

---

# Technical Platform Documentation

Architecture, Threat Intelligence Pipeline,  
API Reference & Product Specifications

---

| VERSION             | CLASSIFICATION           | AUDIENCE                                     |
|---------------------|--------------------------|----------------------------------------------|
| 2.1 — February 2026 | Restricted / Partner NDA | Security Engineers, IT Architects, SOC Teams |

5 Greenwich View Place, London, E14 9NN, United Kingdom  
Company No. 11150273 · VAT GB305742714 · DUNS 223612138  
[onefirewall.com](https://onefirewall.com) · [docs.onefirewall.com](https://docs.onefirewall.com) · [support@onefirewall.com](mailto:support@onefirewall.com)

# Table of Contents

---

|                                   |           |
|-----------------------------------|-----------|
| <b>1. Platform Overview</b>       | <b>3</b>  |
| 1.1 What OneFirewall Is           | 3         |
| 1.2 Alliance Model                | 3         |
| 1.3 Key Metrics                   | 3         |
| <b>2. Architecture</b>            | <b>4</b>  |
| 2.1 Pipeline Stages               | 4         |
| 2.2 Data Flow                     | 4         |
| 2.3 Distribution Layer            | 5         |
| <b>3. Threat Intelligence</b>     | <b>5</b>  |
| 3.1 Indicator Types               | 5         |
| 3.2 Crime Score                   | 5         |
| 3.3 STIX 2.1 / TAXII 2.1          | 6         |
| 3.4 Alliance Intelligence Sources | 6         |
| <b>4. WCF Agent</b>               | <b>7</b>  |
| 4.1 Function                      | 7         |
| 4.2 Supported Platforms (166+)    | 7         |
| 4.3 Deployment Modes              | 7         |
| 4.4 System Requirements           | 8         |
| <b>5. API Reference</b>           | <b>8</b>  |
| 5.1 Authentication                | 8         |
| 5.2 Endpoints                     | 8         |
| 5.3 Response Format               | 9         |
| <b>6. Product Catalog</b>         | <b>10</b> |
| 6.1 CTI Feed & Platform           | 10        |
| 6.2 OneDevice Hardware Appliance  | 10        |

|                                        |    |
|----------------------------------------|----|
| 6.3 OFA Mobile                         | 11 |
| 6.4 Secure DNS                         | 11 |
| 6.5 WAF                                | 11 |
| 6.6 ClosedVPN                          | 12 |
| 6.7 AI Gateway                         | 12 |
| 7. Security & Compliance               | 12 |
| 8. Pricing Model                       | 13 |
| 9. Integration Quick-Start             | 13 |
| Appendix A — Supported Platform Matrix | 14 |

# 1. Platform Overview

---

## 1.1 What OneFirewall Is

OneFirewall Alliance is a Cyber Threat Intelligence (CTI) platform that operates as a crowd-sourced indicator-sharing network. Members — spanning enterprises, government agencies, Telcos, and critical infrastructure operators — submit vetted threat indicators observed in live production environments. Those indicators are validated, enriched, scored, and redistributed in real time to all connected members as enforceable block-lists.

The core differentiator is the origin of the data: indicators are drawn from active detections in highly sensitive environments (ministries, national Telcos, banks, critical infrastructure) rather than from public feeds alone. This gives members access to threat data that rarely reaches conventional commercial circuits, and to do so before attacks propagate at scale.

The WCF (Web Content Filter) Agent translates the intelligence into enforcement policies on existing firewall and IPS infrastructure, requiring no replacement of current security hardware.

## 1.2 Alliance Model

Members contribute and consume in a reciprocal model. Each member organisation running the WCF Agent automatically contributes anonymised indicators it observes locally. Contributions are validated against the alliance corpus before acceptance, preventing injection of false positives or poisoned data. Consuming members receive the consolidated, enriched feed. The platform enforces a contributor threshold to ensure reciprocity.

**Key principle:** An attacker targeting one alliance member is automatically blocked by all others within the same distribution cycle — typically under 200ms from submission to enforcement.

