Security at speed and scale:

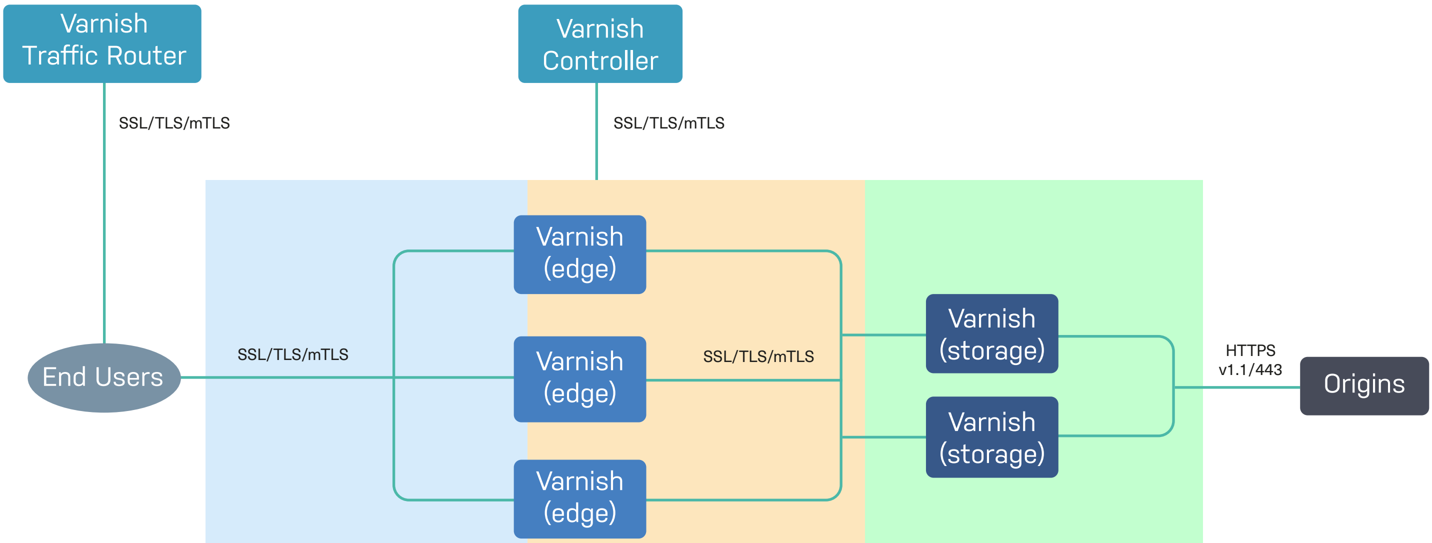
Protecting content delivery operations with Varnish

Varnish Enterprise is content delivery software for web and video services that need speed and scale in order to offer reliable Quality of Experience to large audiences.

These services also face many security threats, from cache poisoning and SQL injection to on-path attacks, malicious API requests and DDoS attacks.

It is a significant challenge to secure content delivery without adding bottlenecks or performance setbacks, but with tools like built-in TLS, Varnish Enterprise secures networks while enabling high-performance content distribution.

Encrypt customer data end-to-end | Protect critical infrastructure | Block bad traffic
Stay online during CDN outages | Introduce Zero Trust security



Edge security

Access tier

- Client-side TLS (External TLS terminator or built-in)
- mTLS
- TLS cipher/protocol logging and statistics

Cache security

Application tier

- Data-at-rest encryption
- Backend-side TLS (built-in)/ mTLS
- JWT verification
- HMAC verification
- GeoIP blocking
- Bot detection
- Request/response allowlisting
- Access Control Lists
- Traffic inspection/ monitoring
- Header/cookie allowlisting

Origin security

Data tier

- Web Application Firewall
- DDoS protection
- Origin shield
- Rate limiting
- Request blocking
- HTTPS v1.1 / 443

Data Privacy / Sovereignty • Dedicated infrastructure • Custom PoP locations

Edge Security

Client-side TLS

External TLS terminator and in-process TLS authentication options.

mTLS

Two-way TLS authentication often used in Zero Trust security frameworks

TLS logging and statistics

Log TLS data for access logging, metrics and data-driven decision making for cipher selection.

Cache Security

Data-at-rest encryption

Encrypt content, response headers and response bodies in cache, and decrypt on delivery

Backend-side TLS (built-in) / mTLS

Secure communication between tiers of Varnish caches

JWT verification

JSON Web Token verification on per-transaction basis

HMAC verification

HMAC Token verification on a per-transaction basis

GeoIP blocking

Integrated IP intelligence for location-specific content delivery and blocking

Bot detection

Forward Confirmed reverse DNS for bot verification and domain-based access control

Request / response allowlisting

Only defined request parameters are kept; all others provided by the client are removed on the fly

Access Control Lists

Identify clients in specific IP ranges to separate in-network clients from out-of-network clients

Traffic inspection / monitoring

Inspect each request and accept or deny based on risk determination

Header / cookie allowlisting

Only defined cookies and headers are kept; all others are removed on the fly to mitigate cache poisoning

Origin Security

DDoS protection

Checks request body to mark potentially dangerous requests

Rate limiting

API to slow down the speed of incoming requests

Request blocking

Specific requests can be blocked if the rate limit threshold is reached

HTTPS v1.1 / 443

Secure communication between Varnish and backend

Web Application Firewall

Integration with ModSecurity to protect against application vulnerabilities like SQL injection

Origin shield

Protect backend from traffic spikes and maintain uptime during CDN outages

Find out more

www.varnish-software.com

info@varnish-software.com