ADAMnetworks Technology Stack Technical Brief

Version 20250423

adam:ONE®

ADAMnetworks® security stack is a technology ecosystem that allows multiple technology elements to function together. The foundation is adam:ONE® - composed of DNSharmony®, Don't Talk To Strangers (DTTS)®, AdaptiveAI™ and ReflexAI™. The solution is categorized in the Secure Access Service Edge (SASE) space. adam:ONE® has multiple deployment models - from a transparent mode in the network, without the need to displace any current technology, to providing full endpoint layer 2 visibility by displacing current internal layer 3 devices.

The adam:ONE® dashboard is a cloud based portal and API where all policy configuration and assignments are managed. The dashboard is multi-tenant so multiple networks and sites can be handled from a single pane of glass.

Features include:

- Smart Rollout - provides low-to-no business disruption deployment.
- Agentless - no endpoint agents required.
- Multi-tenant, multi-site, multi-network dashboard with single pane of glass for all networks and sites running adam:ONE®.
- Automatic device inventory via layer 2 visibility or AD/LDAP integration.
- Active Directory/LDAP integration - provides policies that are based on AD groups and Users.
- Unlimited Per Device Policy creation and assignment.
- Unlimited Per User Policy creation and assignment when used with 802.1X authentication.
- Unlimited Per VLAN/Subnet Policy creation and assignment.
- "Holding Tank" quarantine policy to enforce device quarantine when needed.
- Sovereign Data Custody - no MiTM (miscreant-in-the-middle) decryption required, the enterprise retains full ownership and custody of its unmodified data during transit.
- Network Segmentation achieved via Policies .
- Aggregated real-time DNS threat Intelligence via DNSharmony®.
- Leak-proof DNS (using DNS as root-of-trust) via Don't Talk To Stranger (DTTS)®.
- AI powered Dynamic Allow-listing via AdaptiveAI™ and ReflexAI™.
- Mobile or multi-homed devices protected via adam:GO™ and adam:OSN™.
- Cellular Networks protected via adam:APN™.

adam:ONE® Architecture

Using an on-premise gateway-hosted client (the "muscle") which receives its configuration continuously from a centralized cloud controller (the "brain"), resilience and local performance are simultaneously optimized. DNS queries and answers are channeled to be in geographic proximity to the endpoint and all network traffic decisions are made locally. The muscle can be deployed as a physical appliance, a virtual appliance or as a container.

DNSharmony®

Domain-based reputation systems and DNS threat intelligence sources are readily available both commercially and free/open source. The best DNS threat intelligence source is an aggregation of all of the available sources in a given environment. This is what DNSharmony® is designed to do.

Features include:

- Aggregated DNS threat intelligence out of the box to open source feeds including Cloudflare, Quad9, Clean Browsing, ADguard and more.
- Integration of commercial feeds such as Infloblox and Umbrella available.
- Provides DNS redundancy by default in the case one or more feeds become unavailable.
- Works in conjunction with other DNS servers or can be used as the DNS server for the enterprise.
- Resolver of last resort / Continuous domain validation - provides a final check for all outbound DNS connections when used with ReflexAI™/AdaptiveAI™ Dynamic Allowlisting to ensure a domain hasn't gone "bad".

