

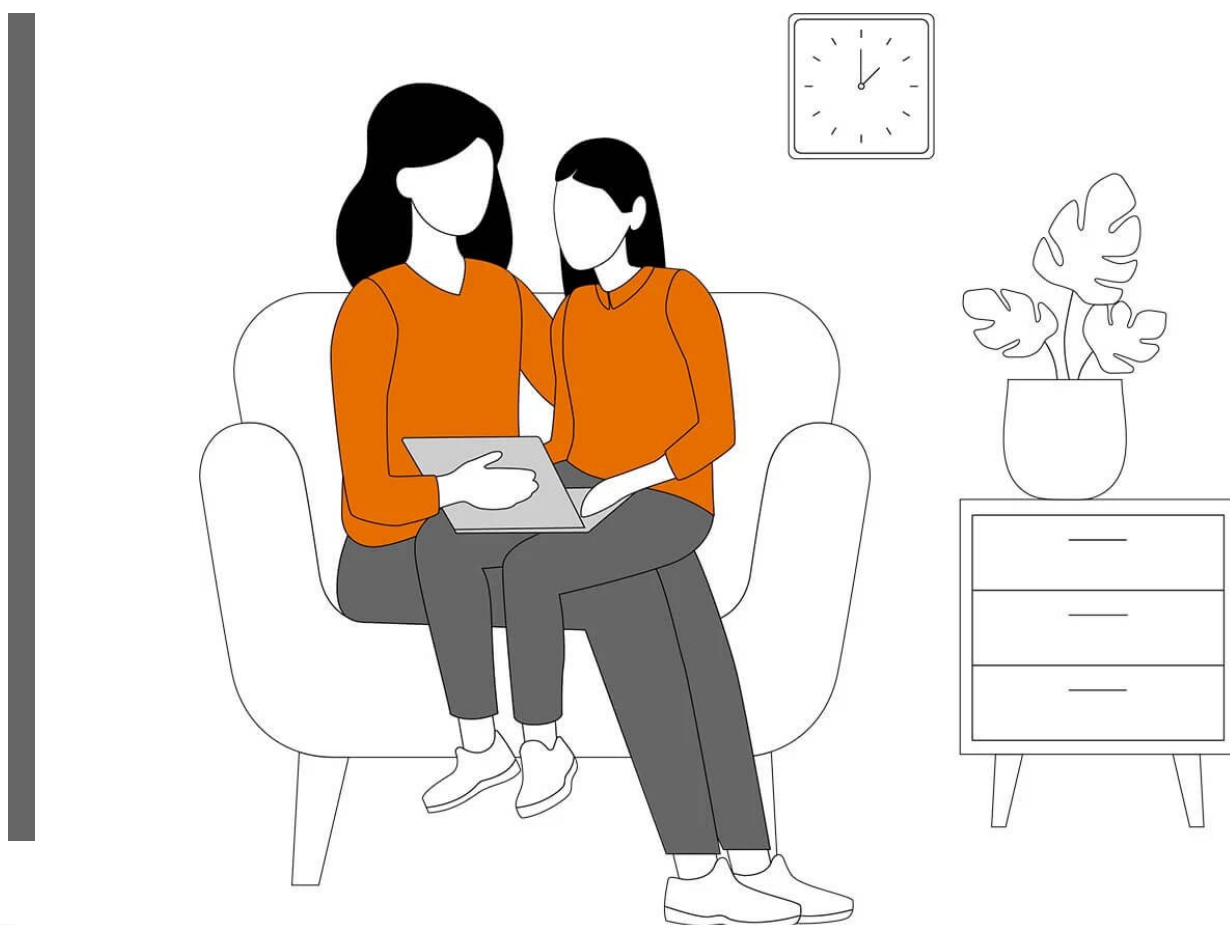
PowerDNS **Protect**

DNS Security & Content Filtering. Network-Based Protection for Service Providers.

The Challenge

Today's Internet users expect more than fast and reliable connectivity. Internet service providers, telecommunications operators, and enterprises must protect subscribers, devices, and networks against malware, phishing, botnets, and inappropriate content - while supporting encrypted DNS traffic and an ever-growing number of connected IoT devices.

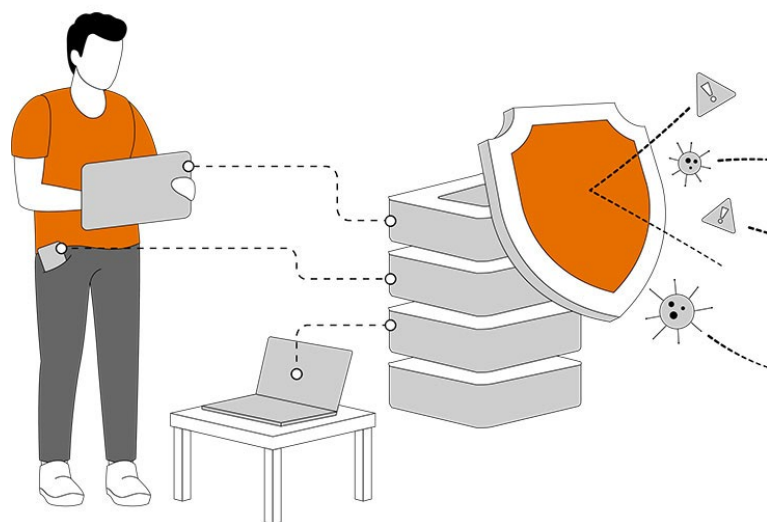
Traditional endpoint security solutions are difficult to deploy across heterogeneous environments and often cannot protect unmanaged or resource-constrained devices. Network operators need a scalable security solution that protects every connected device without requiring additional software or hardware on customer endpoints.



