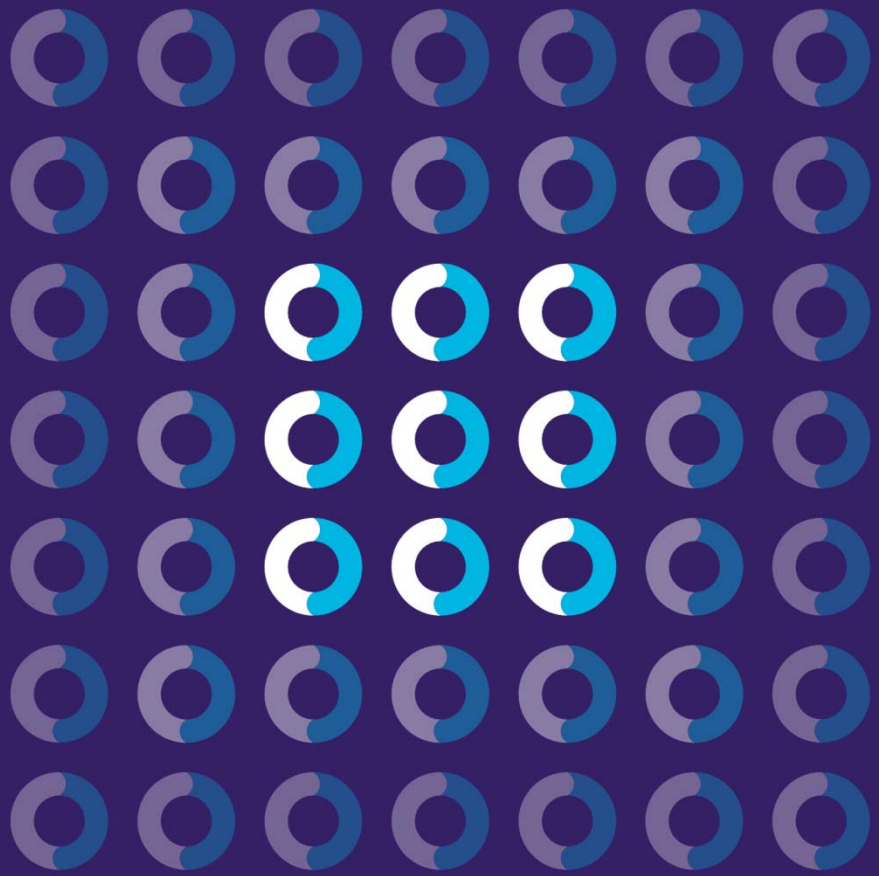
Teladoc HEALTH

Enterprise Security Overview



Enterprise Security Overview

Agenda

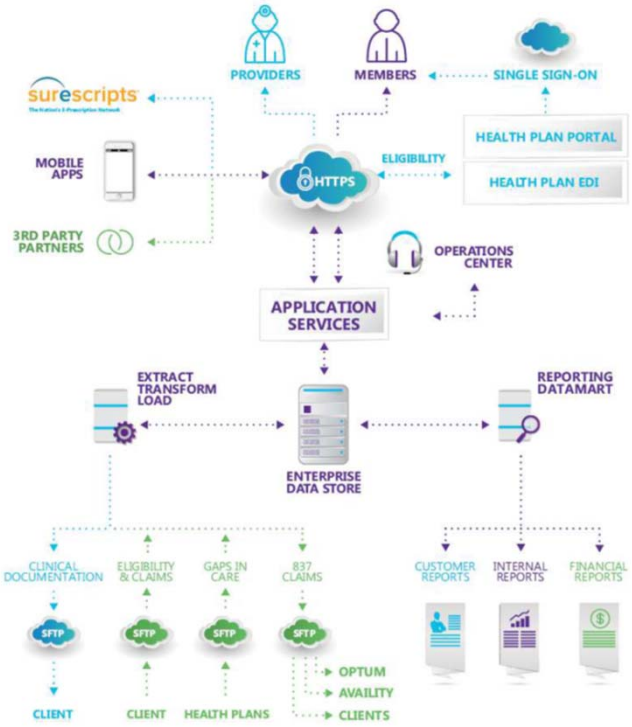
- Data Flows
- Risk Profile
- Security Program Overview
- Application Architecture
- Enterprise Security Architecture

Teladoc HEALTH

Data Flows

Teladoc Health solutions do not require access to client systems and only transmits sensitive data via encrypted means.

