Security White Paper

June 5, 2014

201-20 Amber St
Markham, ON L3R 5P4

p. +1-647-479-4268
f. +1-888-863-3936

info@infradog.com
http://www.infradog.com

Table of Contents

Introduction

Information security is a key consideration for all IT organizations. Multi-device access enables users to be able to access corporate information, file and data from anywhere, but broader access represents another potential attack surface.

When you consider moving your organization to cloud services for productivity services, you have to be able to trust your service provider to take care of the key expectations around processing and managing your data – security and privacy.

Security in InfraDog is an ongoing process, not a steady state. It is constantly maintained, enhanced and verified. We strive to keep software and hardware technologies up to date and refined through robust designing, building, operating and supporting process.

Service-Level Security

Physical layer – facility and network security

Facility

InfraDog uses service providers which provides highest security compliance to store customer data, including Microsoft Azure, etc.

Network

Our network security only allows connections and communications that are necessary to allow systems to operate, blocking all other ports, protocols and connections. Networks within InfraDog data centers are further segmented to provide physical separation of critical back-end servers and storage devices from public facing interfaces.

Logical layer – host, application, admin user

Automated operations

Most of the operations performed on hosts and applications by administrators are automated so that human intervention is reduced to a minimum, reducing the possibility of an inconsistent configuration or a malicious activity.

Admin access to data

Administrator access to InfraDog cloud and your data is strictly controlled. Access control happens at various at various levels:

1. Strict account management, only essential to the task may perform the task
2. Role based access control

Anti-malware, patching and configuration management

The use of anti-malware software is principal mechanism for protection of your assets in InfraDog cloud from malicious software. Changes, such as updates, hotfixes and patches to our cloud servers are mandated by Microsoft Azure. Furthermore, when InfraDog upgrades the software, latest system is always selected for deployment.

Data layer – data

InfraDog cloud is highly scalable multi-tenant service, which means that your data securely shares the some of the same hardware resources as other customers. We have designed InfraDog cloud to host multiple customers in the service in a highly secure way through data isolation.

Data integrity and encryption

Our services follow industry cryptographic standards such as SSL/TLS (Secure Sockets Layer / Transport Layer Security), AES, etc. to protect confidentiality and integrity of data.

All customer-facing servers negotiate secure session using SSL/TLS (Secure Sockets Layer / Transport Layer Security) with client machines, including mobile devices, so as to secure the data in transit. This applies to various protocols such as HTTP(S).

To further protect your data in InfraDog cloud service, some of the data are stored or transported as encrypted by Advanced Encryption Standard (AES) 128bit or AES 256bit.

Independent verification

Service providers providing services to InfraDog are certified, audited by ISO/IEC 2701:2005 Audit and Certification, SOC 1 and SOC 2 SSAE 16/ISAE 3402 Attestations, Cloud Security Alliance Cloud Controls Matrix, Federal Risk and Authorization Management Program (FedRAMP), Payment Card Industry (PCI) Data Security Standards (DSS) Level 1, United Kingdom G-Cloud Impact Level 2 Accreditation, HIPAA Business Associate Agreement (BAA), Family Educational Rights and Privacy Act (FERPA).

On-premise Security

Network layer

Software required to be installed customer data infrastructure doesn't require firewall port to be opened. Dynamic ports are opened when mobile device requests to access corporate data, and will be closed automatically once such data request is fulfilled. This further reduces possibility of hacking attacks, such as DDOS attack, port scans, etc. When user to access corporate data, such as corporate SharePoint web sites, file folder and Active Directory information, the connection is directly established between mobile device and software installed in corporate network, and data is encrypted to be transferred. InfraDog cloud will not monitor the data being transferred mobile device and corporate infrastructure.

Data encryption

Sensitive data are encrypted by Advanced Encryption Standard (AES) 128bit or AES 256bit with the software installed in customer server.

Data privacy

Passwords which are required to access customers' infrastructure to provide InfraDog access are strictly stored on the server where the software is installed, not uploaded to InfraDog cloud. Only essential data are uploaded to InfraDog cloud for system maintenance. User data, such as Active Directory user information, file shares and SharePoint sites are accessed real time through mobile device and corporate infrastructure. Such data will never be uploaded to InfraDog cloud for storage or caching.

