SafeDNS Web Filtering And DNS Firewall

SAFEDNS

To Ban Or Not To Check.
Market Challenges

- Every device on a network relies on the DNS protocol, yet DNS traffic is rarely monitored. Cybercriminals are well aware of this and exploit the DNS protocol to bypass modern firewalls and intrusion prevention systems.

90%
of malware utilizes DNS at some point in the attack lifecycle to further its operations.

88%
of companies report detecting anomalous activity from DNS attacks each year.

34%
of all targeted attacks can be prevented at the DNS level.

The Market Leader
In DNS Security And Filtering.

DNS Resolver

2010–2014

Content Filter

2014–2019

Protective DNS and Content Filter

2020–Present

SOURCEFORGE

Top Performer

★ Winter ★
2025

G2

**Best
Support**

WINTER

2025

G2

**Highest User
Adoption**

WINTER

2025

G2

**Momentum
Leader**

WINTER

2024

Our Main **Advantages**

Protective DNS

Safeguard networks with DNS Security module. DoH / DoT / DNSSEC and more

DNS Security

Protection against zero-day threats, phishing, and malware across 7 cybersecurity categories

DNS Filtering

Control web access with 59 filtering categories, tailored for your needs.

Appblocker

Block over 180+ applications instantly with a single click.

AI & ML Powered Categorization

SafeDNS's AI and machine learning-powered categorization database processes over 1 billion daily DNS requests, categorizing approximately 400,000 websites each day across 66 categories, with daily updates to ensure dynamic and adaptive web content filtering.
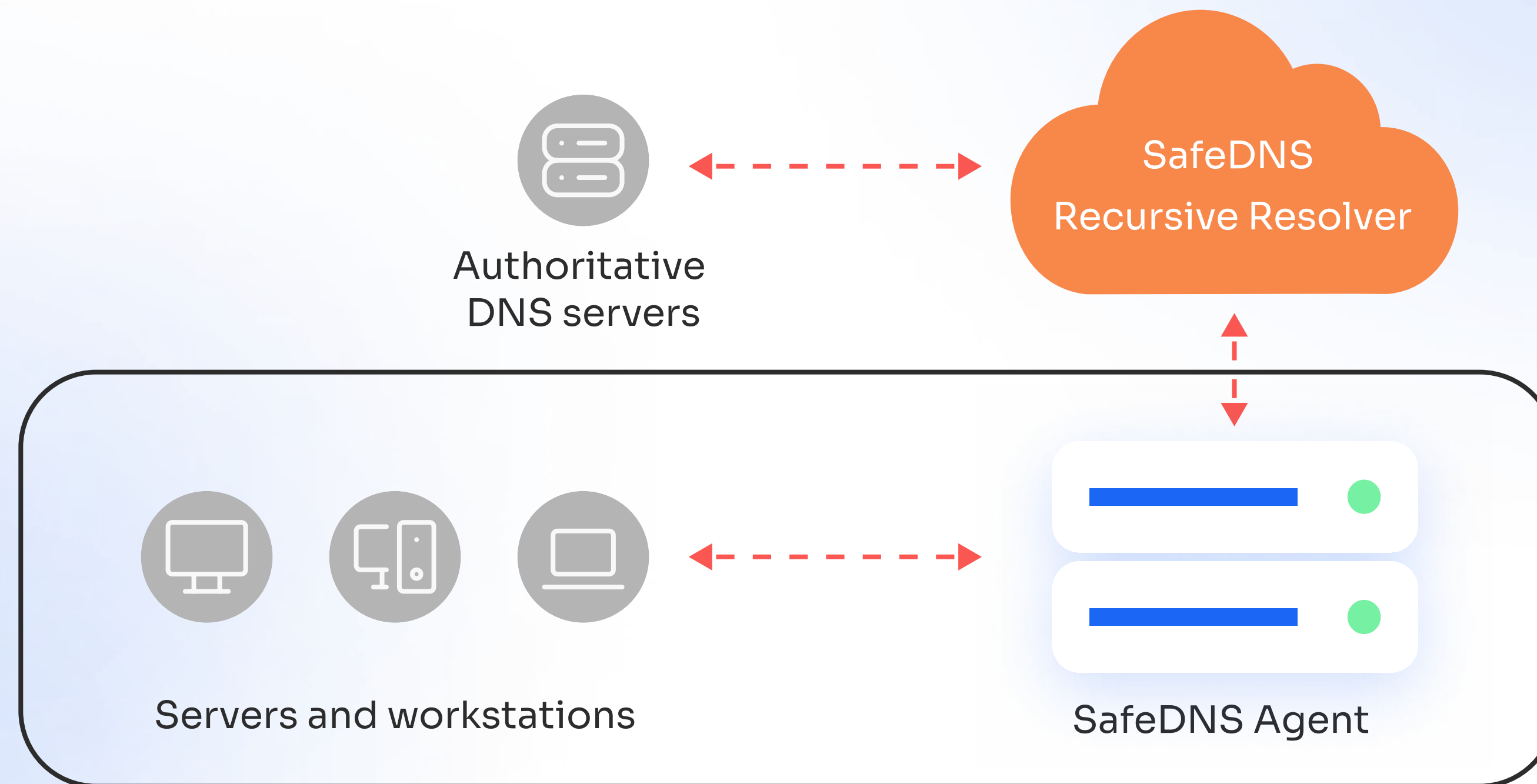
Main Features **+ SafeDNS Cloud**

