DuskRise

Security for the Hybrid Workforce

Corporate network perimeter has been extended into untrusted networks, redefining the enterprise edge. Employees working from home are connecting untrusted BYOD devices via these networks to directly access corporate assets.

The DuskRise solution enables corporate security and segmentation policy management, extending office-grade protection to remote assets and users.

The new attack surface

67% of business-impacting cyber attacks target remote employees. The hybrid workforce is extremely vulnerable, causing both financial and reputational damages to their organizations. DuskRise's edge solution provides a trusted network enclave and simplifies existing security architectures.
The solution creates a barrier between corporate assets and unmanaged environments, protecting the former from threats.

Digital transformation demands consolidation

DuskRise allows companies to quickly and easily reproduce office-grade security controls in remote untrusted networks. DuskRise reduces the attack surface that malicious actors can exploit by consolidating existing security architecture into a unified model.

Edge computing is the future

Edge computing allows DuskRise to deliver a solution which is not limited by bottlenecks of the current SASE architectures. By performing analytics at the edge and utilizing a direct-to-cloud design, DuskRise ensures customer data privacy, low latency, and faster response times for detected threats.

DUSKRISE'S BENEFIT

Network segmentation

DuskRise uses Wi-Fi segregation to create a secure enclave and prevent lateral movement attacks, providing a protected channel for access to corporate assets.

Network policy implementation

The solution enables the enforcement of corporate network security policy and allows for the configuration, control, and management of affiliated remote networks.

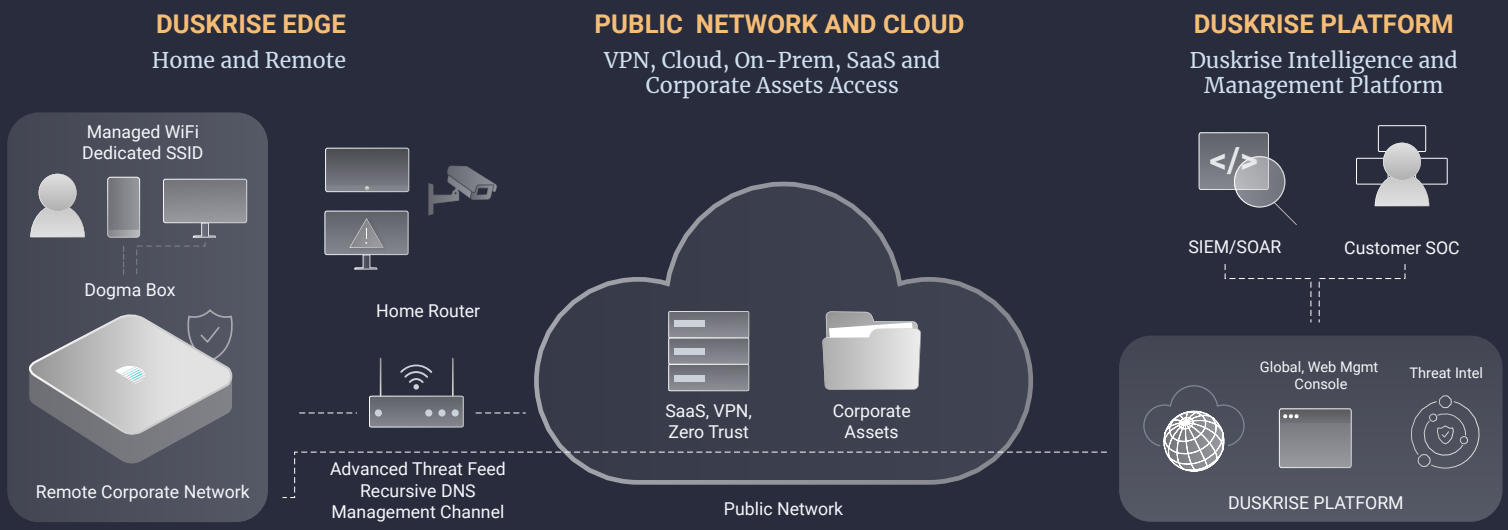
Network-based threat detection

Cyber threats are mitigated through effective control and prevention filters, delivered by Cluster25, DuskRise's cyber threat intelligence unit.

Upskilling your workforce

According to a study by IBM, human error is the main cause of 95% of cyber security breaches. Tailor-built for the end user, the DuskRise app provides visibility of any blocked navigation and useful information about APTs, attack types, and more to increase security awareness.

How It Works



The DuskRise Platform

What does the yearly subscription get you?

Device

Lightweight IoT device connected to an offsite employee's Wi-Fi router.

App

Application used for device set up, security monitoring, and cybersecurity awareness insights.

Dashboard

Web-tool for the enterprise's SOC personnel.

Cloud

Component that powers the solution through in-house cyber threat intelligence from the Cluster25 team.

DuskRise

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 its own Cluster25 threat research and intelligence, 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.

Get a demo
https://get.duskrise.com

Product inquiries
sales@duskrise.com

Contact information
331 Park Avenue South, Floor 4,
New York, 10010