Protect Machines That Can't Protect Themselves

Applying Dispel Cloaking

Gartner Cool Vendor 2017™

Booth 743
Security & Risk Summit
National Harbor, MD
June 4 - 7, 2018

About Dispel

Dispel creates the world's leading cloaking products for your endpoints and networks. Companies, institutions, and governments use Dispel to render their employees and systems invisible to cybercriminals, insider threats, and advanced persistent threats. Our technology radically reduces attack profiles and data breaches through cloud virtualization and dynamic perimeter networking. Dispel deploys in minutes through easy-to-use software clients and hardware devices. Launched in 2014, Dispel is headquartered in New York and operates globally.

This paper is about some of the problems we solve, and how we go about doing it.

Unpatched/Legacy Systems

Legacy systems exist across all large organizations. Some underpin critical networks and are so central to complex systems they cannot be replaced. Almost everyone has a 2003 server living somewhere in their organization.

The problem with legacy systems is they become unsupported and unpatchable. Keeping them online may be a business necessity, but they're also an organizational liability.

Take, for example, a major pharmaceutical company with data coming in from a clinical trial. The data analysis software for this sensitive, pivotal moment runs on an old, unsupported operating system.

Or, consider file servers brokering data exchanges between APIs—dating from before APIs were called that. It's a 24/7 system, without funding or flexibility to hot swap and upgrade without downtime.

Data can be stolen, systems cannot be made compliant, and it all comes down to an increase in monetary and reputational risk.

IT teams carry an additional burden: time. Legacy systems demand inordinate amounts of attention. Manually setting up separate networks, and keeping them interconnected, is costly and time consuming. Motivating teams and hiring are impacted too—no one wants to babysit old tech.

We can help. If you cloak legacy systems, they're not a frontline target. They still need to be updated at some point, but cleaning the junk drawer out doesn't have to be today's chore.

Remote Data Access

When people and systems need remote access, our customers tend to be most concerned by four risks: (1) distrust of the other organization's security; (2) data portals creating vulnerable access points for hacking; (3) complex security procedures preventing a transaction from taking place; and, (4) data access leading to data loss.

Setting up restricted access through VLANs or hardwired networks is cumbersome. Data rooms are often ill-suited to tasks like third parties conducting data analytics. And any solution opens doors for data exfiltration.

CISOs and IT teams have to contend with business pressure to get the integrations done fast, but when something goes wrong they take the blame.

Our customers use Dispel to grant access quickly and safely. They use Dispel virtual desktops to give third parties a powerful looking glass to see data, without the opportunity to steal it or infect the network. And Dispel cloaking keeps outsiders from knowing the location of servers and endpoints, minimizing the attack vector even to those who've used the system before.

Internal Projects

When your team is starting new projects, deploying code, reviewing contracts, finalizing deal books, or planning new acquisitions, they do it digitally.

Employees want to work using fast and modern tools. Tools that usually live in the cloud, outside of your control, in multi-tenant systems. Hacks and legal requests could expose those communications. Reputation damage, downtime, and monetary losses are all concerns for CISOs. Plus, the office gossip in five year old emails plays very well when leaked by hacktivists.

Many of our customers use Dispel's products to chat, send, share, see, and host in a manner that keeps CISOs sane.

For securing data globally without impeding productivity, Gartner recognized Dispel as a 2017 Cool Vendor in Unified Communications.

Technical Overview

Dispel Enterprise Platform

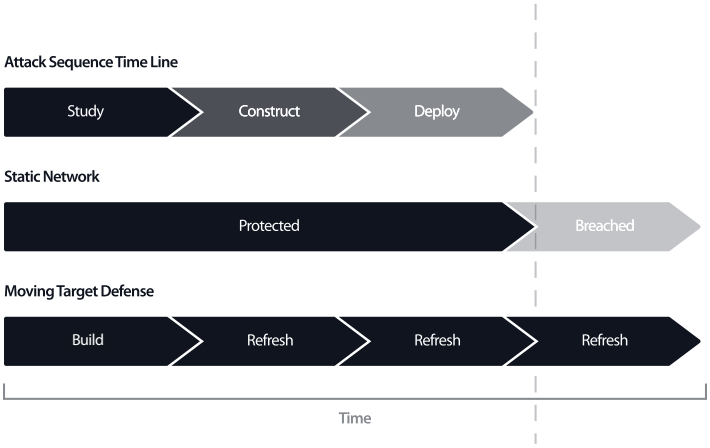
Technical Specifications of Moving Target Defense

