Cloudbyz ITPM

Force.com Platform Security and Network Architecture

CLOUDBYZ

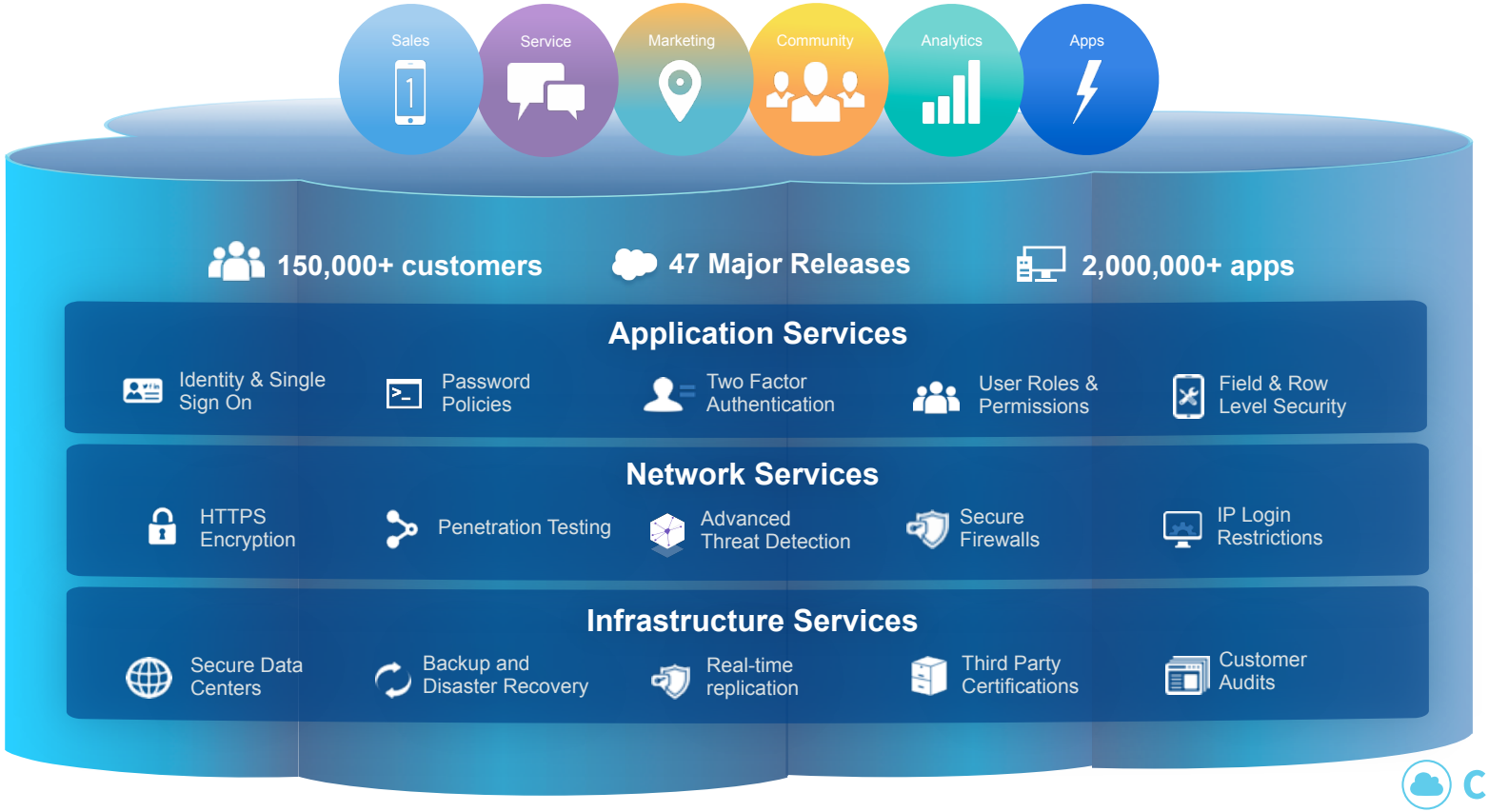
Force.com Platform

Common data model, workflows, and collaboration. Built for desktop and mobile.

CLOUDBYZ

Salesforce Trust Platform

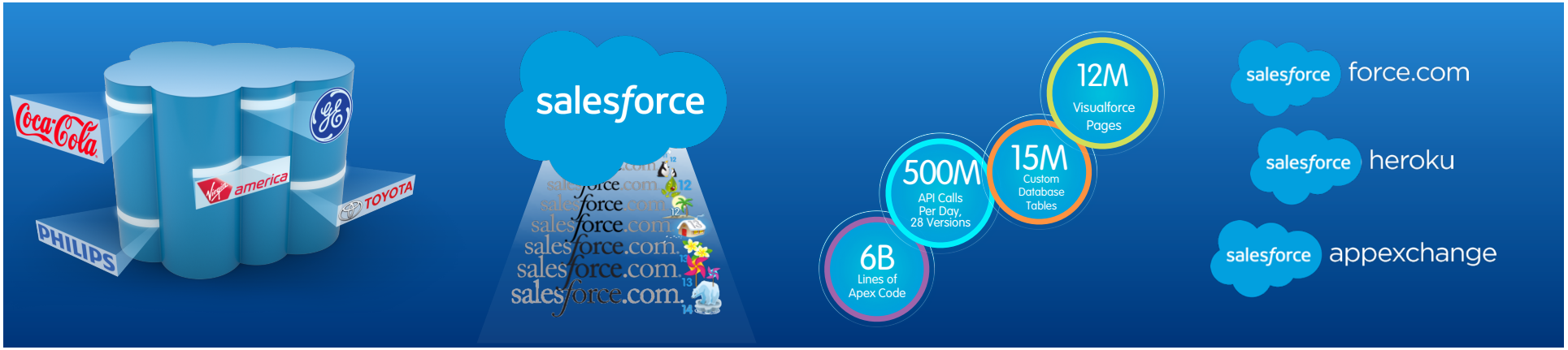
Sixteen years of innovation on the world's most trusted cloud