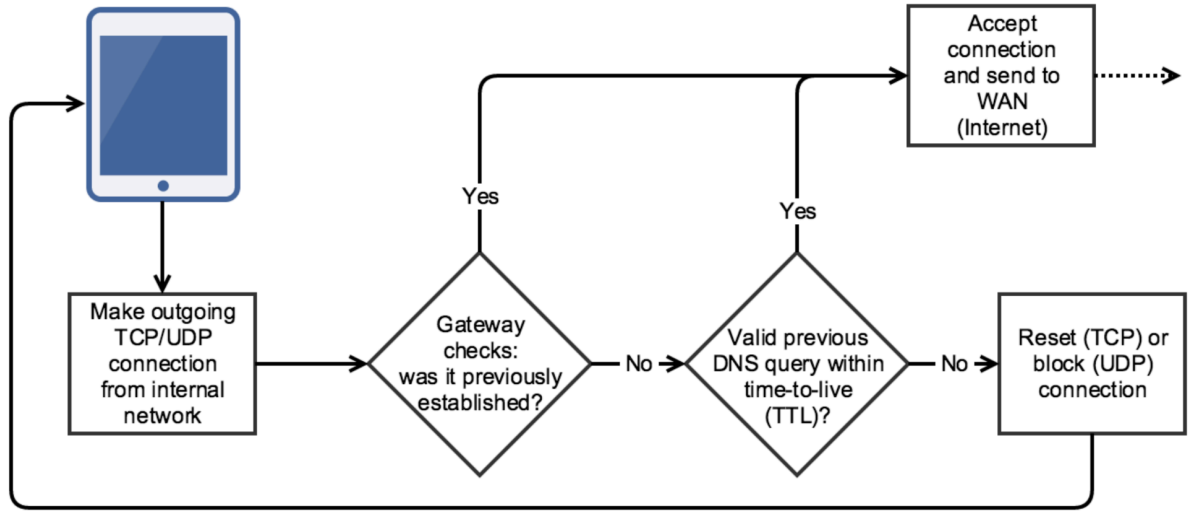
Don't Talk To Strangers (DTTS)®

A stranger in this context is an IP address that has not been resolved or discovered via a permitted DNS query or any form of DNSless traffic. DTTS® is a patented technology which enforces DNS as the root of trust unless the traffic is permitted by policy using an Enabler. Enablers are configurable sets of protocols, ports and IP address(es)/FQDNs thereby allowing the enterprise to shape the type of DNSless traffic it requires while maintaining complete control over outbound connections. DTTS® brings a true proactive approach to Command and Control (C2) connections by simply denying any of these by default. Incidentally, this approach is being formalized via an rfc draft with industry partners, for IETF submission in 2025.

Features include:

- Granular control over IP-to-IP connections and DNSless traffic.
- DTTS® Learning mode - ability to see what would have been blocked had DTTS® been enabled to ensure a non disruptive deployment.
- Verified Enablers for well known applications such as Whatsapp and Apple Services out of the box and maintained by ADAMnetworks®.
- Custom Enablers allow the enterprise to build their own enablers for in house and 3rd party applications.

DTTS® Architecture



AI Powered Dynamic Allow-listing

adam:ONE® utilizes AI/ML engines to power dynamic Allow-listing. This overcomes the issue of maintaining a static white list and allows adam:ONE® to commit to the “Never trust, always verify” zero trust approach to network connections without disrupting business operations. Multiple different approaches in Allow-listing enables a policy to match the role of a user or device.

Fixed rule(s) policy

Using pre-made lists or by observation, a collection of required internet domains and/or FQDNs are established as an allow-list. Fixed rule(s) policies are typically used for Active Directory Controllers, File/Application Servers, Web Servers, IoT Devices, Printers/Scanners.

Features include:

- Fixed domain traffic to only allowed resources.
- No circumvention even if the asset is compromised.

AdaptiveAI™

AdaptiveAI™ takes a learning mode approach over 30 to 90 days on a per site or per network basis and dynamically adds domains as requested by the user(s). In Incident Response cases the learning phase can be skipped to move to full ZTc posture as part of the response and remediation effort to create immediate radio silence to C2 or arrest potential data exfiltration.

Each request passes through a cloud-based sandbox testing and AI inspection which deems whether it is safe for work or not. In the process all “dependencies” for additional domains required for the online service are gathered and tested against the inspection service as well. Only the domains that are deemed safe would then be added to the dynamic allowlist from all the discovered dependencies. AdaptiveAI™ provides a mechanism for the enterprise to tightly define the “Internet” for users while allowing the user to dynamically request additional domains as needed. This policy engine is recommended where the User’s role is very defined such as Accounting departments or High Value Assets such as the C suite.

Feature include:

- Strict shaping of the internet - phishing is mitigated as only allowed domains are able to connect.
- Attacks where traffic is redirected midstream is blocked by default as adam:ONE® vets all destinations prior to the user being able to connect.
- Dynamically added domains must pass through the cloud sandbox, AI testing and can be held for human inspection prior to being allowed.

ReflexAI™

ReflexAI™ is a dynamic allow-listing engine where 82 domain categories/tags are sorted into 5 decision buckets to allow customization of the final decision outcomes. : Always Block, Block, Review, Allow, Always Allow. In addition to creating custom policies, the decision engine also facilitates customizable conflict resolution when collisions between allowed, blocked or send to human inspection occur on multi-category domains. These domain categories are both ADAMnetworks® specific and 3rd party sourced. Sorting the categories into these buckets is customizable and multiple ReflexAI™ policies can be built in this manner as needed by the enterprise. The AI/ML engine is used for conflict resolution and has 3 decision levels: Permissive, Hold for Human, Protective. ReflexAI™ requires no learning time as dynamic allow-lists are created in real-time within user space with no disruption to the end user.