- Eligibility information is encrypted directly from the client to Teladoc Health via SFTP or from the client's health plan to Teladoc Health.
- The Teladoc Health service is not embedded in the client's environment nor is there any connectivity between client networks and the Teladoc network
- Members register and access their accounts securely via web browser and/or native iOS and Android apps



© 2002–2020 Teladoc Health, Inc. All rights reserved.

Risk Profile

- We do not access client networks or servers, nor do we enter client worksites or data centers
- We do not store credit card data. We transmit credit card data to a PCI certified credit card processor.
- We do collect Personal Identifiable Information (PII) and Personal Health Information (PHI) from employees of our clients
- We will send PII via encrypted means to a vendor for Welcome Kit fulfillment (if applicable).
- We do send PHI to an eRX service provider for electronic prescribing when clinically appropriate. All transmissions are encrypted, and the vendor has executed a BAA and is subject to annual vendor risk assessment program.
- We do send data for claims processing to a health plan clearinghouse. All transmissions are encrypted. The vendor has executed a BAA and is subject to annual vendor security review program.

© 2002–2020 Teladoc Health, Inc. All rights reserved.

Security Program - Overview

Meeting legal and data privacy standards through a comprehensive iformation security program.

Teladoc security program highlights addressing the regulation:

- PHI lifecycle governed through classification, access, handling and disposal policy
- Only authorized personnel can access patient medical records (NOT developers or designers)
- Incident response is a continuous process as new threats or changes to the business occur.
- Formal change management process promotes SoD and provides gate for all high risk activities
- Disaster recovery plan is updated and tested, at least annually.
- Mandatory Business Associate Agreements with all material third parties
- Background checks conducted for all employees and contractors including perpetual OIG list
- NDAs are signed with all employees, vendors, and partners
- Training program include initial and annual security awareness training as well as departmental specific offerings for all employees

© 2002–2020 Teladoc Health, Inc. All rights reserved.

Security Program - Overview

Teladoc Health security program follows the NIST cyber security framework and has been HITRUST certified since July 2017.

In addition, Teladoc:

- Role base access control enforce 'least privilege' principal, user/entitlement review is conducted quarterly on all sensitive systems.
- Conduct annual HIPAA, NIST Cyber (800-53) and SOC II Type II assessments of its security program via independent third parties
- Conduct monthly external web application vulnerability scanning via third party
- Conduct bi-annual application penetration tests via internal and external teams
- Ongoing risk management program identifies new threats and risks
- Vendor risk management program is conducted annually on all material vendors

© 2002–2020 Teladoc Health, Inc. All rights reserved.