CLOUDBYZ

The Power of the Salesforce1 Platform

Multi-tenant Infrastructure



Metadata-based Single Code Base and Shared Infrastructure

Automatic Upgrades

46 Major Releases (3x /year)

Unbreakable Customizations

Integrations and customizations auto-upgraded

Open & Extensible

API-First Architecture
2700+ AppExchange Apps

CLOUDBYZ

Now Cloud Computing is the Enterprise Standard

Enterprise
Cloud Computing





Fast	Innovative	Open	Easy	Trusted
No Hardware	Flexible	Any Device	Subscription Model	Secure
No Software	Automatic Upgrades	API First	Real-time	Transparent
Faster ROI	Continuous	Data Portability	Customizations	Performance at Scale
	Improvement		AppExchange	

CLOUDBYZ

Salesforce is Recognized as the #1 Enterprise Cloud Platform

- World's Most Trusted Enterprise Cloud

salesforce 1 platform

#1 IDC Market Share

#1 FORRESTER® Enterprise Platform

Gartner
January, 2014

Magic Quadrant for
Application Platform as a Service

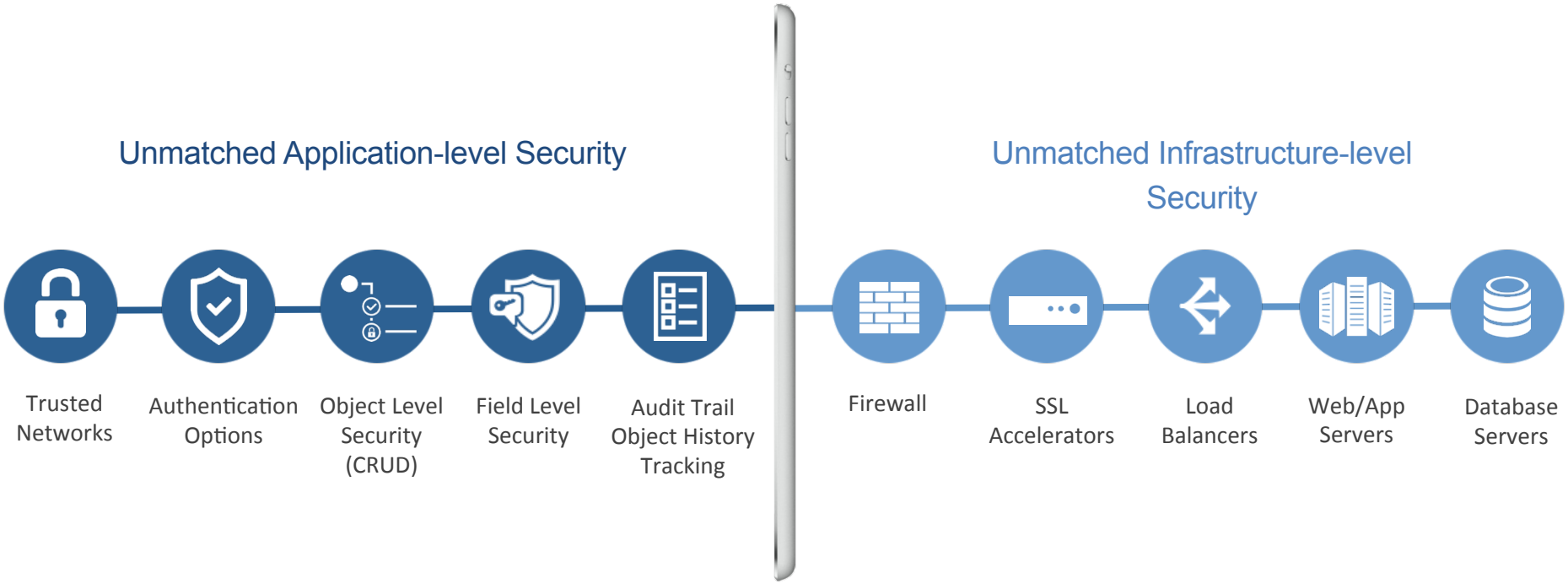
Analyst: Yefim V. Natis

211B+
Q1 Transactions

150k
Customers

2M+
Apps

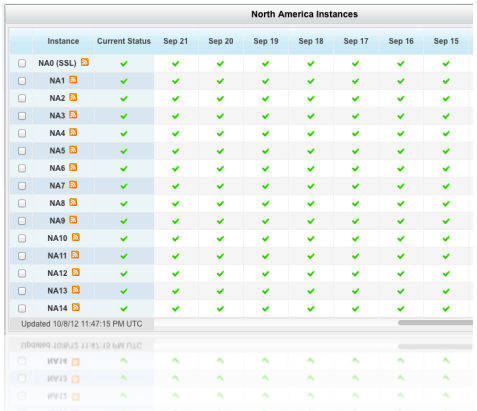
Trust: Security At Every Level

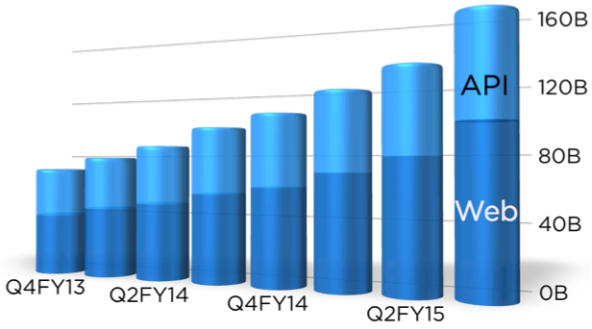


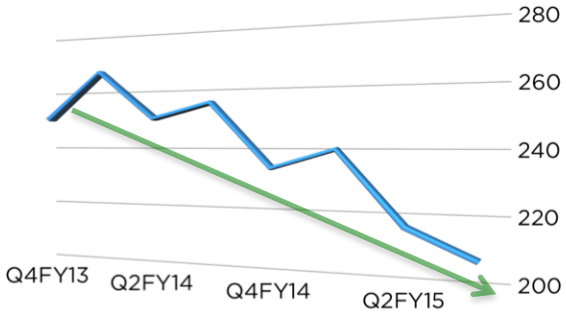
