Start security where threats begin—beyond your edge.

Fact sheet

DNS Safeguard

verizon

Are your branch offices connecting directly to the internet? Are your mobile workers bypassing your virtual private network (VPN) to do their day-to-day business? If so, your network may be vulnerable to some of the most common and damaging internet threats. But Verizon DNS Safeguard can be your first line of defense against threats on the internet.

Help protect your network from internet-based attacks with cloud-based security.

Internet-based attacks in the form of malware, phishing and ransomware can happen fast—and frequently—whenever you access the internet. A successful attack can damage your reputation and bottom line. But no matter the size of your business or the number of remote workers you have, you don't want to be a victim.

The main job of the Domain Name System (DNS) is to quickly translate user-friendly domain names into IP addresses. A DNS request is made before any IP connection and every device uses DNS to connect to the internet.

Stop threats outside of your virtual border.

A cloud-based security platform, DNS Safeguard can help prevent your devices—on and off your network—from connecting to malicious or likely malicious sites. The platform can do this because DNS is a foundational component of how the internet works. Using intelligence, DNS Safeguard can identify where these dangerous domains and other intrusive internet infrastructures are staged. It then blocks malicious requests over any port or protocol—across all devices, office locations and roaming users—helping prevent both infiltration and exfiltration attempts.

DNS Safeguard uses threat intelligence to enforce security at the DNS layers to block malware, phishing, command-and-control callbacks, ransomware and spyware. With no hardware to install or software to manage, DNS Safeguard is a simple and effective security solution that can be deployed quickly.

How it works

DNS Safeguard reviews every DNS request and decides what should be done with it. The solution identifies where the request came from and which security policy to apply. Then it routes the traffic seamlessly to the appropriate location or blocks it if it's identified as malicious.

Traditional web proxies examine all internet requests, which adds latency and complexity for their users. DNS Safeguard sends only suspicious domains for review, so you won't experience the same performance issues that may be experienced when proxying all web traffic. DNS Safeguard automatically blocks malicious domains, allows safe domains and routes requests to potentially risky domains for deeper URL inspection.

Criminals use DNS in an overwhelming majority of malware command-and-control callbacks. DNS Safeguard not only protects against initial infection, it can also help prevent infected machines from contacting command-and-control servers. And if a malicious payload tries to bypass DNS and use a direct-to-IP connection, DNS Safeguard goes further to provide malicious IP blocking and enforcement.

Unlike appliances, DNS Safeguard provides protection for devices both on and off the corporate network. And unlike agents, the DNS layer protection can be extended to every device connected to the network—even internet of things.

DNS Safeguard checks internet traffic.

Safe or whitelisted?
The request is routed as usual.

Malicious or blacklisted?
The request is routed to a block page.

Risky?
The request is sent to our cloud-based proxy for URL inspection.

Verizon DNS Safeguard helps eliminate harmful internet traffic before it gets to your front lines.

DNS Safeguard learns activity patterns to automatically identify and inspect suspicious domains.

Consumes

Millions of data points per second.

Applies

Statistical models and human intelligence.

Identifies

Infrastructure staged for known and emerging threats.

Manage the internet experience with greater control.

DNS Safeguard puts you more in control of where your end users go and what they see on the internet. The solution can help you enforce acceptable use or compliance policies across your network. With flexible policies based on content categories and custom block lists, DNS Safeguard can apply internet access restrictions to every laptop you manage.

Through an easy-to-use cloud console, administrators can quickly set up, manage and test different acceptable use policies per network, group, user, device or IP address—giving you greater control of your organization's internet use.

Improve security with a smart solution and expert insights.

By enforcing security at the DNS layer, we block unsafe destinations before a connection is ever made. Security experts at the Verizon Threat Research Advisory Center (VTRAC) leverage our extensive global network and security operations that handle millions of security incidents and trillions of data events each year.

Our VTRAC team analyzes data from a wide variety of Verizon sources to create a vast indicators-of-compromise (IOCs) repository. This includes data from our IP backbone Netflow, incident response, Managed Security Services, Computer Incident Response Team and Security Operations Centers (SOCs).

DNS Safeguard integrates Verizon threat feeds with the robust threat intelligence from the Cisco Umbrella™ platform to provide unique threat intelligence and effective protection from malicious internet traffic.

In addition to Verizon proprietary threat intelligence feeds, DNS Safeguard uses Cisco® intelligence, which analyzes terabytes of data in near real time across various markets, geographies and protocols. This provides extensive visibility into where the threats are coming from, where they call back to, how widespread they are, the first and last time we saw them, and much more.

Human intelligence is combined with 3-D visualizations to learn new patterns.

Then, statistical models are applied to categorize these patterns, detect anomalies and automatically identify known and emerging threats.

100B+	Internet requests or connections every day.
3M+	New domain names discovered every day.
60K+	Malicious destinations identified every day.
7M+	Malicious destinations enforced at any given time.

*Cisco research

Why Verizon

Cybercriminals are getting smarter, but so are we. Better yet, we know how to help protect against them. We keep up with today's rapidly changing cyber threats by processing more than 1 million security events every day at our global network operations centers and security operations centers. This is just one of the many reasons why we know how to protect you from the attacks not only at your network's edge, but also those threatening beyond it.

Get a wide view of internet threats.*

Learn more:

Find out how Verizon DNS Safeguard can adapt to how you do business and combat cyber attacks well beyond your edge. Contact your account representative or visit:

verizon.com/business/products.dns-safeguard