The Solution

PowerDNS Protect is a DNS-based security platform that protects subscribers, connected devices, and network infrastructures through intelligent DNS filtering.

Built on the proven PowerDNS platform, it blocks access to malicious domains, detects infected devices, enforces configurable content filtering policies, and provides flexible parental controls. Because protection is implemented at the DNS layer, PowerDNS Protect secures traditional endpoints as well as IoT devices without requiring additional software or customer premises equipment. It also supports encrypted DNS traffic, ensuring consistent protection across modern network environments.

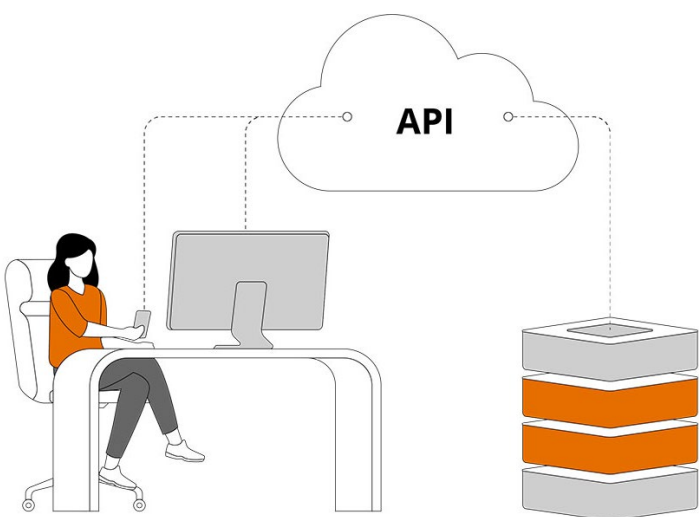


Key Capabilities

DNS-Based Threat Protection.

PowerDNS Protect blocks access to domains associated with malware, phishing, ransomware, botnets, and other cyber threats before malicious connections can be established. Real-time threat intelligence enables continuous protection while preserving user privacy and network performance.

- ✓ Malware protection
- ✓ Phishing protection
- ✓ DNS-based threat blocking
- ✓ Real-time threat intelligence
- ✓ Protection for encrypted DNS traffic



Network-Wide Device Protection

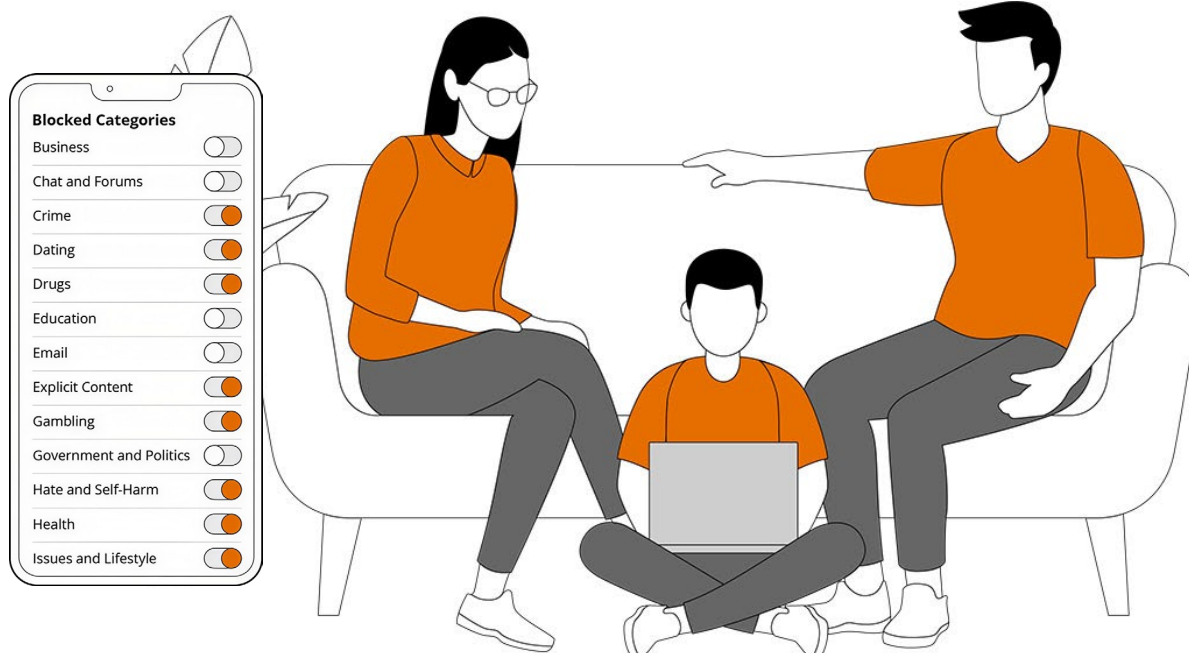
Unlike endpoint security solutions, PowerDNS Protect secures every connected device through the network itself. Traditional computers, smartphones, smart TVs, gaming consoles, and IoT devices all benefit from the same centrally managed protection without additional client software.

