



Home network is now the office network

Replicate office cybersecurity controls for employees in remote locations with network edge security.

THE PROBLEM

The boom of flexible workplace approach has left off-premises networks entirely unprotected and increased the risk of IT security breaches for enterprises.

From smart TVs to printers in employee homes, the spectrum of devices targeted by hackers has expanded; every company that follows a distributed work model requires robust protection.

How can we address this need? By creating an additional security level for remote networks with a hybrid solution that combines hardware and software, powered by in-house cyber threat intelligence research.

THE SOLUTION

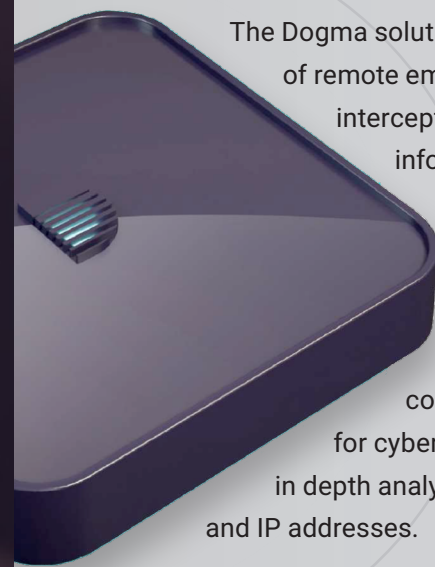
Dogma was developed to fill the gap in remote network security of enterprises, improving cyber threat visibility, detection, analysis, and response capabilities of the dedicated security personnel.

Its hybrid nature and network segregation capabilities make Dogma stand out in the competitive landscape of cybersecurity solutions, delivering full protection to enterprises no matter where their employees are working from.

The Dogma Solution mitigates cyber attack risks for enterprises with four intertwined elements: Device, App, Dashboard, and Cloud.

Dogma Device

Dogma was designed to fill the gap in remote network protection. Through WiFi segregation it prevents lateral movement attacks with proprietary patented technologies.



The Dogma solution provides visibility of remote employee networks and intercepts malicious activity informing the company's security staff about the occurrence of security events.

It applies effective control and prevention filters for cyber threats by performing an in depth analysis of the DNS resolution and IP addresses.

The Dogma modular solution works simultaneously on different protocols both locally and in Cloud.

In addition, Dogma enhances the level of security of devices that by design do not have on-board security software (e.g., printers).

- » Easily connected to the home Wi-Fi router via a RJ45 cable
- » Powered by proprietary internal enterprise level technology
- » Performs Wi-Fi segregation by creating a new and separate Wi-Fi connection
- » Enables direct connectivity through VPN

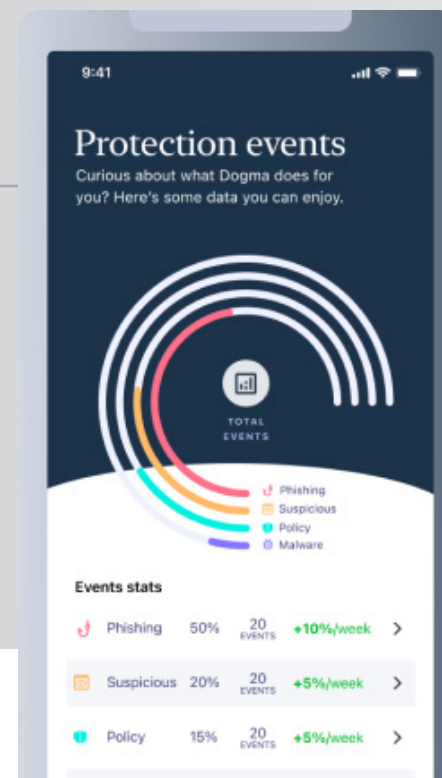
- » Applies effective cyber threat detection, control and prevention over traffic and interactions with the backend system
- » Traffic is observed locally (directly on the hardware device) with metadata analyzed remotely (on Cloud and / or on-premise systems)

Dogma App

The Dogma application is available for download from App Store and Google Play Store.

The app was designed to simplify the installation of the Dogma device, guiding the user through the device setup phases to ensure an immersive and user-friendly experience.

The Dogma app also gives visibility of any blocked navigation and / or non-linear behavior, and provides useful information to increase employee security awareness.