* Applicable to the Sales Cloud, Service Cloud, Communities, Chatter, database.com, site.com and Force.com. For audits, certification and security information or other services, please see the Trust & Compliance section of help.salesforce.com.

Trust: Our Highest Value

- trust.salesforce.com

Trust.salesforce.com	Transactions per quarter	Average Page Time
	159B Transactions in Q1FY15 51% YOY Growth	207ms Latency in Q1FY15 12% YOY Improvement





All Major Security Certification

AICPA SOC · AICPA SOC 2 · SOC 3 · HIPAA · FINRA · PCI · Norton SECURED powered by Symantec · GSA · BSI ISO 27001 IS 534200 · SAS 70 Type II · SysTrust · SAFEHARBOR · TRUSTe EU SAFE HARBOR · TRUSTe CERTIFIED PRIVACY · TÜV Geprüfter Datenschutz · プライバシーマーク制度 PRIVACYMARK SYSTEM

CLOUDBYZ

Force.com Cloud Computing Platform

Multi-Level Security

Host Security	Logical Network Security	Database Security	Multi-Tenant Application Security
Media Management Security	Transmission Level Security	Multi-Tenant Architecture Security	DDOS Security
Customer Controlled Security	Multiple Authentication	Encryption and Data Protection	Security Monitoring
Forensics Services	Security Audits	Internal Vulnerability Assessments	External Vulnerability Assessments

Fully Mirrored Cloud Computing Infrastructure

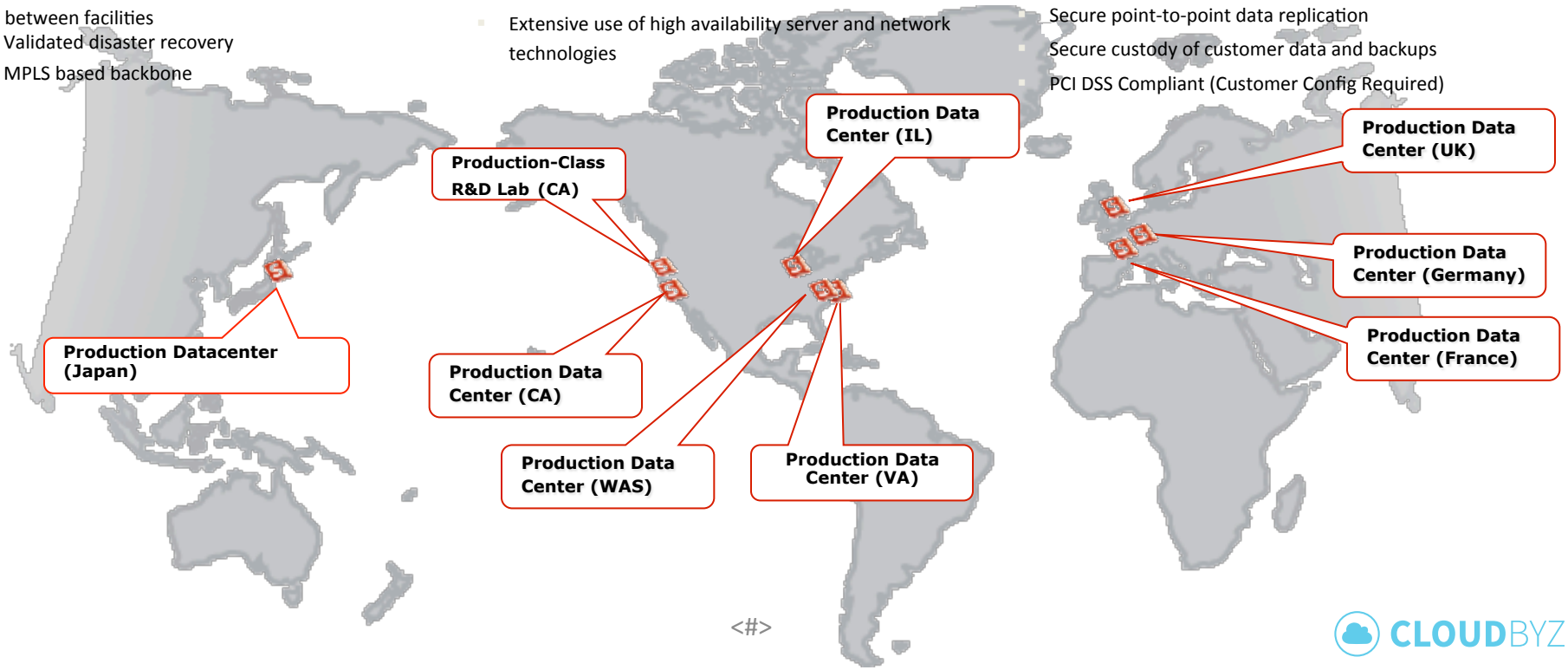
Continued Investments. Unparalleled Confidence.