Essential Data uploaded to cloud

Server Admin

1. **Windows computers** – hardware model/serial number/OS version/CPU/memory/network information
2. **VMware** – OS version/CPU/memory/network information
3. **Active directory** – domain controller IP
4. **IPMI** – hardware information/temperature/fan readings
5. **Network device** – network information

Employee Self-Service

1. Self-service basic configuration, enabled domain, OU, email reminder days, two factor enabled, mobile PIN enforced
2. Announcement
3. Shared folder and SharePoint site configuration (no password)
4. Security questions and answers (AES-256 encrypted)

Mobile Device Security

Data store and encryption

Only minimal data are stored in InfraDog mobile app, including Server Admin and Self-Service to provide access for the mobile app to corporate infrastructure. Password is encrypted by AES 256bit and stored with built-in mobile OS keychain service to ensure highest level security. Other data are encrypted by AES 256bit if necessary.

Data privacy

Data stored with InfraDog app will be deleted when the mobile app is reset, initiated by user or admin. If the mobile app is uninstalled from the mobile device, all the data stored with the app will also be removed at the same time.

Mobile device protection

System administrators have the option to enforce PIN code protection on the app. When the option is turned on, user will be required to enter PIN code every time to access the app. This provides extra layer of security to protect the app being misused.

In the event mobile device is lost, user will be able remotely reset the app and data by logging to other mobile device, or request administrators to reset the app from administration portal provided by InfraDog.

Privacy

When you entrust your data to InfraDog cloud, you remain the sole owner: you retain the rights, title, and interest in the data you store in InfraDog cloud.

- We do not mine your data for advertising or for any other purpose other than providing you services you have paid for.
- If you ever choose to leave the service, all configurations stored in InfraDog cloud will be removed permanently from our database.

Appendix

Infrastructure Architecture

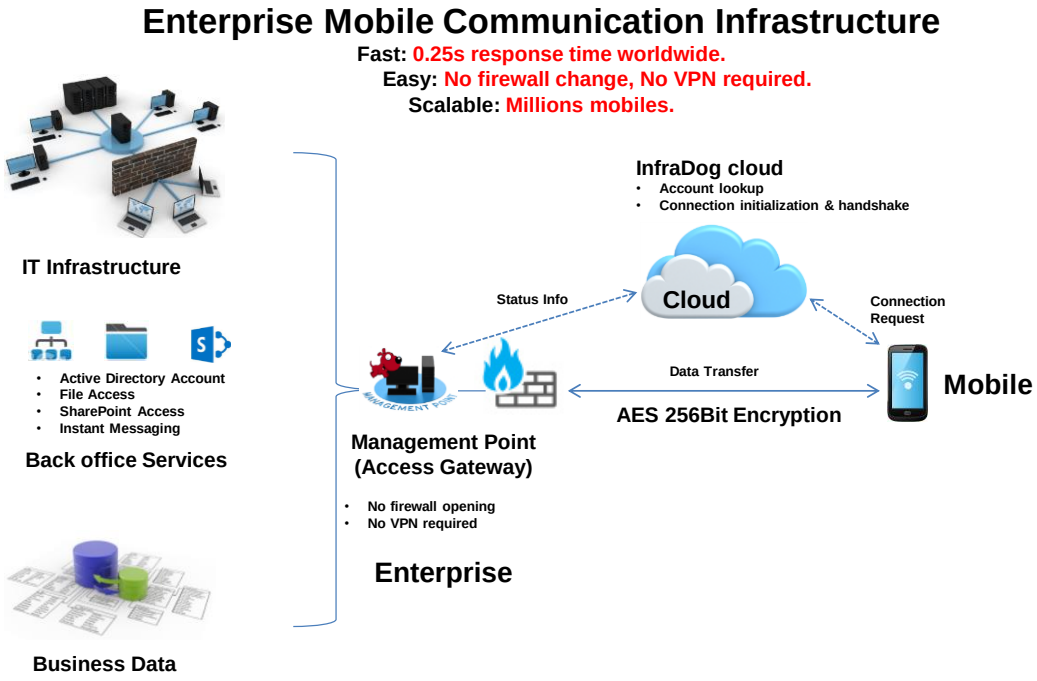

Figure 1. InfraDog Cloud Infrastructure Architecture