Features include:

- User transparent protection - blocks will only occur if the user is trying to connect to a domain that is outside of the parameters set by the enterprise.
- Proactive defense against phishing and redirect attacks - similar to AdaptiveAI™, all destinations are validated prior to the user being allowed to connect.

- Domain Categorization allows the enterprise to shape the Internet for their end users - Appropriate Use Policies are enforceable.
- Domains which are “uncategorized” and generally unknown are denied by default - the connection fails closed.

adam:ONE® Summary

Combining any of the above policy engines with DTTS® brings devices into a Zero Trust connectivity (ZTc)™state. A device in a ZTc™ state is proactively protected with true proactive egress control against any malicious outbound connections such as what is used by C2 beacons or data exfiltration. Users of ZTc hardened devices are proactively protected against phishing attacks. Even if the user makes the mistake of clicking on the malicious link, the default deny-all state of the device will refuse the connection to be made - unless verified and allowed by policy.
A network which is governed by ZTc™ policies allows only verified good destinations rather than constantly spending resources on the attempt to detect an indication of compromise or reactively terminate a connection to a known malicious destination which could only happen after a victim was identified to submit the destination to an intelligence source.

adam:GO®

adam:GO® is a technology stack available for Windows OS, iOS, iPadOs, Mac OS, Chrome OS and Android OS designed for the protection of mobile or other multi-homed devices.
adam:GO™ can be distributed via an UEM (EMM/MDM) enforced VPN which gives the same level of security as devices which are behind adam:ONE® on the enterprise network.
adam:GO® can be used as a back-to-base connection to the on-premise adam:ONE® at the enterprise or in association with an adam:ONE® cloud exit point(s) in different geographical locations.

Features include:

- UEM (EMM/MDM) agnostic solution.
- OS agnostic: Windows 10+, Android 9+, iOS/iPadOS 16+, ChromeOS 110+.
- Unified policy creation in the adam:ONE® dashboard.
- Device protection regardless of the network used to connect to the Internet.
- Circumvention protection - unauthorized DoH, DoT, Proxies and other methods are denied by default and replaced by internal DoH element that can be pointed to any DoH upstream resolver set of the administrator’s choice.
- DTTS® functionality on mobile devices is the same as on enterprise network devices.
- Various VPN modes supported via MDM enforcement: lodVPN (Locked on demand), odVPN (On demand), aoVPN (Always On VPN).

adam:OSN™

Operating System Native (adam:OSN)™ implementation is a ZTc stack for mobile devices which brings the perimeter edge onto the device. Currently there are two deployment types: Apple iOS and Windows OS.

adam:OSN™ for iOS & iPadOS

The adam:OSN™ app is designed to provide adam:ONE® with DTTS® implementation natively on iOS. It leverages iOS SDK providers to perform system-wide network filtering by intercepting all socket and DNS queries and applying a set of rules defined by the policy that is used on the device, eliminating the need for VPN or local gateways. This setup enhances network management and security at the system level with defined sandbox restrictions for user's privacy.

The adam:OSN application utilizes the iOS Network Extension framework to perform system-wide network filtering.
iOS Specifications

- iOS Version - Minimum iOS 16 or later.
- Supervised Mode - The device must be in supervised mode. Supervised mode is essential for enabling Content Filter Providers and enforcing DTTS logic.
- MDM Configuration - Used to upload the configuration profile necessary for filtering and policy enforcement.
- Initial Network Requirements - Stable network connectivity is required during the initial setup.
- Post-Configuration - After successful setup, the app can function without stable network connectivity, using adam:ONE® with DTTS for Internet connections.

adam:OSN™ for Windows OS (in development)

adam:OSN on Windows performs packet filtering locally on an endpoint machine. It does so by hooking into the filter engine using the Windows Filtering Platform (WFP) API and returning block/permit decisions. Because all filtering is done locally, blocked packets are discarded before they ever leave the machine.

adam:OSN Windows is composed of two parts, one in kernel mode and other in user mode.

- A WFP callout driver (**kernel mode**). The driver hooks into the filter engine by adding filters to it. All traffic that matches the filters are passed to the driver, where it must then make a block/permit/continue decision. The driver does so by queuing the packets, passing relevant info about the packets to the userspace app (where the decision is made), and then applying the verdict it subsequently receives.
- A userspace application (**user mode**). This app has the ability to dynamically start the driver as a service (no need to install the driver as a separate step). Once filtering has

started in the driver, the app begins to read DNS packet information, determines whether the packet should be allowed, and returns a verdict to the driver.