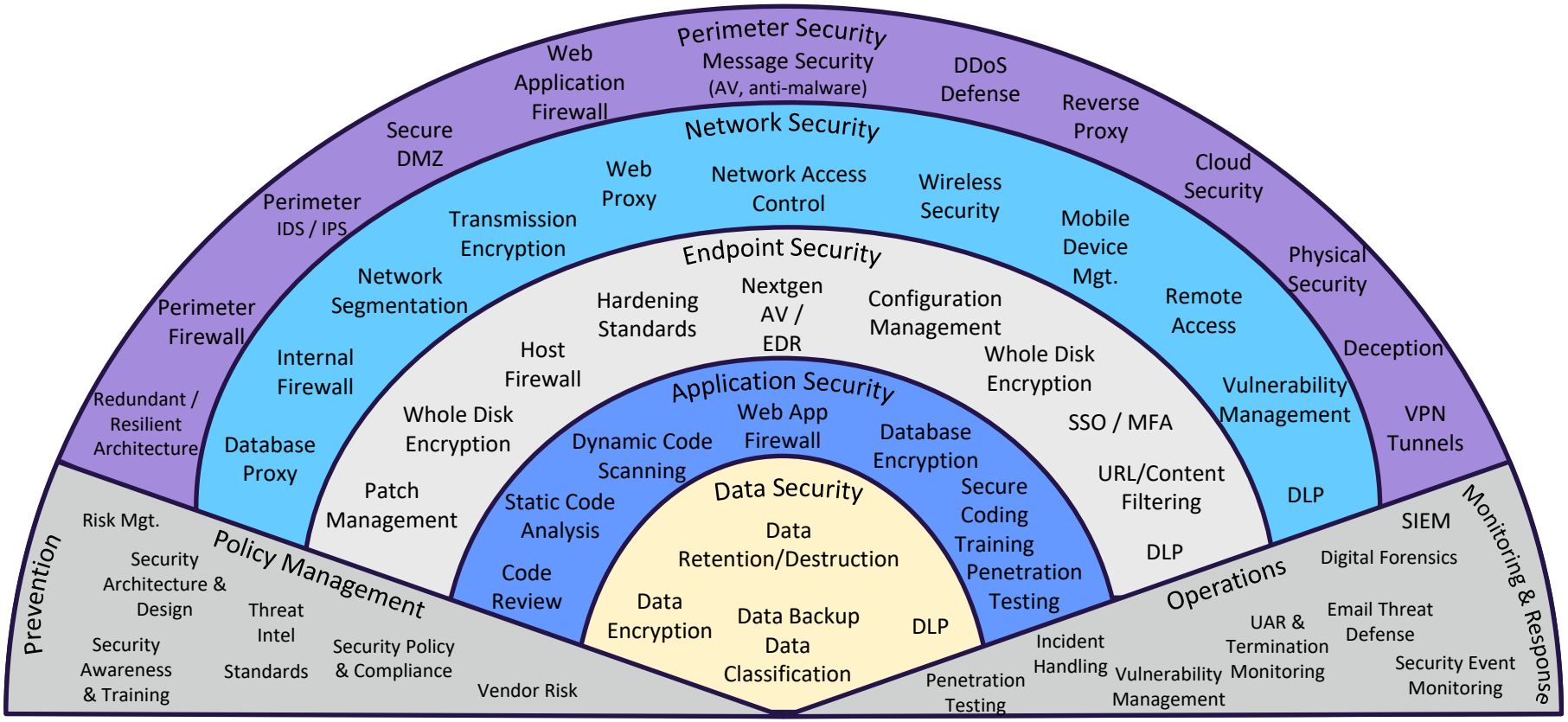
Application Security Architecture

Teladoc Health's internet-facing and back-end systems are architected to protect client and member data from cybersecurity threats.

- Firewalls, IDS/IPS, and reverse proxies provide perimeter security and layered defenses
- N-Tier architecture separates DMZ network from database network via firewall
- SSL termination of Internet traffic on load balancers
- DDoS and WAF sit in front of the application to provide advanced threat protection
- SDLC incorporates security checkpoints throughout the development lifecycle
- Mandatory annual developer training focused on defensive coding / OWASP top 10
- Secure email capability and TLS option for partners
- Registration process requires matching on demographic eligibility data provided by clients
- Unique user ID with complex password requirements / Automatic idle timeout
- HIPAA compliant encrypted video technology
- SSO available via SAML v. 2.0 specification

© 2002–2020 Teladoc Health, Inc. All rights reserved.

Enterprise Security Architecture



Teladoc HEALTH

© 2002–2020 Teladoc Health, Inc. All rights reserved.

Teladoc HEALTH

Teladoc Information Security

Jeff Nadler
Chief Information Officer
jnadler@teladochealth.com

John Mutuski
Chief Information Security Officer
jmutuski@teladochealth.com