force.com cloud infrastructure

- Unmatched Reliability
- 5 mirrored production data centers plus isolated production-class lab facility
- Near real time replication between facilities
- Validated disaster recovery
- MPLS based backbone

- Maximum Uptime & Performance
- Carrier neutral network strategy
- No single points of failure
- Carrier level scalability
- Extensive use of high availability server and network technologies

- Trusted Security
- World-class security specs
- SOC-1, 2, & 3
- ISO 27001 Certified
- Secure point-to-point data replication
- Secure custody of customer data and backups
- PCI DSS Compliant (Customer Config Required)



CLOUDBYZ

Fully Mirrored Cloud Computing Infrastructure

Continued Investments. Unparalleled Confidence.

force.com cloud infrastructure

Security: Facilities

Maximum Facilities Security

- 24 x 365 on-site security
- All doors, including cages, are secured through a combination of biometrics and/or proximity card readers.
- Multiple security challenges required to reach Salesforce environment
- Low profile fully anonymous exteriors
- Digital camera (CCTV) coverage of entire facility
- Perimeter bounded by concrete bollards/planters
- A silent alarm and automatic notification of appropriate law enforcement officials protect all exterior entrances.
- CCTV integrated with access control and alarm system.
- Motion-detection for lighting and CCTV coverage.

World-Class Infrastructure

Delivering leading On-Demand availability

- Five production data centers and a production-scale lab facility worldwide:
  - 70,000 + total sq. feet of cage environment across six data centers.
  - Mirroring is about more than just having a copy of your data
  - Salesforce.com maintains a full-scale replica of the production facility as well as your data
- Power:
  - Next generation UPS systems based on battery banks & rotary fly wheel machines setup in an N+1 configuration
    - Designed to maintain uninterrupted power supply to customer load.
    - Provides transparent transition from UPS to generator load in the event of utility disturbance.
    - Guaranteed backup fuel supply
- Cooling:
  - Precision, minimum N+1 HVAC
  - Hot/Cold Aisle Configuration
  - Guaranteed by backup water supply

CLOUDBYZ

Network

Industry leading performance, scalability and redundancy

- **Carrier-class and carrier-neutral model: multiple transit vendors**

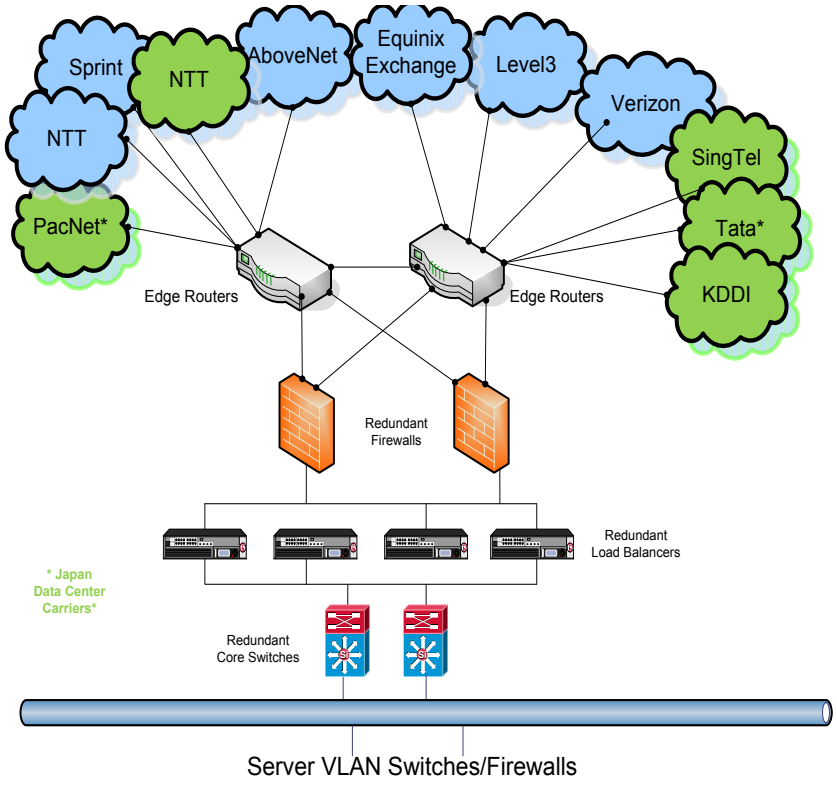
AboveNet	**NTT (APAC)**
Verizon	**PacNet (APAC)**
Level 3	**Tata (APAC)**
NTT	**KDDI (APAC)**
Equinix Exchange	**SingTel (APAC)**

- **Lightning-fast performance worldwide**
  - Data centers located at core Internet hubs
  - Multi-gigabit IP transit for external customer service
  - Access to thousands of global Internet peering points
  - Private peering with key carriers and partners (30+)
- **MPLS/ VPLS Network Architecture**
  - Encrypted, self-healing network paths between all datacenters
  - 10 Gigabit Ethernet-based backbone ensures bandwidth for current and future needs
  - Network architecture provides multiple global secure Points of Presence (PoP) for efficient data replication.
  - Multiple, diverse-path carriers
  - Dedicated bandwidth and devices for inter-site traffic ensures internet-bound (customer) traffic does not compete with inter-site traffic
- **Highly Available Network Architecture**
  - No single-points-of-failure
  - Globally dispersed DNS
  - Critical devices all use active-active or quick-failover configurations
  - Multiple paths between sites and critical devices allows routing to avoid problems