## 1.3 Key Metrics

|                                 |                                  |                                    |                                     |                                  |
|---------------------------------|----------------------------------|------------------------------------|-------------------------------------|----------------------------------|
| <b>180+</b><br>Alliance Members | <b>&lt;200ms</b><br>Sync Latency | <b>166+</b><br>Supported Platforms | <b>12</b><br>Contributing Countries | <b>Real-Time</b><br>Feed Updates |
|---------------------------------|----------------------------------|------------------------------------|-------------------------------------|----------------------------------|

IoC counts per country (illustrative real-time sample): Italy 412,800 · UK 287,400 · USA 524,100 · Germany 276,500 · France 231,800 · Brazil 204,700 · Spain 198,600 · UAE 167,900 · Holland 143,700 · Chile 112,300 · Greece 98,400 · Portugal 87,600

## 2. Architecture

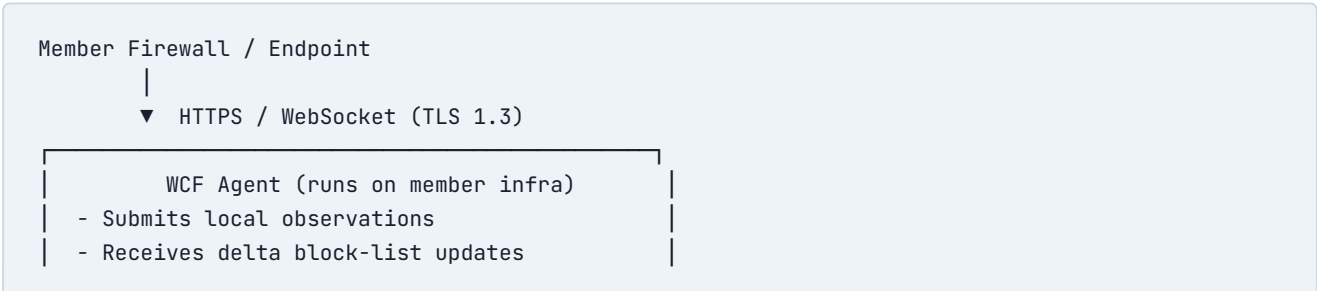
### 2.1 Pipeline Stages

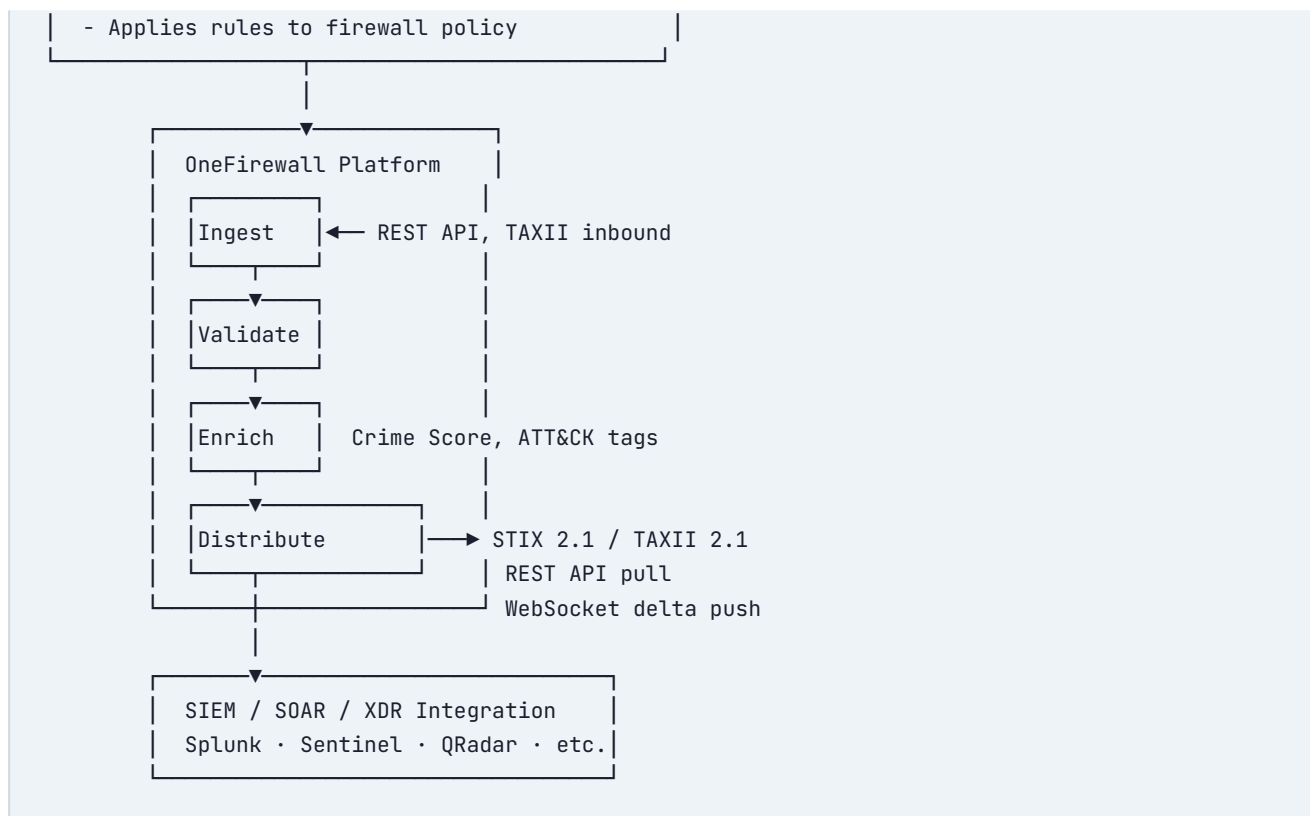
The threat intelligence pipeline processes every submitted indicator through six sequential stages before enforcement:



| Stage                       | Description                                                                                                                                                                                           | Output                                |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 01 — Intelligence Ingestion | Member WCF Agents and API submissions deliver raw indicators (IPs, FQDNs, URLs, hashes) to the ingestion layer via authenticated HTTPS POST. Batch and streaming modes supported.                     | Raw indicator records                 |
| 02 — Threat Validation      | Automated deduplication, format normalisation, false-positive suppression, and cross-reference against existing corpus. Indicators failing validation are quarantined for analyst review.             | Validated, deduplicated indicators    |
| 03 — Enrichment Layer       | Enrichment applies GeoIP resolution, ASN mapping, WHOIS data, passive DNS history, MITRE ATT&CK technique tagging, sector targeting classification, and Crime Score calculation.                      | Enriched indicator objects (STIX 2.1) |
| 04 — Distribution Engine    | Enriched indicators are published to the distribution layer. Delivery targets include: REST API pull, TAXII 2.1 push, WCF Agent WebSocket channel, and SIEM connectors.                               | Distributed feed records              |
| 05 — IPS Synchronisation    | The WCF Agent on each member's firewall receives delta updates via persistent connection. The agent translates indicator sets to platform-native block-list format and applies them to active policy. | Native firewall block rules           |
| 06 — Real-Time Prevention   | Traffic matching distributed indicators is blocked at Layer 3/4 or Layer 7 depending on integration type. Block events are logged and fed back into the ingestion pipeline as sighting telemetry.     | Blocked connections + sighting events |

### 2.2 Data Flow





## 2.3 Distribution Layer

The distribution engine supports four delivery channels simultaneously:

| Channel           | Protocol                 | Use Case                                        | Latency        |
|-------------------|--------------------------|-------------------------------------------------|----------------|
| WCF Agent Push    | WebSocket over TLS 1.3   | Real-time enforcement on firewall/IPS           | <200ms         |
| REST API Pull     | HTTPS REST (JSON)        | On-demand feed consumption, custom integrations | Poll interval  |
| TAXII 2.1         | HTTPS + TAXII 2.1        | SIEM/SOAR platform ingestion (STIX 2.1 bundles) | Near real-time |
| Syslog / JSON API | UDP/TCP Syslog, JSON API | Remote logging, SIEM raw event forwarding       | Near real-time |

## 3. Threat Intelligence

### 3.1 Indicator Types

The platform ingests, validates, and distributes the following indicator types:

| Type                        | Format                 | Example                          |
|-----------------------------|------------------------|----------------------------------|
| IPv4 Address                | CIDR or single host    | 198.51.100.42 , 10.20.0.0/16     |
| IPv6 Address                | Standard IPv6 notation | 2001:db8::1                      |
| Fully Qualified Domain Name | RFC 1123 FQDN          | malicious.example.com            |
| URL                         | RFC 3986 URL           | https://evil.example/payload.exe |
| File Hash                   | MD5, SHA-1, SHA-256    | d41d8cd98f00b204e980099...       |
| Email Address               | RFC 5321               | Phishing sender addresses        |

### 3.2 Crime Score

Every indicator carries a proprietary **Crime Score** — an integer from **0 to 1000** representing the aggregated confidence and severity of the threat. The score is recomputed on each sighting event.

