



Forseti brings you unparalleled DNS security and adds threat prevention and HIPS to your network.

This helps by greatly enhancing your protection against APTs, data leaks, ransomware and network malware.

Forseti uses Machine Learning on device-to-infrastructure communication to spot and stop attacks that firewalls can't see, offering you an essential threat hunting tool to prevent attacks on your network.

Protect your perimeter with a truly unique approach to DNS security.

With Forseti, your network is protected against:

✓ RANSOMWARE

✓ DATA EXFILTRATION

✓ APTs

✓ MALWARE



Block malicious web content

Over 22% of all new domains are created for illegal purposes. And it would be impossible for your users to know exactly which websites are completely safe.

For instance, malicious code can be often found in banners on entirely legitimate websites.

But Forseti blocks access to websites containing malicious code and to servers controlled by cybercriminals. Every day, we evaluate over 300,000 domains.



Prevent data leakage

Forseti also stops communications from any existing malware intrusions, avoiding data leaks by detecting and blocking malicious traffic initiated by threats such as APTs and ransomware.



Detect advanced malware

If Forseti ever identifies an infection, we send you alerts for every type of device that's been infected, including PCs, Macs, Androids and iOS devices.

Fully secure your network at perimeter-level with Forseti.

Next-gen network security with added HIPS capabilities to stop threats before they infect your organization.

In recent years, traditional security products turned out to be highly inefficient in an ever-changing threat environment.

49% COST INCREASE

The average DNS attack cost has risen by 49%.

- IDC 2019 Global DNS Threat Report

20% BUSINESSES LOSS

20% of businesses lost over \$1 million per attack.

- IDC 2019 Global DNS Threat Report

34% INCREASED ATTACKS

In 2019, DNS attacks have increased by 34%.

- IDC 2019 Global DNS Threat Report

DNS is commonly used in data breaches as a pathway for data exfiltration, since traditional security products don't know how to address this issue.

But Forseti is based upon a technology that reveals and stops data leakages through DNS. It also employs machine learning-driven intelligence to instantly identify threats, helping you protect your organization from DNS queries to malicious domains.

Customer voice

"It used to take days between knowledge of a threat to actual protection against it."

We now use Forseti to make that process a whole lot faster."

- THOMAS KAABER
IT Manager at Bang & Olufsen



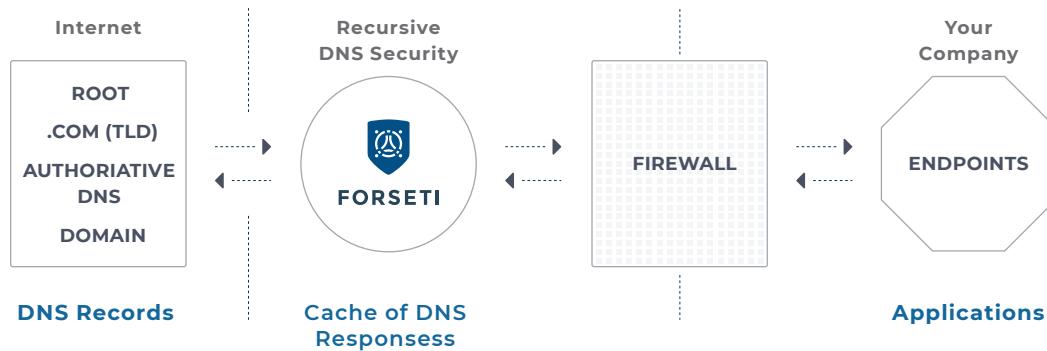
FORSETI

Add an extra layer of protection through advanced Machine Learning and strong, actionable intelligence.

Instantly trace infections to specific users and entry points.

- ✓ Significantly raise your overall security
- ✓ Minimize your costs
- ✓ Protect your infrastructure
- ✓ Don't lose your revenue, intellectual property, and productivity.
- ✓ Free up your internal resources.
- ✓ Access a real-time overview of your current security status

Forseti in the network



Don't leave your network vulnerable!

Cybercriminals won't stop exploiting the existing security holes in the Internet's infrastructure. Be one step ahead of them and secure your network at DNS-level!

Features	FORSETI	REGULAR FIREWALL
Detect & block web-based threats	✓	✗
C&C callback blocker	✓	✗
Network based malware & APT detection	✓	✗
Data leakage prevention	✓	✓
Hosted service - no servers or client software	✓	✗
Supports all servers, desktops & mobile devices	✓	✗
Custom block and allow list	✓	✗
Basic statistics	✓	✓
Advanced statistics & forensics, with internal IP-addresses and hostnames	✓	✗
Run it in passive/IDS mode	✓	✗
Customized block page (OPTIONAL)	✓	✗

Stop threats before they damage your organization!

- ✓ Implementation takes less than 15 minutes.
- ✓ Perimeter Recursive DNS
- ✓ Hunt and detect advanced network threats.
- ✓ Run it in Active and Passive Modes.
- ✓ Benefit from machine learning-driven intelligence.
- ✓ See exactly where attacks are coming from.
- ✓ Using ITILv3 standard for security incidents helps you comply with ISO27001/2.
- ✓ Spot hidden threats using Vector™ Detection's Machine Learning.
- ✓ Best protection/investment ratio.

With Forseti, you can now significantly raise your security level with minimal impact on your existing IT setup.

At the same time, you can protect your most vulnerable infrastructure and minimize your administrative costs.

- ✓ Subscription model, no initial investment needed.
- ✓ Continuous updates with no administration or maintenance.
- ✓ Fully hosted: experience zero downtime or service interruptions.
- ✓ No configuration changes or server reboots needed.
- ✓ Automatically covers all devices in your network.

Get in touch today to experience how Forseti can fully secure your network against the most sophisticated DNS attacks.



Contact us at

+45 7199 9177
or
corpsupport@heimdalsecurity.com