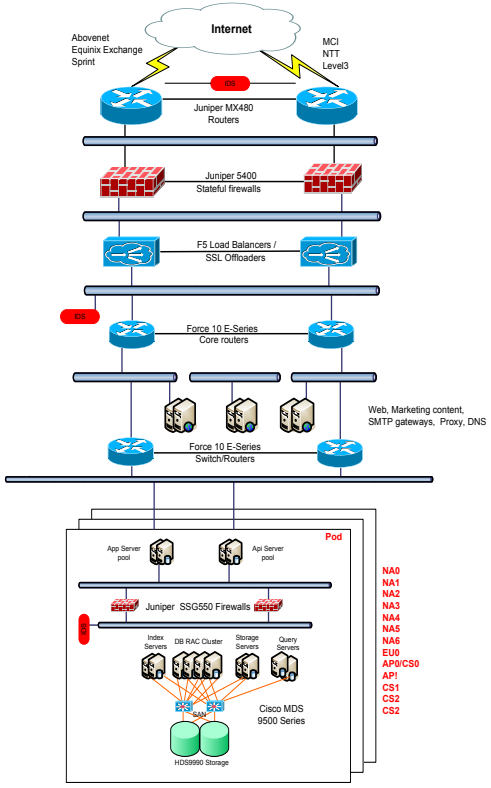
- Multiple Network Carriers For:
  - Customer connectivity
    - Multiple ISP's for customer transit
  - Internal replication
    - Multiple dedicated connections for DR/BCP.
- Redundant Routers at Entry Points
- Fail-over Configured Firewalls
- Redundant &Load Balancers
- Redundant Hubs/Switches at VLANs
- Web, Application, API, Cache, Search, Index, Query, Batch Servers
  - Load Balanced, Fail-over / Clustered
- Data Base Servers
  - Oracle RAC EE
  - 8 Node Clusters (CRS & ASM) sized to sustain Peak Load if Node fails
- Storage
  - Multiple paths for reliability
  - 4 inter-connects per DBMS Server
  - Alternate paths to separate Storage Directors

Network

Industry leading performance, scalability and redundancy



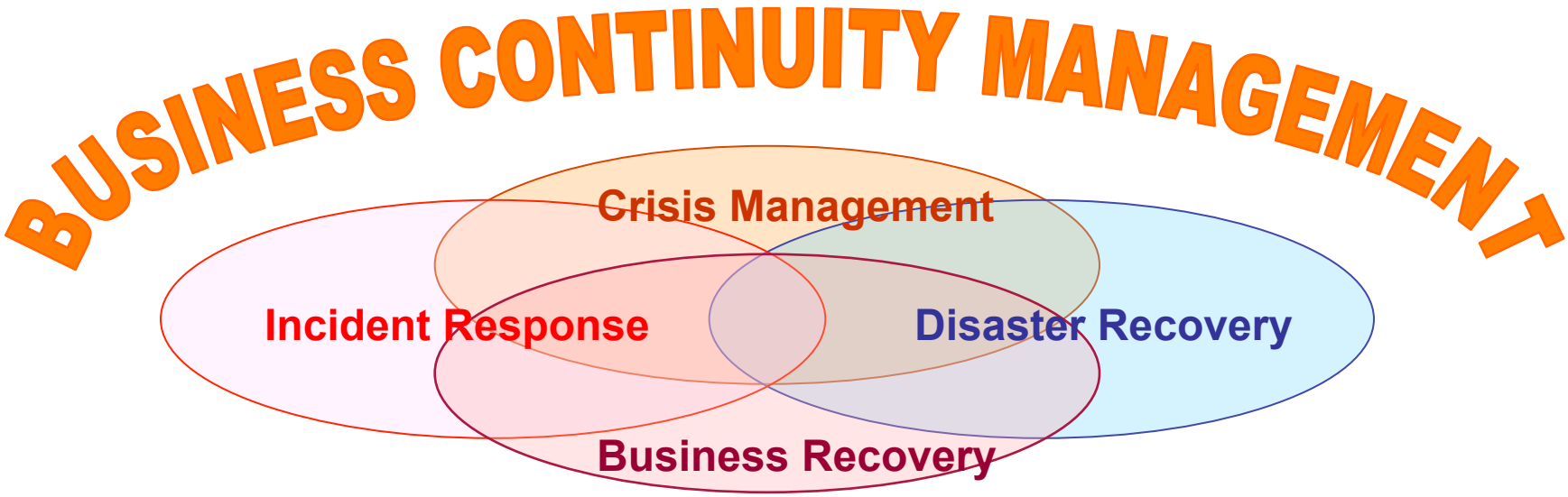
Multiple Network Carriers and Redundancy at the Edge



Data Flow

Logical Network Diagram

Holistic DR Approach



Disaster Recovery Summary

- Holistic approach to Continuity Planning
  - Executive Management support and participation
- Un-paralleled Disaster Recovery strategy
  - 100% Data Center replication (Network, Storage and Servers)
  - Near real time data replication
- Proven Disaster Recovery Plan
  - Exercised in a production environment with client participation
  - Cross functional response through entire SFDC organization
  - Exercises managed from 3 countries
  - Customer Participation

Disaster Recovery

- Follows the Disaster Recovery Institute International (DRII) methodology

- In Compliance with the following standards:
  - SAS/70 Type II attestation
  - ISO27001 Certification (April 2008)