Dispel has established an industry-leading security program. Our security practices are, at a minimum, aligned to NIST 800-160 and DoD 5220.22-M. The company undergoes regular audits by both external black/white-box penetration testers and internal security teams.

Dispel's platform employs Moving Target Defense (MTD) to cloak enterprise networks, enable traceless communications, secure & segment corporate data, and deploy dynamic virtual infrastructure. Moving Target Defense has traditionally circulated within academic and defense communities, with Dispel being the first to evolve the theory to enterprise networks and make those advancements commercially available.

MTD addresses the flawed, static nature of traditional enterprise networks. When given time, adversaries will patiently find the weakness in an organization's defensive tool set, burrow into their corporate networks, and execute their attack—whether that is data exfiltration, DDoS-ing systems, or holding the organization ransom. In any cyber-attack, the most time consuming aspect is properly finding the weakness to exploit and gaining access. MTD thwarts enemies trying to locate or map a network's topology and segments critical assets and data repositories from threats.

Moving Target Defense interrupts the Attack Sequence



The techniques and design considerations for MTD are outlined in NIST 800-160 Volume 2. They include:[1]

Adaptive Response
Optimize the ability to respond in a timely and appropriate manner to adverse conditions, stresses, or attacks, or to indicators of these, thus maximizing the ability to maintain mission or business operations, limit consequences, and avoid destabilization.

Analytic Monitoring
Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.

[1] U.S. Department of Commerce. *Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. By R. Ross, R. Graubart, D. Bodeau, and R. McQuaid. Available at: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf. Accessed April 13, 2018. (National Institute of Standards and Technology Special Publication 800-160, Volume 2).

Coordinated Protection
Require an adversary to overcome multiple safeguards (i.e., implement a strategy of defense-in-depth).

Deception
Mislead or confuse the adversary, or hide critical assets from the adversary, making the adversary uncertain how to proceed, delaying the effect of the attack, increasing the risk of being discovered, causing the adversary to misdirect or waste its resources, and exposing the adversary tradecraft prematurely.

Diversity
Limit the possibility of loss of critical functions due to failure of replicated common components.

Dynamic Positioning
Increase the ability to rapidly recover from non-adversarial events (e.g., fires, floods). Impede an adversary's ability to locate, eliminate, or corrupt mission or business assets, and cause the adversary to spend more time and effort to find the organization's critical assets, thereby increasing the probability of the adversary revealing its actions and tradecraft prematurely.

Non-Persistence
Reduce exposure to corruption, modification, or compromise. Provide a means of curtailing an adversary's intrusion and advance and potentially removing malware or damaged resources from the system.

Privilege Restriction
Restrict privileges based on attributes of users and system elements as well as on environmental factors.

Realignment
Minimize the connections between mission-critical and noncritical services, thus reducing the likelihood that a failure of noncritical services will impact mission-critical services. Reduce the attack surface of the defending organization by minimizing the probability that non-mission or business functions could be used as an attack vector.

Redundancy
Provide multiple protected instances of critical resources.

Segmentation
Contain adversary activities and non-adversarial stresses (e.g., fires, floods) to the enclave or segment in which they have established a presence. Limit the set of possible targets to which malware can easily be propagated.

Substantiated Integrity
Ascertain whether critical system elements have been corrupted.

Unpredictability
Make changes randomly or unpredictably. Increase an adversary's uncertainty regarding the system protections which they may encounter, thus making it more difficult for them to ascertain the appropriate course of action.