#### SCORE COMPOSITION

| Factor                          | Weight     | Description                                                                              |
|---------------------------------|------------|------------------------------------------------------------------------------------------|
| Alliance sighting frequency     | High       | Number of distinct members that observed this indicator, with recency decay applied.     |
| Repeat offence history          | High       | Historical sighting count across previous reporting windows.                             |
| Sector targeting profile        | Medium     | Whether the indicator targets critical sectors (government, finance, healthcare, Telco). |
| MITRE ATT&CK technique severity | Medium     | Severity of the mapped ATT&CK technique(s) associated with the indicator.                |
| Community confidence weighting  | Medium     | Contributor reputation score applied to submissions from each member organisation.       |
| Source diversity                | Low–Medium | Corroboration across independent sources increases confidence.                           |

#### RECOMMENDED ENFORCEMENT THRESHOLDS

| Score Range | Classification  | Recommended Action                           |
|-------------|-----------------|----------------------------------------------|
| 700–1000    | High confidence | Automated block — safe for production policy |

| Score Range | Classification    | Recommended Action                              |
|-------------|-------------------|-------------------------------------------------|
| 400–699     | Medium confidence | Alert + log; manual review or conditional block |
| 100–399     | Low confidence    | Log and monitor; investigation recommended      |
| 0–99        | Informational     | Observation only; do not block                  |

Thresholds are configurable per member environment via the WCF Agent policy.

**Note:** The Crime Score threshold used for automated blocking is configurable in the WCF Agent policy file. Default installation uses 700 as the blocking threshold. Lowering this value increases coverage but may increase false-positive rate in environments with unusual traffic patterns.

### 3.3 STIX 2.1 / TAXII 2.1

All enriched indicators are available in **STIX 2.1** format via the TAXII 2.1 server endpoint. Connecting a STIX/TAXII-capable platform (Splunk, Microsoft Sentinel, IBM QRadar, Elastic SIEM, Palo Alto XSOAR, etc.) requires only an API key and the TAXII collection URL — no custom parsing required.

#### STIX OBJECT STRUCTURE (SIMPLIFIED)

```
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--<uuid>",
  "name": "Malicious IP 198.51.100.42",
  "pattern": "[ipv4-addr:value = '198.51.100.42']",
  "pattern_type": "stix",
  "valid_from": "2026-02-25T14:00:00Z",
  "confidence": 85,
  "labels": ["malicious-activity", "botnet"],
  "extensions": {
    "x-onefirewall": {
      "crime_score": 823,
      "sector_targets": ["finance", "government"],
      "mitre_techniques": ["T1071.001", "T1102"]
    }
  }
}
```

### 3.4 Alliance Intelligence Sources

Intelligence is contributed by members operating in 12 countries across government, critical national infrastructure, financial services, telecommunications, and enterprise sectors.

| Country  | Sector Focus                        | Indicative IoC Volume |
|----------|-------------------------------------|-----------------------|
| USA      | Enterprise, Finance, Federal        | 524,100+              |
| Italy    | Critical Infrastructure, Gov, Telco | 412,800+              |
| UK       | Government (DSIT), Finance, Defence | 287,400+              |
| Germany  | Industrial, Enterprise              | 276,500+              |
| France   | Enterprise, Telco                   | 231,800+              |
| Brazil   | Enterprise, Finance                 | 204,700+              |
| Spain    | Enterprise, Government              | 198,600+              |
| UAE      | Government, Finance                 | 167,900+              |
| Holland  | Logistics, Enterprise               | 143,700+              |
| Chile    | Enterprise                          | 112,300+              |
| Greece   | Maritime, Gov                       | 98,400+               |
| Portugal | Enterprise, Telco                   | 87,600+               |

IoC volumes are live cumulative totals and increase continuously.

## 4. WCF Agent

---

### 4.1 Function

The **WCF (Web Content Filter) Agent** is the enforcement component installed on a member's existing security infrastructure. It handles bidirectional communication with the OneFirewall platform:

- **Inbound:** Receives delta block-list updates from the distribution engine via persistent WebSocket (TLS 1.3). Translates received STIX objects into platform-native policy rules and applies them without service interruption.
- **Outbound:** Observes blocked and suspicious traffic events locally, packages them as anonymised indicator submissions, and forwards them to the platform ingestion layer to enrich the shared corpus.

The agent operates as a daemon process and requires no user interaction once deployed. Configuration is managed via a JSON policy file and the web-based management dashboard.

**Key behaviour:** The WCF Agent performs incremental (delta) synchronisation, not full list replacement. Only changed records are transmitted, minimising bandwidth and eliminating enforcement gaps during updates.

### 4.2 Supported Platforms (166+)

The WCF Agent ships with native integration modules for the following platform families:

|                    |                    |                 |                    |
|--------------------|--------------------|-----------------|--------------------|
| Check Point NGFW   | Fortinet FortiGate | Forcepoint NGFW | Cisco ASA / FTD    |
| Palo Alto PAN-OS   | Juniper SRX        | Sophos XG / XGS | pfSense / OPNsense |
| SonicWall NSA      | WatchGuard Firebox | Cisco Meraki MX | Barracuda CloudGen |
| Microsoft Sentinel | Splunk SIEM        | IBM QRadar      | Elastic SIEM       |
| Palo Alto XSOAR    | CrowdStrike Falcon | SentinelOne     | Rapid7 InsightIDR  |

Full platform compatibility list: [docs.onefirewall.com](https://docs.onefirewall.com). New platform modules are added regularly.