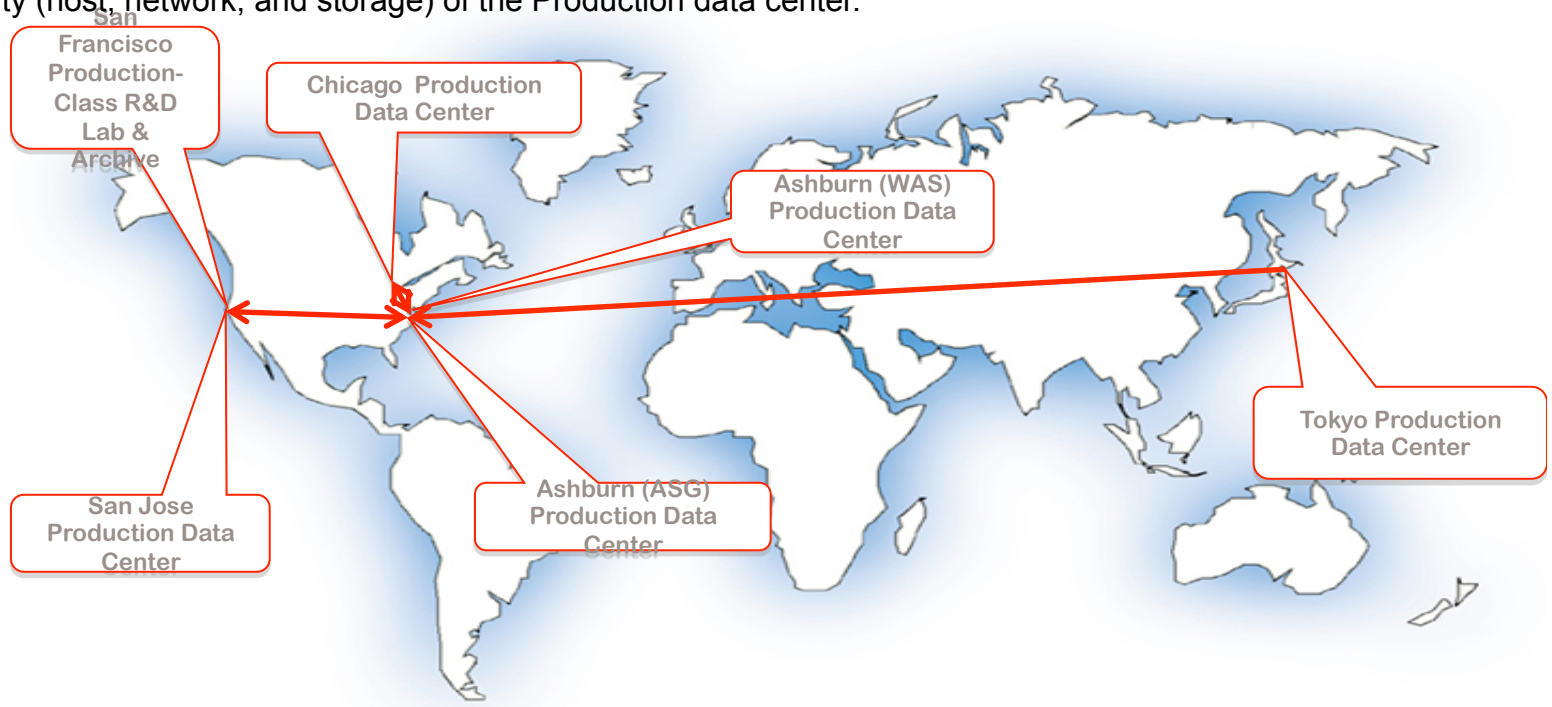
CLOUDBYZ

Disaster Recovery Strategy

Salesforce.com (SFDC) maintains a Mirror Site that is 100% staged warm site with near-real time data replication. The secondary data center is replicated at 100% of capacity (host, network, and storage) of the Production data center.

Focus on Infrastructure

- Near real-time replication
- Validated disaster recovery strategy
- Secure encrypted point to point data replication
- Weekly p
- p Schedule- Multiple Full / Multiple Incremental
- Carrier neutral network strategy
- MPLS / VPLS Network Architecture



Information Security Operations

- Dedicated Information Security Organization
- Strategy/Charter
- Mitigate risks while complying with legal, statutory, contractual, and internally developed requirements
- Develop and enforce policies and procedures
  - Design and secure information systems using security domains, defense in-depth and least privilege principles
  - Develop and integrate security architecture into business processes (CobiT, ISO27002)
  - Conduct employee security awareness training classes
  - Perform regular vulnerability assessments and audits
- Addresses all layers
  - Physical Security
  - Logical Network Security
  - Host Security
  - Transmission Level Security
  - Database Security
  - Development Lifecycle

CLOUDBYZ

Worldwide Security Certifications

force.com cloud infrastructure

- ISO 27001
- SSAE 16 (SOC 1, 2, and 3)
- GSA moderate level ‘Authority to Operate’
- PCI DSS
- JIPDC (Japan Privacy Seal)
- Tuv (Germany Privacy Mark)
- SysTrust

BSI ISO 27001 IS 534200 · SAS 70 Type II · SysTrust · SAFEHARBOR · TRUSTe EU SAFE HARBOR · TRUSTe CERTIFIED PRIVACY · TÜV Geprüfter Datenschutz · プライバシーマーク制度 PRIVACYMARK SYSTEM

CLOUDBYZ

Operational Access Control

- Private management network
  - 2-Factor Authentication
  - Secure Global Desktop
    - Restrict cut/paste, public IM, print, data copying
  - Bastion host for terminal services
  - Bluecoat proxy server for authorized web services
  - Imperva DBA activity monitoring