Main features for Cloud Solution

- User-friendly traffic investigation panel and automatic threat notifications

- Lightning-fast 24/7 support with SLA for first reply under 2 minutes

- Agents available for all platforms (Windows, Linux, Mac, Android, iOS, iPad) with protection against disabling/removal and support for mass/silent installations (Active Directory, MDM)

- Easy scalability for departments and remote branches

- DNS-over-HTTPS, DNS-over-TLS, NAT DNS, and DNSSEC Support

- Comprehensive statistics with general trends, query logs and S3 integration

- Customization of block pages directly from the personal account

Integration **Scheme**

Our Anycast Infrastructure

Seattle
Toronto
New York
San Jose
Chicago
Atlanta
Miami
Los Angeles
Dallas
Santiago
Sao Paulo
Manchester
Amsterdam
London
Warsaw
Bucharest
Paris
Frankfurt
Madrid
Dubai
Johannesburg
Mumbai
HongKong
Singapore
Tokyo
Sydney

22ms
Avg latency worldwide

99.95%
Avg uptime worldwide

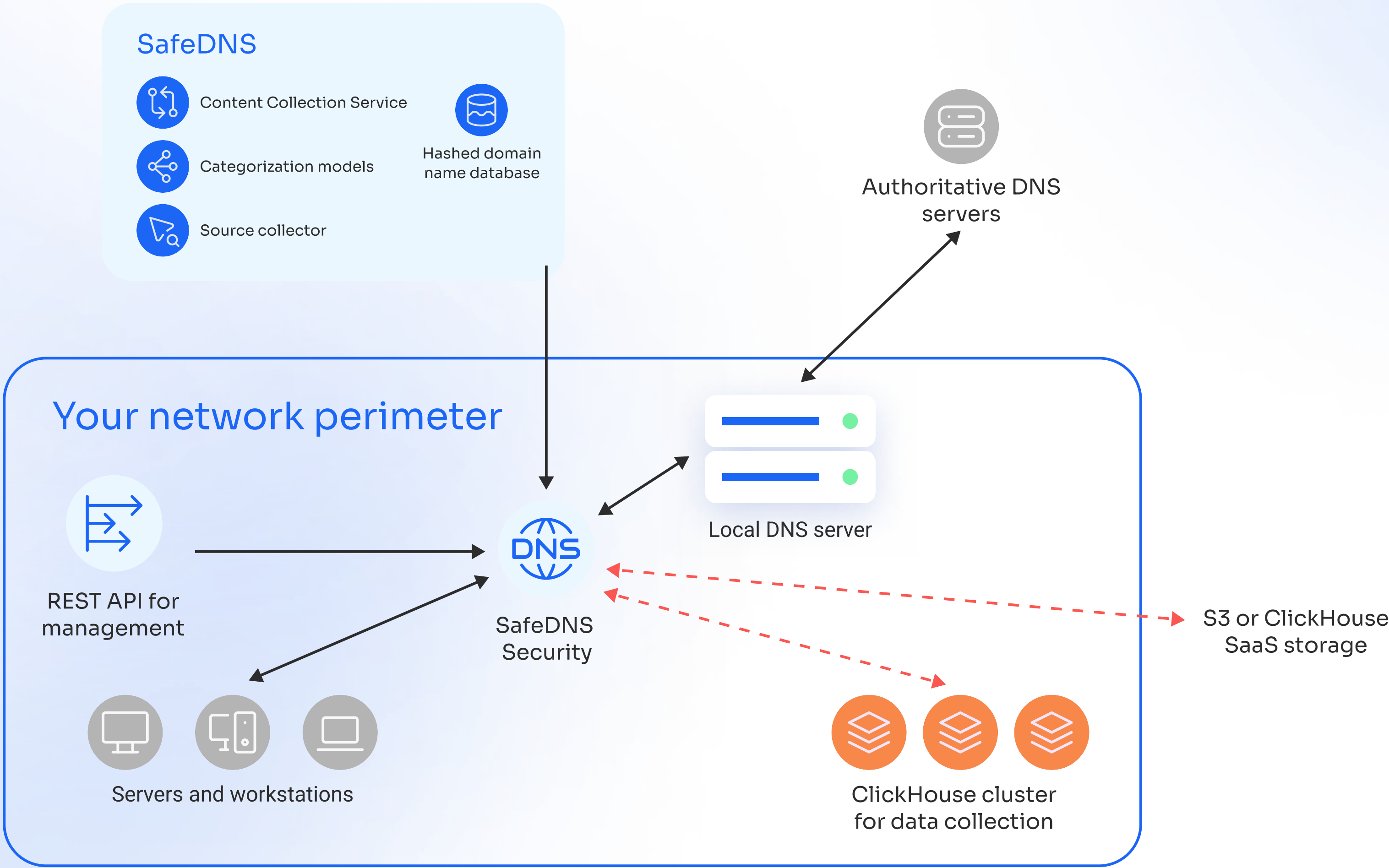## 36 sites
Locations with nodes

SafeDNS |

Main Features + SafeDNS On-Premise

Main features for On-Premise

- Data hosted within the company's infrastructure (DNS proxy with speeds up to 2 million QPS)

- Clear REST API for integration with CGNAT, NAT44, and more

- Deployment via a Virtual Machine using an ISO image

- Extensive API for Custom Management and automation

- Visibility of all DNS traffic tied to your infrastructure with zero latency

- Export of statistics to SIEM, S3, ClickHouse SaaS, or a built-in ClickHouse cluster

Integration **Scheme**

SafeDNS

- Content Collection Service
- Categorization models
- Hashed domain name database
- Source collector