## 4.3 Deployment Modes

| Mode                    | Description                                                                                                                    | Typical Use Case                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Inline<br>(enforcement) | Agent directly modifies active firewall policy. Blocks are applied in real time. Full enforcement mode.                        | Production perimeter enforcement                        |
| Monitor<br>(passive)    | Agent receives the feed and logs matching traffic without blocking. Generates alerts and sighting telemetry.                   | PoV testing, SOC alerting, pre-production validation    |
| Hybrid                  | High-confidence indicators (Crime Score $\geq 700$ ) are blocked; medium-confidence indicators (400–699) generate alerts only. | Risk-controlled production deployment                   |
| SIEM-only               | No firewall integration. Feed delivered as STIX/TAXII stream to SIEM for correlation and detection rules only.                 | Environments where direct firewall access is restricted |

## 4.4 System Requirements

| Requirement      | Minimum                                          | Recommended                            |
|------------------|--------------------------------------------------|----------------------------------------|
| Operating System | Linux (kernel 4.x+), hardened                    | Ubuntu 22.04 LTS / Debian 12           |
| CPU              | 1 vCPU                                           | 2 vCPU                                 |
| RAM              | 512 MB                                           | 1 GB                                   |
| Disk             | 500 MB                                           | 2 GB (for local log retention)         |
| Network          | HTTPS outbound to api.onefirewall.com (port 443) | Dedicated management VLAN              |
| Auth             | API key (Bearer token, HTTPS)                    | API key + IP allowlist                 |
| Updates          | Automatic OTA                                    | Automatic OTA with rollback capability |

## 5. API Reference

### 5.1 Authentication

All API requests require a Bearer token passed in the `Authorization` header. API keys are issued per member organisation via the dashboard at [app.onefirewall.com](https://app.onefirewall.com).

```
Authorization: Bearer <your-api-key>
Content-Type: application/json
Accept: application/json
```

API keys are organisation-scoped and carry permissions for read (CTI feed consumption), write (indicator submission), and admin (policy management). Keys should be rotated every 90 days.

### 5.2 Endpoints

Base URL: <https://api.onefirewall.com/v2>

| Method | Path                                         | Description                                                                                                                                                                                                                     |
|--------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET    | <code>/indicators</code>                     | Retrieve current active indicator feed. Supports <code>?since=&lt;ISO8601&gt;</code> for delta pulls, <code>?min_score=&lt;int&gt;</code> for filtering by Crime Score, <code>?type=ip fqdn url hash</code> for type filtering. |
| GET    | <code>/indicators/{id}</code>                | Retrieve a single indicator object by ID. Returns full STIX 2.1 object with enrichment fields.                                                                                                                                  |
| POST   | <code>/indicators</code>                     | Submit one or more new indicators. Accepts STIX 2.1 bundle or simplified JSON array. Returns submission receipt with validation status per indicator.                                                                           |
| GET    | <code>/feed/stix</code>                      | Full STIX 2.1 bundle export. <code>?since=&lt;ISO8601&gt;</code> for incremental bundles.                                                                                                                                       |
| GET    | <code>/taxii/collections</code>              | TAXII 2.1 collections endpoint. Lists available indicator collections.                                                                                                                                                          |
| GET    | <code>/taxii/collections/{id}/objects</code> | TAXII 2.1 objects endpoint. Returns STIX objects from a given collection.                                                                                                                                                       |
| GET    | <code>/stats</code>                          | Platform statistics: total indicators, per-type breakdown, recent submission rates, alliance member count.                                                                                                                      |
| POST   | <code>/sightings</code>                      | Submit sighting events (traffic blocked by a member matching an existing indicator). Feeds back into Crime Score calculation.                                                                                                   |
| GET    | <code>/health</code>                         | Platform health and distribution engine status. Returns sync lag, queue depth, and node status.                                                                                                                                 |

## 5.3 Response Format

### INDICATOR OBJECT (SIMPLIFIED JSON)

```
{
  "id": "indicator--3f4a1b2c-...",
  "type": "ip",
  "value": "198.51.100.42",
  "crime_score": 823,
  "confidence": 0.85,
  "first_seen": "2026-01-14T08:22:11Z",
  "last_seen": "2026-02-25T16:45:02Z",
  "sightings": 47,
  "tags": ["botnet", "c2", "ransomware-infrastructure"],
  "mitre": ["T1071.001", "T1102"],
  "sectors": ["finance", "government"],
  "geo": {
    "country": "RU",
    "asn": "AS15169",
    "asn_name": "EXAMPLE-AS"
  },
  "stix": { ... } // Full STIX 2.1 object included on request
}
```