- Configure systems and devices for least privilege

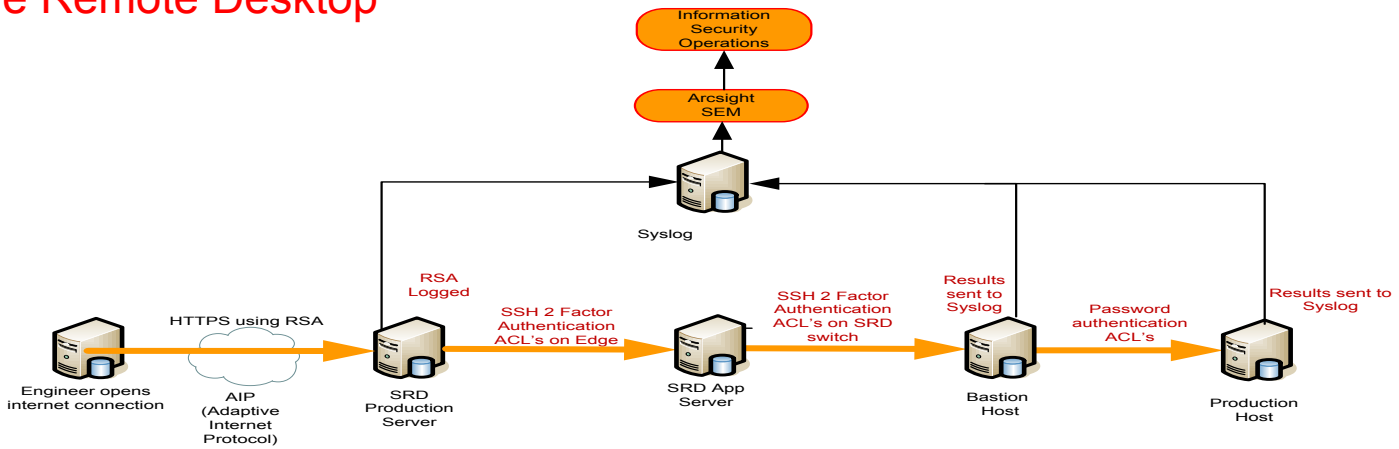
- Salesforce service managed by FTEs only

- Background Checks
  - HireRight
  - Seven year criminal background check
  - Employment, education verification
  - Motor Vehicle, Social Security records
  - References

CLOUDBYZ

Technical Operations Management

Secure Remote Desktop



Key Points

- Datacenter access through secured terminal servers located in each datacenter.
- Terminal server client restricts/prevents copy/paste and file transfer between remote systems and client workstation.
- Internet access via dedicated, logged content filters.
- No access to corporate services (email, etc).
- Strong SSL encryption of all network communications between an employee's terminal and the terminal servers is enforced.
- Establishing a terminal server session requires the use of two-factor authentication.
- Access into systems beyond the terminal server itself requires additional, separate authentication.
- All terminal server administrative and user sessions and the applications utilized during those sessions are logged in detail. These logs are maintained in a secure area to prevent tampering.
- Terminal server sessions are managed, enabling access point administrators to immediately terminate all sessions associated with a user in case such a need arises.

force.com cloud infrastructure

Host Security

- Linux and Solaris systems only
- Hardening
  - Remove unnecessary processes, accounts, protocols
  - Change defaults, remove banners
  - Don't run services as 'root'
  - Patching
- Kerberos Authentication
  - Uses strong cryptography
  - Requires mutual authentication
- Central logging
- Load balanced App - Stateless app/web tier
- Resin/Java
- Anti-Virus

CLOUDBYZ

Media Management Security

Salesforce.com follows **NIST SP 800-88 Data Disposal Standards**:

Failed hard drives undergo 3 pass data overwriting procedure performed in house **(clearing)**

Secure chain of custody

Mechanically failed hard drives & backup tape media are securely **purged & destroyed.**

Process validated and independently audited against NIST 800-53 Rev. 3 requirements.

Logical Network Security

- Perimeter Edge Routers (Juniper MX480)
- Stateful Firewalls (Juniper)
- Load Balancers (F5)
  - NAT, RFC1918
- Core Routers (Force10) / core firewalls (Juniper)
- Bastion Hosts / 2-Factor auth (RSA)
- Intrusion Detection Systems (IBM/ISS)

Transmission Level Security

- SSL 128-bit Verisign Global Step up Certificates
  - Currently deploying EV Certs
- SSL Session terminates on F5 Load Balancers / SSL offloaders
- Email relay over TLS

Database Security

- Customer passwords are stored in DB using SHA256
- DBA Access
- Field level encryption
- Imperva database monitoring tool

Multi-Tenant Application Security

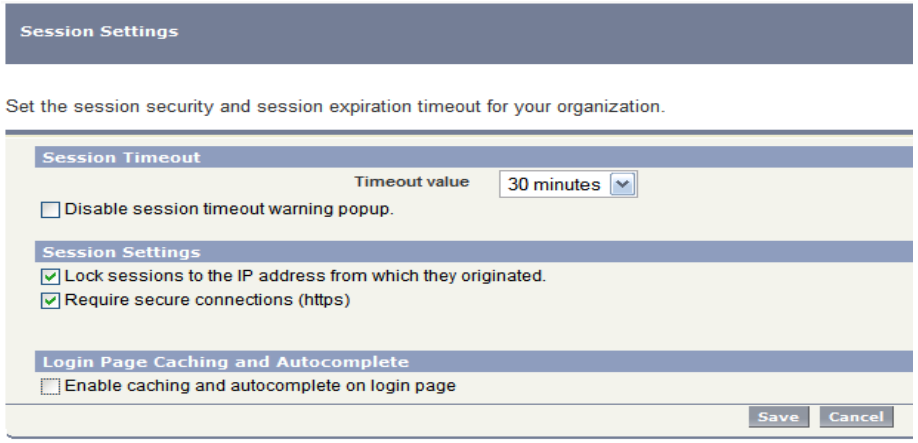
force.com cloud infrastructure

Strong Session Management

Every row in the database contains a base62-encoded ORG_ID - Unique encoded string. This field contains an internal identification of the organization that owns the row.