MTD Implementation

Dispel uses three methodologies to implement MTD:

1. Virtualization,
2. Software-Defined Networking, and
3. Encryption & Data Management.

Virtualization

With the advent of cloud, successful Moving Target Defense became feasible within the last decade. Traditional networks rely upon physical hardware to create LANs and VLANs, and are difficult to reconfigure in real time. Reverse proxies have limited capabilities and are static.

Virtualization allows the rapid deployment of on-demand and disposable networking resources. For example, a server acting as a VPN access point may be replaced with another in a different data center mid-attack—leaving enemy surveillance wondering what happened and keeping recovery simple. Mass virtualization also allows for automated patching, saving corporations hours of administration and overhead.

Dispel is cloud agnostic, and fully integrated with seven major public cloud providers to form hybrid networks: Amazon Web Services, Microsoft Azure, DigitalOcean, IBM SoftLayer, Google Cloud Platform, Rackspace, and Vultr. Dispel also supports two on-premises cloud implementations: OpenStack and VMWare.[2] All told, Dispel deploys thousands of virtual resources spread over more than 150 global data centers on a weekly basis. These virtual resources are used to augment existing networks with layers of MTD, or to create disposable, concealed networks—called Enclaves—which are primarily used for communications.

Cloud Providers & On-Prem Implementations

Dispel's system deploys three types of virtual components on both Linux and Windows operating systems: (1) Networking, (2) Collaboration, and (3) Custom.

1. **Networking** components include entry points, exit points, disassociating joints, health monitoring components, and PKI that enable self-healing and resiliency. These components route traffic over both TCP/UDP protocols with optimizations in place to ensure high availability, transmission integrity, and maximum network speeds.

2. **Collaboration** components include file sharing, team messaging, video conferencing, telephony, logging, and remote workstations. Since these components may be created and securely networked together in under 30 minutes, Dispel Enclaves can be transaction-specific without the bulk and persistence of a traditional network, or multi-vendor SaaS offerings.

3. **Custom** components are "blank servers" which function like stem cells—quickly configured to run any form of containerized application. For instance, virtual desktops are often customized to meet requirements for specific applications or pre-configured security settings.

Software-Defined Networking

Many of Dispel's technologies concentrate on the secure networking and self-healing of deployed virtual resources. Dispel deploys in one of two ways:

1. Cloaking existing infrastructure to add layers of Moving Target Defense; and,

2. Deploying self-contained networks users connect to through either a client application or hardware device.

With rare, explicitly stated exceptions, Dispel production environments are single-tenant for each customer. This prevents one client from abusing the information they have about their Dispel network in order to attempt to attack another client on the same system. Networks are usually further segmented in scope based on project or system. That means any threat is segmented to a per-project or per-scope minimum attack vector.

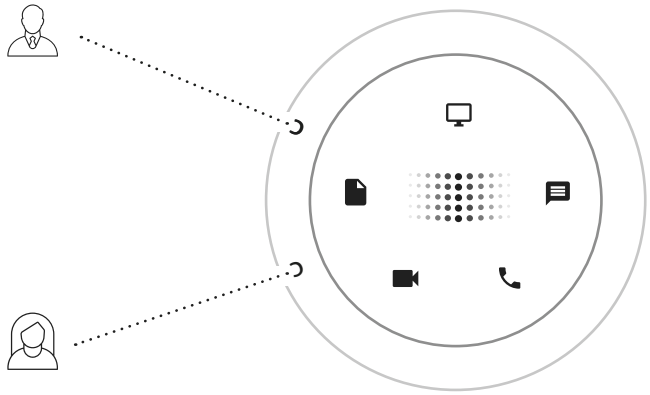
We compare this practice of hyper-segmentation to pre-emptively fighting a fire. If the fire spreads, the forest

[2] AWS and Azure are both FedRAMP certified cloud providers, with Amazon capable of handling Secret level information.

is lost. However, if effectively isolated and quarantined, the damage can be mitigated and quickly overcome. Similarly, if the adversary can find or compromise an executive's credentials to a data lake, the goal is to minimize the possible damage.