### SUBMISSION RESPONSE

```
{
  "submitted": 3,
  "accepted": 2,
  "rejected": 1,
  "results": [
    { "value": "198.51.100.42", "status": "accepted", "id": "indicator--..." },
    { "value": "10.0.0.1", "status": "rejected", "reason": "RFC 1918 private address" },
    { "value": "evil.example", "status": "accepted", "id": "indicator--..." }
  ]
}
```

### PAGINATION

All list endpoints support cursor-based pagination via `cursor` and `limit` parameters. Default page size is 1,000 indicators; maximum is 10,000.

```
GET /indicators?limit=5000&cursor=eyJzYXN0X2lkIjoimTIzNDUifQ==
```

# 6. Product Catalog

## 6.1 CTI Feed & Platform

The core intelligence product. Provides the real-time indicator feed, Crime Score enrichment, STIX 2.1 / TAXII 2.1 output, and the alliance management portal. Consumable via REST API, TAXII, or WCF Agent. Covers IPs, FQDNs, URLs, and file hashes.

## 6.2 OneDevice — Hardware Firewall Appliance

A proprietary hardware appliance combining pfSense-based stateful firewalling with integrated OneFirewall threat intelligence enforcement. Designed for SMEs that require managed, on-premise network security without internal IT overhead.

The device runs a custom pfSense module that receives intelligence updates via OTA and applies them to Layer 3–4 policy automatically. Full management is delegated to the OneFirewall operations team.

### HARDWARE SPECIFICATIONS

| Component           | Specification                                              |
|---------------------|------------------------------------------------------------|
| Processor           | Quad-core ARM Cortex-A72 @ 1.8 GHz                         |
| Memory              | 4 GB DDR4 RAM                                              |
| Storage             | 64 GB eMMC Flash (expandable via microSD or USB)           |
| WAN Interface       | 1× Gigabit Ethernet                                        |
| LAN Interface       | 1× Gigabit Ethernet                                        |
| Wireless (optional) | Wi-Fi 5 / Wi-Fi 6                                          |
| USB                 | 2× USB 3.0                                                 |
| Video               | 1× HDMI 2.0 (setup/monitoring only)                        |
| Form Factor         | Fanless, passively cooled · 100 × 100 × 35 mm · 12V DC, 2A |
| OS                  | Hardened Linux with custom pfSense module                  |
| Firewall Engine     | Stateful Layer 3–4 (pfSense) + Layer 7 content inspection  |
| Threat Intelligence | Integrated OFA feed · STIX/TAXII compatible                |
| Deployment Modes    | Transparent bridge · Router/gateway · Passive monitoring   |
| Management          | Web-based GUI (HTTPS) · Syslog · JSON API                  |
| Updates             | Automatic OTA firmware and intelligence updates            |

| Component  | Specification                                                |
|------------|--------------------------------------------------------------|
| Compliance | GDPR-ready · ISO/IEC 27001-aligned · Encrypted config backup |

## 6.3 OFA Mobile

Mobile application for iOS and Android. Creates a local VPN tunnel on the device that routes traffic through a local inspection engine. All connections are evaluated against the alliance indicator feed before completion. Blocks malicious IPs, C2 domains, phishing URLs, and botnet endpoints on any network (Wi-Fi, LTE/5G, roaming). Operates independent of corporate perimeter.

Enterprise mode supports policy-based controls and centralised fleet visibility via the management portal.

| Parameter           | Value                                                 |
|---------------------|-------------------------------------------------------|
| Platforms           | iOS 15+, Android 9+                                   |
| VPN mode            | Local VPN (no external proxy server required)         |
| Filtering layers    | DNS + IP layer blocking                               |
| Intelligence update | Continuous background sync from OFA platform          |
| Enterprise features | Policy enforcement, fleet management, MDM integration |

## 6.4 Secure DNS

Alliance-powered DNS resolver. DNS queries for domains present in the indicator feed (above the configured Crime Score threshold) are intercepted and returned with a NXDOMAIN or sinkhole response, preventing resolution of malicious domains before any TCP connection is initiated.

Supports DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). Drop-in replacement for existing resolver configuration. Full documentation: [docs.onefirewall.com/essentials/ofa-dns](https://docs.onefirewall.com/essentials/ofa-dns).