Authoritative DNS servers

Your network perimeter

Local DNS server

REST API for management

SafeDNS Security

Servers and workstations

S3 or ClickHouse SaaS storage

ClickHouse cluster for data collection

Our **Database**

400K
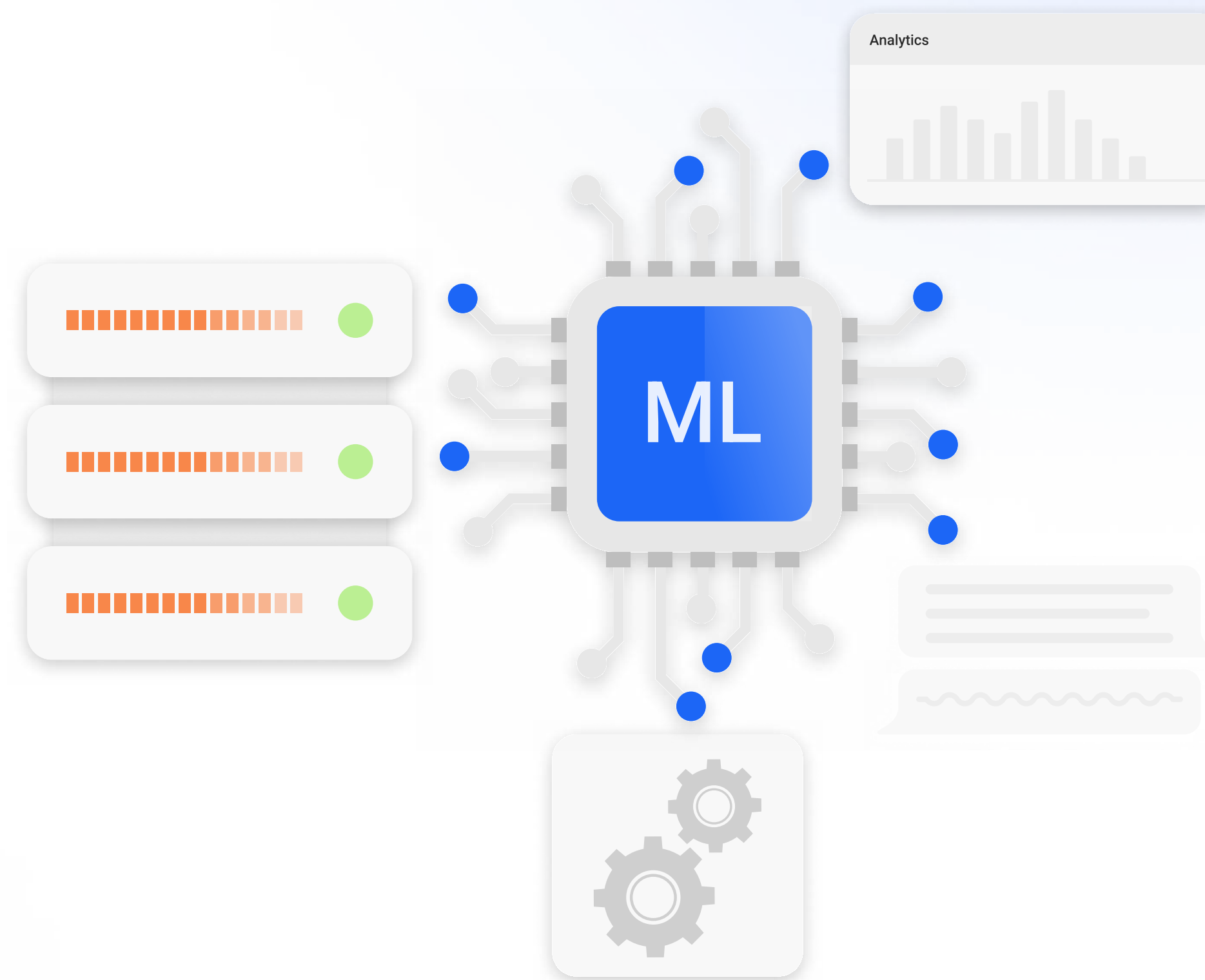URLs Categorized Per Day

116 Million
Domain Names in the Database

2 Billion
URL Records in Total

100+
Classifiers and Smart Algorithms

SafeDNS |

Use Case: Securing Hybrid Environment

Organization overview:

One of the largest banks in Argentina (58 branches and thousands of remote employees)

Initial Issue:

Cybersecurity threats, regulatory compliance challenges, and decentralized network management issues, requiring a scalable solution to protect sensitive data and ensure seamless security for both local and remote users.

Solution:

To address these challenges, SafeDNS deployed its advanced SafeDNS Shield and agents for remote workers.

Use Case: Network Level Filtering

Organization overview:

One of the largest financial companies in Philippines (220 branches and thousands of remote employees with VPN connection)

Initial Issue:

Regulatory compliance with CSAM and application blocking, along with the need for seamless security when accessing office infrastructure via VPN

Solution:

SafeDNS implemented a solution to redirect all traffic through its secure filtering infrastructure.

Why SafeDNS?

116 million
sites in the database

66 Categories
of content, categorized by subject

73 million
cyber threats blocked daily

AI & ML
powered web filtering

SAFEDNS

Based in Alexandria, VA
Out on the market since 2010
Join 4000 companies that trust us

SOURCEFORGE
Top Performer
★ Winter ★
2025

G2
Best
Support
WINTER
2025

G2
Highest User
Adoption
WINTER
2025

G2
Momentum
Leader
WINTER
2024

www.safedns.com   sales@safedns.com