CLOUD SECURITY

WHITE PAPER

INTRODUCTION

The ever-growing interest in Software as a Service (SaaS) has necessitated a new paradigm for security requirements. Since customer information is transferred, processed and stored outside the customers' usual environment, emphasis must be placed on securing this information.

We have put security at the heart of our online business experience platform development and deployment in order to ensure several well-controlled layers of security, with a particular emphasis on Security in Depth.

The following overview is intended to introduce the methodology we follow to secure our most valuable asset: our customers' data. It is intended to be a high-level document describing methodologies and techniques used to mitigate security risks.

SECURITY IN DEPTH

The concept of "*Security in Depth*" at Dassault Systèmes relies on the fact that several independent mechanisms are put in place in order to mitigate any single risk. An unlikely failure to block the malevolent action will therefore not result in a threat but will be subsequently blocked by a different mechanism.

The security processes of our online **3D**EXPERIENCE Platform follow industry standards and best practices, where practical and applicable, with a particular emphasis on:

- ISO 2700x standards, and in particular **Implementation Guide ISO 27002**
- **NIST 800 series**
- **OWASP methodologies**
- **CobIT framework**

INTERNET SECURITY

Several security layers are in place to ensure that only intended traffic and activities are actually processed by the online platform.

All incoming Internet traffic is filtered by independent mechanisms ensuring reliability and lack of vulnerability cascading. Moreover, the internet-scale hosting environment is robust to Distributed Denial of Service attacks.

Secured communication channels between the hosting environment and the customer's premises are used, where applicable, to ensure the confidentiality and integrity of the transferred data.

APPLICATION-LEVEL SECURITY

The application layer of the Dassault Systèmes online solution undergoes a very strict security design and review process. Our Development & Verification processes are designed with security awareness & controls embedded in them. The code is aligned with industry best practices and recommendations and is double-peer reviewed (internally and externally). Special attention is placed on the top OWASP threats. A cyclic penetration testing exercise is performed on the application ecosystem to add an additional protection check which complements the secure coding paradigm. Finally, a continuous process of scans is in place to constantly monitor various modules of the application.

IN-CLOUD SECURITY

While inside the Dassault Systèmes cloud, the security of the customer environment relative to other elements in the cloud (in-cloud security) is once again ensured though independent layers of solutions. Beyond traffic restriction (firewalls), each customer works on instances that are independent from the other systems. Such an approach protects from cross-customer data access; this compartimentation is also hardcoded at the application level.

The structure of the cloud environment which ensures the separation above also mitigates classical risks of network reconnaissance and attacks. In particular sniffing and IP spoofing is not feasible by design.

VIRTUAL SYSTEMS SECURITY

The virtualized systems on which the data and applications are hosted are closely scrutinized from a security standpoint prior to being released into production. The security lifecycle applied to these systems is very strict and maintains a high level of security after the production release.

Beyond classical security maintenance activities (system patching, services review), Dassault Systèmes regularly proceeds with attack-like scenarios that test the integrity of a model system, as well as the reactivity of the operational teams. The cyclic, yet random, nature of these tests ensures a reunification of the findings (causal analysis).

PHYSICAL SECURITY

Customer data (or IP) is stored and processed in nondescript data centers to which access is strictly limited to authorized staff.
All contractors and visitors are escorted at all times.
All physical access to data centers is logged and audited.
Physical storage is also secured via redundant disks, disaster recovery, and backup and restore procedures.

SECURITY TESTS AND REVIEWS

Information security is built into the process of developing Dassault Systèmes cloud solutions for our customers. This is the result of a common effort undertaken by R&D and Information Security teams who work closely together to identify and address all potential issues.

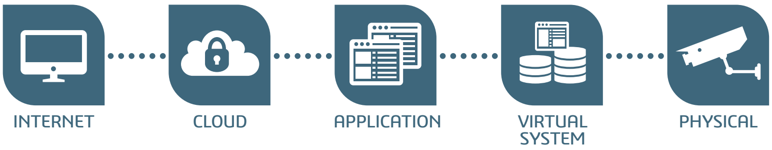
In addition to these proactive efforts, independent tests are performed at least yearly and at each major change of the platform. These tests stress the various security layers, and attempt to breach the environment in a hacker-like manner.

