DISPEL

Gartner Cool Vendor 2017™

Moving Target Defense

Booth 743

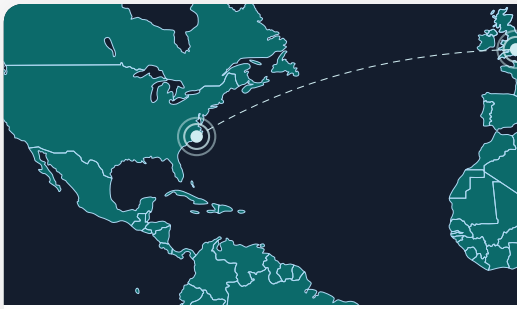
Network Cloaking & Secure Data Flow

Dispel helps enterprises proactively defend their critical data, legacy/unpatched infrastructure, and executive credentials from cybercriminals, insider threats, and advanced persistent threats. Dispel's platform cloaks networks, enables protected work spaces for multiple parties, and allows secure access to, and handling of, sensitive data and systems.

The Dispel Enclave

Data, Uncompromised.

Data theft is a 400+ billion dollar industry.[1] Dispel provides executives with the peace of mind that their data and credentials are protected. We segment and protect your data in encrypted, traceless Enclaves that can be deployed on-demand and over which you have complete control.



enclave-us-eu-asia

Hub
New York City, NY

Entry Points
New York, Washington Show Info ↓

Exit Points
New York, London, Singapore Show Info ↓

Video Conference
London, UK Launch

Virtual Desktop
Singapore, SG Connection Info ↓

Users

Anna
anna@state.gov

Steve
steve@corp.org

Defend Your Reputation

Identifying a breach doesn't mean it never took place. Stop attacks before they happen.

Ease Administration

Create project-specific Enclaves in minutes with Dispel's simple admin console *(shown right)*.

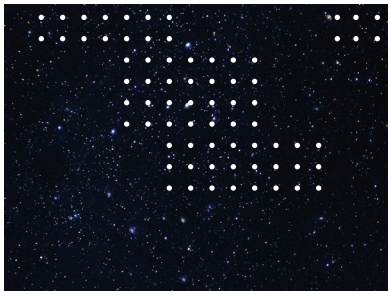
Simplify Compliance

Geospecific, single-tenant, encrypted, and auditable. GDPR is here, and we can help.

Streamline Control

Get project teams, including external partners, on-board faster without sacrificing security.

[1] Update to the IP Commission Report [2017] *The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy.* http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf



Implementation Steps

1. Build

Use the Administrative Console to select the resources, cloud providers, and locations you wish to include in your Enclave.

2. Deploy

The Dispel Engine will deploy and configure your single-tenant, uniquely-keyed Enclave within 30 minutes.

3. Segment

Never worry about exposing IP. Each Enclave is scoped to the project and physically segmented from other business data.

4. Work

Add teammates and systems with a single click. Leverage a single-tenant collaboration environment.

5. Destroy

When the network is no longer needed, download data for long-term storage and delete the Enclave.

DISPEL

Cloud Native Defense

Dispel has helped companies of all sizes tackle the issues of cyber resiliency, data management, third-party trust, compliance, and identity, in some of the world's most hostile cyber environments.

Dispel's Platform employs Moving Target Defense (MTD) to cloak enterprise networks, enable traceless communications, and segment corporate systems. Dispel Networks are composed of virtual machines deployed within seven public cloud providers and, as available, on-prem cloud implementations.[2] Dispel Networks can be integrated into an existing enterprise network to endow it with a dynamic secure access layer, or can be created as a self-contained, off-channel network.

Secure Legacy Systems

Enclaves may be used to wrap vulnerable legacy/unpatched infrastructure and segment it from potentially malicious parties. Administrators can grant encrypted, allow-list access based on a combination of time or user permissions. Any Internet accessible device can be cloaked within a Dispel Network.

Enable Private Multi-Party Interactions

Move fast without breaking things. Dispel lets organizations team up and get projects securely underway in less than 30 minutes. Administrators can enforce strong encryption, data protection, and access control. All of Dispel's networks are self-contained, single-tenant, and 100% auditable. Your data belongs to you.

Customizable Virtual Desktops

Access other sensitive parts of your company without wondering about the state of local machines. Dispel provides custom Windows and Linux boxes programmatically air-gapped form the user's local computer.

[2] Public Cloud providers include AWS (commercial and FedRamp), Azure (commercial and FedRamp), DigitalOcean, SoftLayer, GoogleCloud, Rackspace, and Vultr. Private Cloud providers include OpenStack and VMWare.