To prevent outsiders from identifying, prodding, or connecting to virtual resources, all public interfaces on Dispel-deployed servers are turned off. Instead, virtual machines and integrated corporate servers within a network speak to each other through custom private interfaces. For example, both WannaCry and Petya relied upon overlooked, publicly accessible ports on Windows servers to deploy their ransomware. On networks where Dispel was deployed, those interfaces did not respond to the malicious prodding, and the Legacy resources—even unpatched Windows 2003 servers—contained within the MTD layer were protected.

Project-Specific Enclave



Software-defined networking mandates individuals must first permission and authenticate before they are granted knowledge of the location for networks. This method mitigates both insider threats and phishing attempts. For example, even if an executive's file server credentials are compromised, the attacker cannot not find the file server to abuse the stolen credentials.

Dispel customers deploy networks through our administration console, where they choose component type(s), geographic location(s), cloud provider(s), and virtual machine size(s). Each network has its own Access Control List, and all servers are single-tenant. Our commitment to a single-tenant, Zero Trust[3] model differentiates us from our competitors. Unlike other 3rd party SaaS providers, Dispel never co-locates customer data alongside another's. If one of their network is compromised, your data will not be vulnerable. Furthermore, Dispel can pass contractual ownership of deployed virtual resources over to the customer, so that they can assure complete control over their network.

Finally, all of our components speak syslog, and our networks are deployed with an ELK Stack logging platform standard (ELK - Elastic Search, LogStash, Kibana). In addition, we are happy to integrate specific monitoring and threat detection tools into our networks as required.

Encryption & Data Management

Dispel transmits information over the public Internet. We protect data in transit with strong encryption, reviewing and updating to employ latest cryptographically reliable cipher suites.

For example, at this time, when you are connected to your Dispel services through our client application or a hardware device, and for internal server-to-server transmissions, we use two layers of cascade ciphered AES-256-CBC with independent 4096-bit RSA keys for the initial key exchange. Keys are typically generated by segmented compute systems designed with randomness in mind, and distinguished between clients.

When you are using one of our browser-accessible applications, we employ AES-256-GCM encryption. These may be secured using SHA-256 with 2048- or 4096-bit RSA keys, depending on the security requirements of the application. This means many communications through Dispel are protected by three layers of encryption. We encrypt data

[3] We use Zero Trust in the model that assumes users and systems are compromised. Therefore, Enclaves are given unique encryption keys and only have access to data pertinent to their project-specific function. Further, customers do not even need to trust Dispel, as we also provide full engine licenses wherein companies can bring the entire system on-premises.

multiple times, using different ciphers, for several reasons. As one example, by using different ciphers encrypted data is less susceptible to a zero day flaw that could affect both at the same time.

Client data is encrypted at rest in file systems—but client machines are usually active and, therefore those drives are mounted in the OS. The hardware is subject to physical safeguards.

Dispel's MTD model disassociates the identities of corporate users from local, ISP, and State-level surveillance. To an outsider, the connection looks exactly like a user browsing the web for personal use—encrypted, unremarkable, and not worth pursuing.

Traditionally, corporations have not had a means of combating State-level actors. Dispel's platform allows them to evade illegal surveillance, and protect themselves from insider plants or phished credentials.

Dispel networks simplify data management by ensuring a self-contained environment from the moment of network creation through termination. Access to networks can be regulated through single-use workstations that are programatically air-gapped from the user's local host. The end result is a geo-specific, auditable environment allowing organizations to comply with domestic and international regulations like GDPR.

Connect with Dispel

If you've found this interesting—and that you reached the end of this paper would suggest you did—please contact us at:

Web dispel.io
Phone +1.917.268.4390
Email enterprise@dispel.io

[*] *Gartner, Cool Vendors in Unified Communications, 2017, 11 May 2017.* The Gartner Cool Vendor Logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.