The application can be used for the following:

- » Initial device set-up Factory reset
- » Display of notifications about security events and / or company policies

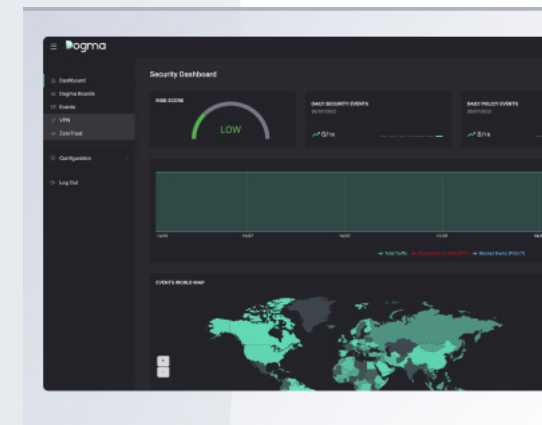
- » Information on the secure remote network created by Dogma and access to credentials for the connection of company endpoints
- » Listing of the connected devices
- » Access to history of alert notifications and anomalies

Dogma Dashboard

The Dashboard is integrated within the SOC to provide complete visibility of remote networks security events, allowing for effective policy management.

The dashboard enables the enforcement of company security policies and allows for the configuration, control and management of individual Dogma devices, groups of devices, and all the devices that are affiliated with the company.

The dashboard displays the following information for the aggregate remote networks perimeter and individual / groups of Dogma boards: security level, security events (both Policy and Security type), as well as the geographic attribution of security events.



The dashboard provides the following information:

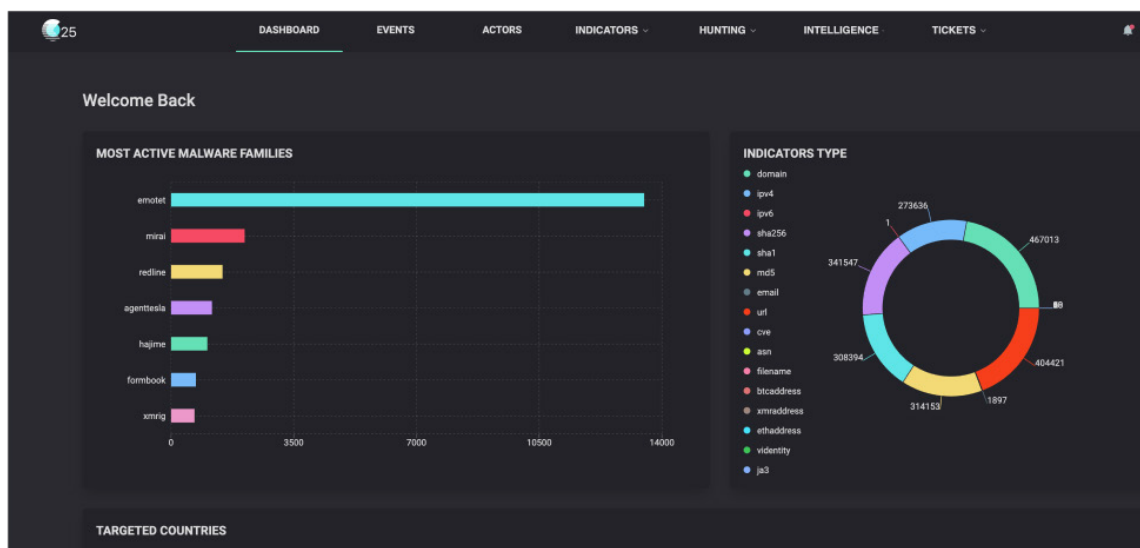
- » Security events graph (Policy & Security type)
- » The geography of security events
- » Single board details: serial number, last access time, security status, connected devices
- » Domain / IP of blocked threats
- » Security policy applied to individual devices, groups of devices & all devices affiliated with the company

Dogma Secure Cloud

Dogma Secure Cloud provides software functionalities that are based on complex in-house developed algorithms and aimed at the identification and blocking of cyber threats.

Dogma Secure Cloud is powered by continuously updated cyber threat intelligence insights, retrieved by Cluster25, the internal cyber research division of DuskRise. The origins of gathered data mainly fall under the following categories:

- » Open Source: Data is gathered through software connectors capable of taking data from freely accessible sources.
- » Semi-open Source: Corresponds to the point 1, with the difference that the source requires a non-exclusive registration to access the data.
- » Closed Source: corresponds to the point 1, with the difference that the data is accessed through a formal acceptance process or on a commercial basis.
- » Internal Research: gathered cyber threat intelligence research and threat detection performed by the Cluster25 team.



DuskRise covers a new gap in enterprise security that has been exposed by the shift to work from home. Building on the expansion of the enterprise from traditional endpoints, to IoT and BYOD, DuskRise empowers Security and Operations teams to make sure these remote networks, and any device on them, are secure.

Powered by Cluster25, the threat intelligence arm of DuskRise, companies can extend security to the edge of the network, with a seamless integration process and a beautiful user experience.

DuskRise is enabling a secure workforce without boundaries. Learn more at DuskRise.com.

Schedule a Consultation
get.duskriase.com/consultation

Product Inquiries
sales@duskriase.com

Corporate Headquarters
331 Park Avenue South, Floor 4,
New York, NY 10010