These activities are all carefully planned and executed as part of our global design, implementation & validation cycle.

In addition to platform security mechanisms, a complete roles-based access control is implemented within the application, enabling the data owner to set granular access rights.

Finally, access to the application is possible only after a correct license has been obtained, minimizing the possible surface of attack. TLS based mechanisms ensure a safe connectivity, addressing the risk of eavesdropping or Man-in-the-Middle attacks.

LAYERS OF SECURITY IN DEPTH



CONCLUSION

As you have seen, the concept of Security in Depth is designed around several independent mechanisms for mitigating any single risk on the Dassault Systèmes 3DEXPERIENCE Platform when it is deployed On Cloud. Customers can feel confidence in using our SaaS platform because we have placed security at the heart of our online business experience platform.

GLOSSARY

METHODOLOGY

Causal analysis

A process improvement technique which seeks to define the causes and relationships of these causes following the discovery of a defect.

OWASP

OWASP (Open Web Application Security Project) – a security organization that sets standards for application security and specifically issues a list of the most critical vulnerabilities in web applications. Widely recognized as the "gold standard" for web security.

ATTACKS

Distributed Denial of Service

An attack in which a very large number of requests from many sources are made against an attacked system. The objective is to cause that system to become unresponsive while trying to process them all at the same time.

Eavesdropping, network sniffing

The act of intercepting data traffic for malicious analysis and reuse. This attack can rely on Man-in-the-Middle techniques (see below) or make use of specific network configurations which allow traffic intended to be contained between two systems (usually a client and a server) to be intercepted by a malicious entity.

IP spoofing

IP spoofing is a hacking technique where the real network address of the attacker is modified so that the target system is led to believe that the traffic comes from a trusted machine.

Man-in-the-Middle attack

An attack in which a malicious host is placed on the communication path between a legitimate client and a legitimate server. This malicious host will try to capture the traffic before passing it to the legitimate recipient in a transparent way. The captured data can then be analysed later for malicious purposes.

Network reconnaissance

Hacking techniques to discover the topology of the target network, systems and services. Allows the planning and structure of later attacks.

Vulnerability cascading

A design and implementation flaw where a single issue on a system reverberates on other security layers.

XSS

A family of attacks on applications that exploiting flaws in how access controls are handled, which have been introduced by insecure coding methodologies.

PROTECTION

Penetration testing

An exhaustive set of security tests where hacking activities are carried out against a system in the same way a hacker would.

Secure coding

A subset of rules, methodologies and frameworks aimed at avoiding the introduction of vulnerabilities into web applications. Strongly linked with OWASP standards.

Security in Depth

A security concept where the protection of information relies on sets of independent mechanisms. A breach of any one mechanism does not impact the others, or make it easier to defeat them.

System patching

The assurance that all components of the system are up to date with the recommendations of the vendors.

TLS

An encrypted channel for network communication, which allows for secure communications over insecure media such as Internet.

Our 3DEXPERIENCE Platform powers our brand applications, serving 12 industries, and provides a rich portfolio of industry solution experiences.

Dassault Systèmes, the **3D**EXPERIENCE Company, provides business and people with virtual universes to imagine sustainable innovations. Its world-leading solutions transform the way products are designed, produced, and supported. Dassault Systèmes' collaborative solutions foster social innovation, expanding possibilities for the virtual world to improve the real world. The group brings value to over 170,000 customers of all sizes in all industries in more than 140 countries. For more information, visit **www.3ds.com**.

3DEXPERIENCE

DASSAULT SYSTEMES | The **3D**EXPERIENCE Company

Americas
Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA

Europe/Middle East/Africa
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Asia-Pacific
Dassault Systèmes K.K.
ThinkPark Tower
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japan