Technical requirements and any other specs.

- Windows 11.
- Administrative privileges are required to install the driver.
- Deployment via MDM (optional).

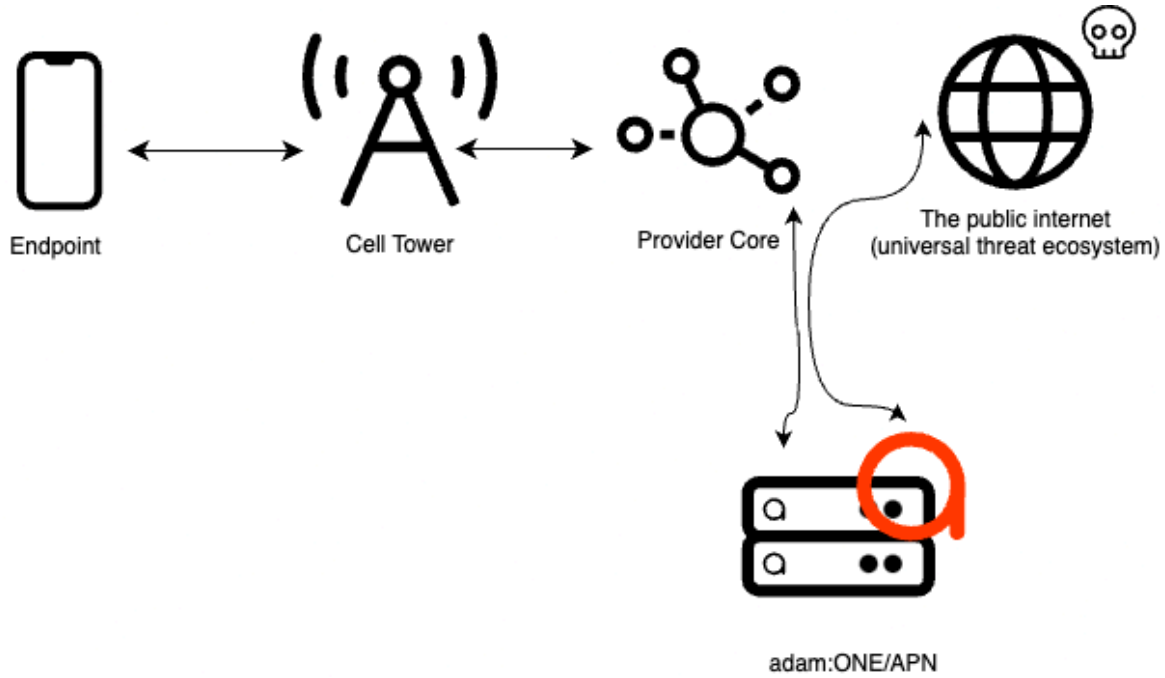
Features for both versions include:

- ZTc functionality without a VPN.
- Unified policy creation in the adam:ONE® dashboard.
- Device protection regardless of the network used for internet connectivity.
- Circumvention protection - non-adam:OSN™ DoH/DoT, Proxies and other methods are denied by default.
- DTTS® functionality native to the OS on the device.

adam:APN™

For devices on cellular networks, the provider traditionally assigns network functionality including DNS servers to use, with very little flexibility. Outside of some potential MDM payloads to modify the DNS client-side behaviour, the options are limited.

For cellular providers offering a custom Access Point Name (APN), adam:ONE can be provisioned to deliver adam:APN services to any/all cellular endpoints using said APN:



Requirements for adam:APN

In order to deploy adam:APN, the following requirements must be met:

- Cellular provider must offer a custom APN option (e.g. att.com and rogers.com offer such services to SMB and Enterprise customers).
- Cellular provider must offer network routing details, including BGP details and provisioning support.
- Cellular customer must have one or more methods of applying custom APN to the endpoint, such as pre-provisioned SIM/eSIM or a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) platform for devices such as smartphones.
- Cellular provider must provide physical or virtual capacity to deploy size-appropriate hardware that can run VyOS 1.4 or later and be remotely accessible for deployment by ADAMnetworks/LTP.
- Cellular provider must allow for a minimum of two (2) appliances for High Availability purposes.
- ZTc SMB or ZTc Enterprise plans required for each appliance, virtual or physical.
- Environment must be supported by a Licensed Technology Partner in good standing with ADAMnetworks.