## 6.5 WAF (Web Application Firewall)

Reverse-proxy WAF with OFA threat intelligence enrichment. Provides OWASP Top 10 protection, rate limiting, bot mitigation, and dynamic blocking of IP addresses flagged in the alliance feed. Deployable as a managed cloud service or on-premise. Full documentation: [docs.onefirewall.com/products/waf](https://docs.onefirewall.com/products/waf).

## 6.6 ClosedVPN

Dedicated VPN service for enterprise environments. Traffic is inspected against the alliance indicator feed in-line. Prevents VPN-connected clients from reaching C2 infrastructure, malicious domains, or known attacker IPs regardless of the exit node. Available at [closedvpn.io](https://closedvpn.io).

## 6.7 AI Gateway

Firewall purpose-built for AI service access (public LLM APIs, model endpoints). Enforces data loss prevention (DLP) policies on outbound AI requests, prevents credential exfiltration in prompts, and applies network-level controls to known malicious AI-abusing infrastructure. Available at [onefirewall.ai](https://onefirewall.ai).

## 7. Security & Compliance

| Area                | Detail                                                                                                                                                                                                                                                                  |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Classification | The platform processes only threat indicators (IP addresses, FQDNs, URLs, file hashes). No personal data is processed or stored in the threat intelligence corpus. Member contact/billing data is handled separately under UK GDPR Article 6.                           |
| UK GDPR / DPA 2018  | OneFirewall Alliance LTD operates as a data controller and processor in compliance with UK GDPR and the Data Protection Act 2018. Privacy Policy: <a href="https://onefirewall.com/tnc.html">onefirewall.com/tnc.html</a>                                               |
| Cyber Essentials    | Certified (current). Covers boundary firewalls, secure configuration, access control, malware protection, and patch management.                                                                                                                                         |
| ISO/IEC 27001       | Processes and controls aligned with ISO/IEC 27001 practices. OneDevice appliance compliance-ready by design.                                                                                                                                                            |
| Transport Security  | All API and WCF Agent communications use TLS 1.3. TLS 1.2 is supported for legacy compatibility only. Certificates issued by a public CA; pinning available for WCF Agent channels.                                                                                     |
| Authentication      | API: Bearer token (API key). Management portal: username/password + MFA. WCF Agent: API key + mutual TLS optional.                                                                                                                                                      |
| Indicator Privacy   | Submitted indicators are anonymised before being shared. The submitting member is never disclosed to other members. Only the indicator value and associated metadata are shared.                                                                                        |
| Data Residency      | Platform infrastructure is UK-hosted. Cross-border transfers use contractual safeguards per UK GDPR Chapter V.                                                                                                                                                          |
| Incident Response   | Platform security incidents are disclosed via <a href="https://status.onefirewall.com">status.onefirewall.com</a> . Members subscribed to the status page receive real-time notification.                                                                               |
| EULA                | Use of the platform and WCF Agent is governed by the End-User Licence Agreement at <a href="https://onefirewall.com/eula.html">onefirewall.com/eula.html</a> . The EULA includes prohibitions on reverse engineering, competitive use, and unauthorised redistribution. |

**Cyber Essentials Certified:** OneFirewall Alliance LTD holds current Cyber Essentials certification. Certificate details and scope are available upon request via [support@onefirewall.com](mailto:support@onefirewall.com).

## 8. Pricing Model

OneFirewall uses **device-based pricing**. The subscription cost is calculated per protected device (firewall node, endpoint, or network segment), not per traffic volume, alert count, or indicator quantity. This makes costs predictable regardless of attack scale or feed volume.

| Pricing Axis        | Model                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------|
| Billing unit        | Per protected device / firewall node                                                             |
| Traffic volume      | Not metered — unlimited                                                                          |
| Alert volume        | Not metered — unlimited                                                                          |
| Indicator feed size | Not metered — full feed included                                                                 |
| Overage charges     | None for intelligence consumption                                                                |
| Tiers               | Intelligence-only · Intelligence + WCF Agent · Full managed (incl. OneDevice or managed service) |

Proof of Value (PoV) programme available prior to subscription commitment: connect to the live feed, run in monitor mode, and quantify impact on existing infrastructure before purchasing. Contact: [onefirewall.com/proof-of-value.html](https://onefirewall.com/proof-of-value.html)

## 9. Integration Quick-Start

### 9.1 REST API — First Pull

```
# Retrieve the last 1 hour of high-confidence indicators
curl -s -X GET "https://api.onefirewall.com/v2/indicators" \
  -H "Authorization: Bearer YOUR_API_KEY" \
  -G \
  --data-urlencode "since=$(date -u -d '1 hour ago' +%Y-%m-%dT%H:%M:%SZ)" \
  --data-urlencode "min_score=700" \
  --data-urlencode "limit=5000"
```