- ✓ Protection for unmanaged devices
- ✓ IoT security
- ✓ No endpoint software required
- ✓ No software updates required
- ✓ Immediate protection for new devices
- ✓ Network-wide security policies

Family Protection & Content Filtering

PowerDNS Protect enables operators to offer configurable content filtering and parental controls for subscribers. Filtering policies can be applied per household, subscriber profile, or even per individual device, with configurable schedules for homework, bedtime, or other access policies.

- ✓ Category-based filtering
- ✓ Configurable parental controls
- ✓ Per-device policies
- ✓ User and group profiles
- ✓ Time-based access schedules



Flexible Policy Platform

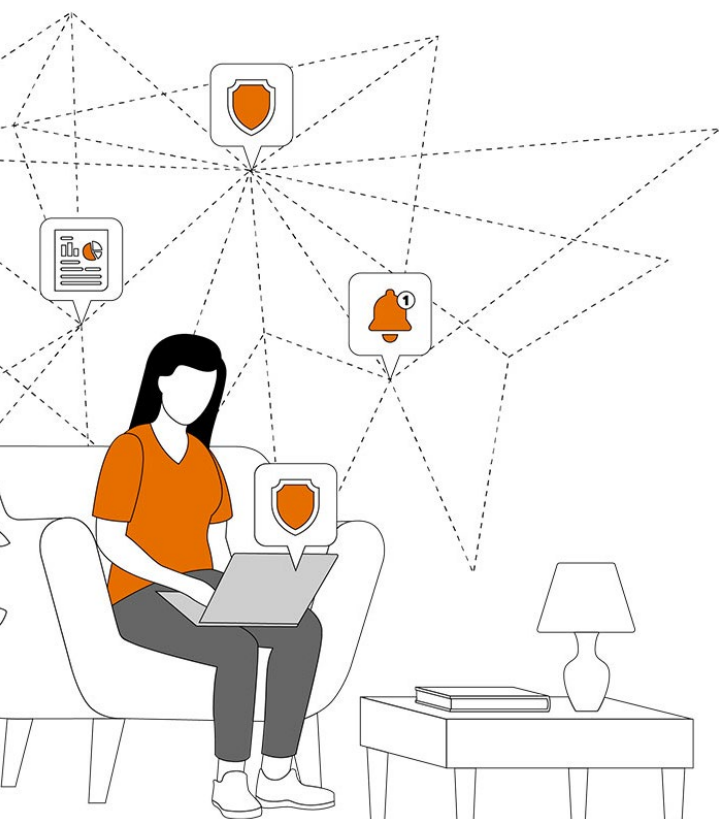
PowerDNS Protect includes the Platform Filter component, which combines DNS- and HTTP-based filtering with flexible policy enforcement, centralized management, and subscriber identification. This enables operators to implement flexible DNS policies for security, compliance, and acceptable-use requirements. Policies can be centrally managed and applied consistently across subscriber groups, business customers, or entire networks.

- ✓ Central policy management
- ✓ Flexible DNS filtering
- ✓ Subscriber-specific policies
- Extensible policy framework

Subscriber Access

PowerDNS Protect includes a white-label management portal and REST APIs that allow operators to integrate security services directly into existing customer portals and mobile apps. Subscribers can manage devices, profiles, filtering policies, and notifications through an intuitive interface.

- ✓ White-label web portal
- ✓ REST APIs for integration with existing portals and apps



Infrastructure Protection

PowerDNS Protect also safeguards provider infrastructure by detecting infected devices communicating with malware command-and-control servers and preventing compromised systems from participating in DDoS attacks. Security teams receive immediate notifications, enabling faster incident response and reducing operational risk.

- ✓ Detection of infected devices
- ✓ Command-and-control detection
- ✓ DDoS mitigation
- ✓ Security notifications
- ✓ Protection of provider infrastructure

Key Benefits at a Glance



Scalable network security



Family-safe browsing
and parental controls



Protects every **connected device**



Flexible DNS policy enforcement



Protection **without**
endpoint software



White-label subscriber portal



Malware and phishing protection



REST API integration



IoT device protection

Ready to Offer Scalable, Secure Internet Access?

Discover how PowerDNS Protect enables cost-efficient network-based security, flexible DNS filtering, and subscriber protection without additional endpoint software or hardware.

[Contact us](#)

docs.powerdns.com

