Security at Dispel

Internal procedures

Security is what we do at Dispel, and we take it very seriously. This page discusses what we do to protect you, your company, and your data. If you ever have any security questions or issues, feel free to get in touch with us at security@dispel.io.

This is a living document. This PDF was made on May 24, 2018 1:26 PM, and may have changed. You can always get the latest copy from the Dispel GitHub.

Dispel's Approach to Security

Dispel is on a mission to allow anyone to connect any kind of system to the Internet, without creating a target profile. To achieve this, we have to thoughtfully develop software and systems designed to protect our customers. Through transparency with how to accomplish security at Dispel, we help educate users on our practices and engender a strong company culture.

Dispel has established an industry-leading security program, ensuring our customers have a high degree of confidence and trust in our stewardship of their data and operations. Many of our security practices are aligned to NIST 800-160 and DoD 5220.22-M, and we regularly undergo audits by penetration testers and our customers to make sure we're on the top of our game.

Sections

Organizational Security

Dispel maintains a culture of trust but verify. Personnel security programs are designed to protect the personal data of our employees and our customers.

Personnel security

Dispel's personnel practices apply to all employees and contractors who make up the Dispel workforce. All workers are required to understand and follow internal policies and standards.

Prior to access to Dispel systems, workers agree to confidentiality agreements and consent to background investigations. The depth of a personnel security investigation depends on the kind of access the individual may have. Workers also attend regular security awareness training, including topics such as device security, avoiding phishing, data privacy, physical security, incident reporting, and workplace ethics.

Upon termination of work at Dispel, all access to Dispel systems is removed immediately.

Privacy & security training

Dispel provides all employees with security training and briefings commensurate with their involvement with sensitive information. This training covers topics such as general security awareness, device security, insider threat awareness, reporting requirements, and data protection. Workers are encouraged as part of the culture to personally verify identities when other worker ask for system access.

Foreign ownership, control, or influence

Cybersecurity is geopolitical. Dispel is sensitive to the risks associated with possible foreign ownership and influence. To that end, we have taken the follow steps:

Our core technology is developed on U.S. soil. Technology areas with lesser security requirements, such as our informational website, may be developed in both U.S. and allied territories. Dispel does not outsource software development of our core technologies. Our engineers are U.S. citizens or authorized for employment by the U.S. Government.

Some of our systems use open source software, which we do not control. When we use open source software, we reasonably update which software is used in a publicly available list.

Designated security roles

Dispel has defined roles and responsibilities to distinguish which personnel have security obligations and responsibilities. At the center of our security efforts is the Dispel Security Team. These personnel are responsible for supervising and directing security measures necessary for implementing applicable requirements for sensitive information.

Workstation security

Access to Dispel office workstations is secured by video surveillance, locks, keyed access, and intrusion detection systems as appropriate for the sensitivity of the material handled at the relevant facility.

All computers used by workers are configured to comply with our standards for security. These standards require all computers to be properly configured, kept updated, and run security monitoring software. When new workers start, their computers are configured to encrypt data, have strong passwords, restrict remote access, and lock when idle. Computers run up-to-date monitoring software to report and detect potential malware and malicious activity.

Policies & standards

Dispel has internal policies we maintain in order to safeguard information, and create a culture of trust and security awareness. This document is among those. Through culture and policy, our security documents help Dispel

workers operate reliably and ethically. These policies are living documents, and are updated and made available to all workers to whom they apply.

Audits, compliance, & independent assessments

Dispel both self-audits and uses independent parties to assess our systems and procedures.

Audits

When appropriate for meeting a particular standard, Dispel undergoes independent audits of our procedures and facilities. When appropriate and with approval, some customers also perform their own security audits of our technology. Our Security Team works with other companies' security and architecture teams to make sure we address questions prior to a deployment.

Penetration testing

We undergo regular independent white box penetration testing. The results of these tests may be made available under a non-disclosure agreement.

Communicating with Dispel

If you would like to contact us about a security concern, or if you believe you have experienced a security breach, the fastest way to get in touch with our security team is at security@dispel.io. Email us for our PGP key.

Technological Security

The purpose of Dispel's technological security practice is to prevent the unauthorized access of user data, and minimize the potential for third-party observation and analysis to determine metadata-based user intent.

Code review & handling

Dispel uses version control software to store code. We try to push code to production as often as safely possible, so bugs get fixed quickly. We like to have second sets of eyes look at code. When code moves from a feature branch to staging to production, it is subject to a code review when the pull request is made to merge the branch into staging.

Transport security

Dispel uses Moving Target Defense to cloak and segment your networks on Dispel, and enable traceless connections. Dispel implements MTD through: (i) Virtualization, (ii) Software-Defined Networking, and (iii) Encryption & Data Management.

For instance, when you connect to an Enclave that belongs to your company that infrastructure is only used by other members of that Enclave.

Data security & encryption

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 visit Dispel-hosted web applications, we employ AES-256-GCM encryption, with SHA-256 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 multiple times, using different ciphers, for several reasons. For instance, differing ciphers are less susceptible both having the same zero day flaw at the same time.

Network security

Data on Dispel systems is protected through physical measures. With rare, explicitly stated exceptions such as our Retail service, 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. It also means any threat is segmented to a per-client minimum attack vector.

Client data is encrypted at-rest in file systems—but client machines are usually active and therefore those drives are mounted in the OS. In those cases, hardware is protected by physical safeguards implemented by the cloud provider.

Dispel divides its networks into separate infrastructure in order to protect more sensitive information. Systems supporting testing and development environments are distinct from production environments. Access and credentialing to production systems and databases is restricted to engineers with specific business requirements. Network access to production systems is isolated to protocols needed to support the applications. System logs are generated and stored in accordance with customer requests. Dispel security and engineering teams receive notifications depending on state and status of Dispel network infrastructure.

Authorizing access

Dispel employs a system of least trust when granting systems access in order to minimize the risks of a data breach and the possibility of insider threat. Dispel grants access to code repositories, billing systems, customer relationship management tools, email servers, and cloud environments based upon business requirements.

Workers must request access from their manager or responsible owner when seeking to escalate privileges. When workers no longer require access, their credentials are revoked. Access audits are conducted quarterly to determine if granted accesses are still necessary.

Authentication

Dispel uses multi-factor authentication on systems containing more sensitive information, and generally whenever possible. Where applicable, Dispel uses private keys for authentication. Where SSH keys are used, knowledge of those keys is restricted to individuals with a specific business need. When credentials are transmitted between workers, encryption methods such as public-key cryptography or out-of-band transmission are used. When credentials are encrypted using public keys for transmission, data transit is still conducted under encrypted protocols. In production environments requiring the highest level of security, single-tenant systems are provisioned without root access and will not provide access credentials to anyone.

Dispel requires the use of approved password managers. Password managers help prevent the re-usage of passwords and reduce the chance passwords are physically written down. They also reduce the risk of successful phishing attacks.

System monitoring & logging

Dispel logs access and activities on production and development environments. Notices on code repositories, servers, databases, and other systems are distributed in reasonably real-time to relevant workers.

Responding to security incidents

If a security incident is detected, the matter will be handled by the Computer Security Incident Response Team (CSIRT), part of the Security Team. The CSIRT's goal is to minimize and control the damage resulting from incidents by responding and recovering, and subsequently putting in corrections to prevent similar future incidents from taking place.

The Dispel CSIRT is also involved in improvement programs, including postmortems after any incident to evaluate how it happened, and how to improve the response.