### 9.2 Submit an Indicator

```
curl -s -X POST "https://api.onefirewall.com/v2/indicators" \
  -H "Authorization: Bearer YOUR_API_KEY" \
  -H "Content-Type: application/json" \
  -d '{
    "indicators": [
      {
        "type": "ip",
        "value": "198.51.100.42",
        "tags": ["c2", "ransomware"],
        "confidence": 0.9
      }
    ]
  }'
```

```
]
}'
```

## 9.3 TAXII 2.1 Collection Discovery

```
curl -s "https://api.onefirewall.com/v2/taxii/collections" \
-H "Authorization: Bearer YOUR_API_KEY" \
-H "Accept: application/taxii+json;version=2.1"
```

## 9.4 WCF Agent Deployment (Linux)

```
# Download and install
curl -sSL https://install.onefirewall.com/wcf-agent | sudo bash

# Configure API key
sudo wcf-agent configure --api-key YOUR_API_KEY --mode inline --min-score 700

# Enable and start
sudo systemctl enable --now wcf-agent

# Verify status
sudo wcf-agent status
```

**Firewall-specific integration guides:** Check Point, Fortinet, Forcepoint, Cisco, Palo Alto, pfSense, OPNsense, Juniper, and Sophos integration docs are available at [docs.onefirewall.com](https://docs.onefirewall.com).

# Appendix A — Supported Platform Matrix

Representative selection from the 166+ supported platforms. Full list at [docs.onefirewall.com](https://docs.onefirewall.com).

| Vendor            | Platform / Product            | Integration Method                    | Blocking Layer  |
|-------------------|-------------------------------|---------------------------------------|-----------------|
| Check Point       | NGFW, R80.x / R81.x, SecureXL | WCF Agent (SecureXL API)              | L3/L4           |
| Fortinet          | FortiGate, FortiOS 6.x / 7.x  | WCF Agent (FortiGate API)             | L3/L4/L7        |
| Forcepoint        | NGFW 6.x / SMC                | WCF Agent (Forcepoint SMC API)        | L3/L4           |
| Cisco             | ASA, FTD, Firepower           | WCF Agent (FMC REST API)              | L3/L4           |
| Palo Alto         | PAN-OS, Panorama              | WCF Agent (PAN-OS XML API)            | L3/L4/L7        |
| Juniper           | SRX Series, Junos             | WCF Agent (Junos RPC)                 | L3/L4           |
| Sophos            | XG, XGS, Firewall OS 18+      | WCF Agent (Sophos API)                | L3/L4/L7        |
| Netgate / pfSense | pfSense CE / Plus, OPNsense   | WCF Agent + built-in OneDevice module | L3/L4           |
| SonicWall         | NSA, TZ Series, SonicOS 7     | WCF Agent (SonicOS API)               | L3/L4           |
| WatchGuard        | Firebox M/T Series            | WCF Agent (WatchGuard API)            | L3/L4           |
| Microsoft         | Azure Sentinel, Defender XDR  | TAXII 2.1 / STIX 2.1                  | SIEM detection  |
| Splunk            | Splunk SIEM, SOAR             | TAXII 2.1 / STIX 2.1                  | SIEM detection  |
| IBM               | QRadar SIEM                   | TAXII 2.1 / STIX 2.1                  | SIEM detection  |
| Elastic           | Elastic SIEM / Security       | TAXII 2.1 / STIX 2.1                  | SIEM detection  |
| CrowdStrike       | Falcon XDR                    | STIX / Threat Intel API               | XDR prevention  |
| SentinelOne       | Singularity XDR               | STIX / Threat Intel API               | XDR prevention  |
| Palo Alto         | XSOAR (Cortex)                | TAXII 2.1 / REST API                  | SOAR automation |
| Cisco             | Meraki MX                     | WCF Agent (Meraki Dashboard API)      | L3/L4           |
| Barracuda         | CloudGen Firewall             | WCF Agent                             | L3/L4           |
| Rapid7            | InsightIDR                    | TAXII 2.1                             | SIEM detection  |

OneFirewall Alliance LTD · 5 Greenwich View Place, London E14 9NN, United Kingdom · Company No. 11150273 · VAT GB305742714 · DUNS 223612138  
onefirewall.com · docs.onefirewall.com · support@onefirewall.com · +44 (0)20 3807 8020

Classification: Restricted — Partner / Prospect NDA Required | Version: 2.1 | Date: February 2026 | Next Review: August 2026

