and environments with minimal disruption.



## How adam:ONE® works

At the core, adam:ONE® is a highly optimized DNS caching resolver that lives on top of a firewall engine in a Muscle - Brain hybrid configuration: Gaining the resilience of a distributed deployment and the benefit of centralized control. Out-of-band protection means its protection is applicable to all types of devices including OT, IoT and IT with no endpoint agent required. The Muscle can be applied to a flexible edge on-premise or in-cloud at any point between the endpoint and its connection to the Universal Threat Ecosystem (a.k.a.: the Internet). A cloud controller (Brain) is used for orchestration and controls.

1. Starting in a Default-Deny-All state, by the use of aggregated intelligence merged with AI driven dynamic allowlisting, a dynamic policy is written as a device needs to access verified connections to web services.
2. To be able to use DNS as a functional root of trust, it enforces our patented technology called Don't Talk to Strangers (DTS)® that denies all IP connections by default, unless first requested by DNS and allowed by the dynamic policy.
3. If allowed by policy, it opens a hole to establish the verified connection, and then collapses it as soon as the connection expires.

Allowed connections are cross-checked by DNSHarmony® aggregation of protective DNS resolvers of your choice. This aggregates threat intelligence in real-time for enhanced performance and creates resilience beyond the standard single resolver set.



The net result: **Zero Trust connectivity for any device requesting connection through adam:ONE®.**  
**ZT protection invisible to the user.**



[contact@adamnet.works](mailto:contact@adamnet.works)

For more information  
on adam:ONE® and ZTc:  
<https://adamnet.works>



**Reduce your Attack Surface 7000:1.**

All items © 2024; Adam Networks LLC. All trademarks are the property of their respective owners.