Session Tokens – user unique, non-predictable long random value generated for each session combined with a routing "hint" and checksum, base64 encoded

Contains no user-identifiable information
Session Timeout – 15 Mins to 8 Hrs
Lock Sessions to IP – prevent hijacking and replay attacks
SSLv3/TLS used to prevent token capture / session hijacking
Session Logout – Explicitly expire and destroy the session
Application self-monitors for security violations

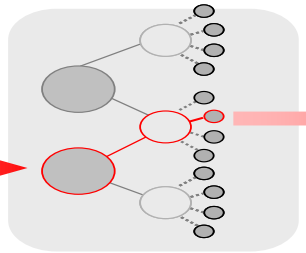


CLOUDBYZ

Multi-Tenant Application Security

force.com cloud infrastructure

Login... | Authenticate... | Apply Data Security Rules... | View Filtered Content



- User enters credential over SSLv3
  - Password policies checked
  - Identity Confirmation checked
- …or… SAML authentication
- Login Profile Restrictions che[illegible]

- Salesforce authenticates
  - Credential
  - Delegated Auth
- Unique, non-predictable session token issued
- All subsequent requests carry the session token
- Session token maps to user context
  - userID
  - orgID
- Client Hash Value set
  - orgID, userID,

- Client Hash Validator confirms calculated Client Hash Value matches Client Hash Value set on login
- Page rendered

- After login, any application request for database connection requires user context for request partitioning
- Org processing node and data partitioned by hash of orgID
- Every row in the database contains an orgID
- All DB queries include user context in “where” clause
- Proprietary sqlvalidator used in testing to scan all sql run by database to confirm inclusion of user context in “where” clause
- Every returned row confirmed against orgID value
- Client Hash Value calculated server side with each request

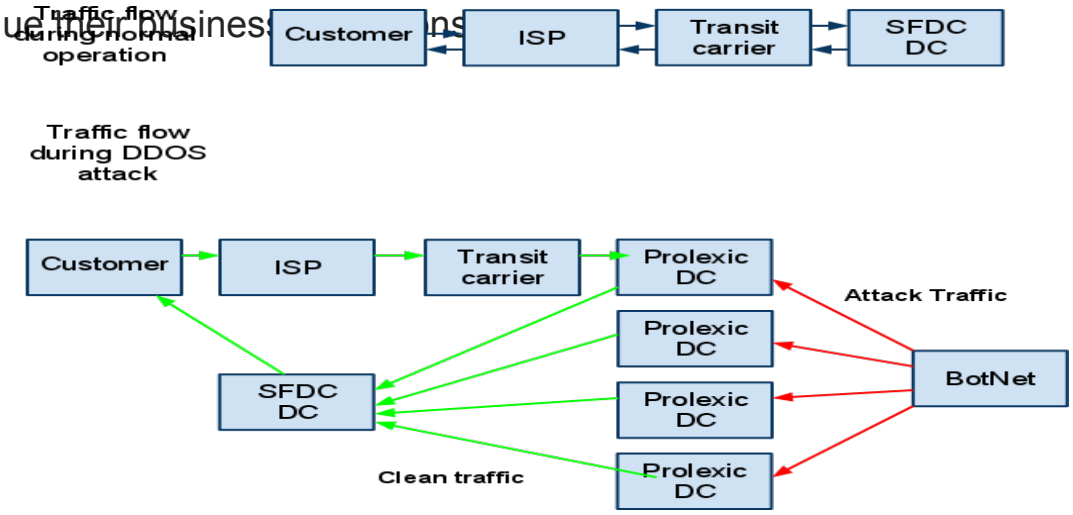
CLOUDBYZ

DDoS Protection

- Salesforce.com technology risk mitigation strategy put together to counter and continue business operations in the event of a well planned DDoS attack.

- DDOS vendor chosen to protect business from the “debilitating service disruptions caused by DDoS attacks.”

- Vendor has **geographically diverse data center** & operational presence to re-route Salesforce.com traffic to their facilities to ensure it is clean and ensure that our customer base can continue their business operations



Customer Controlled Security Features

force.com cloud infrastructure

Sophisticated sharing model

Login History log

CRUD and field level security

Setup Audit Trail log

Authentication options

Object history tracking

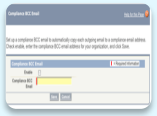
Trusted Networks

Compliance bcc

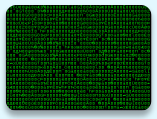
CLOUDBYZ

Customer Controlled Security Features

force.com cloud infrastructure


Sandbox environments


Automated user management


Encrypted Custom Fields & Apex encryption


APEX callouts/outbound messaging


User permissions


Portal Health Check Report

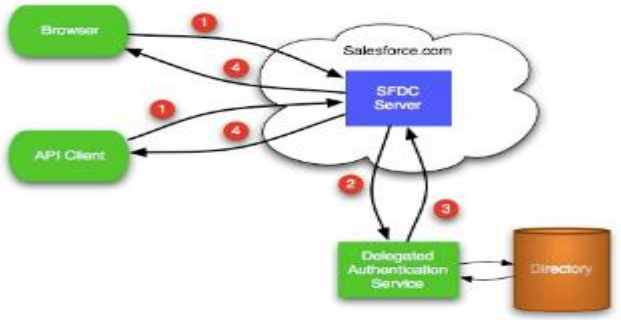

CAPTCHA for reports & export

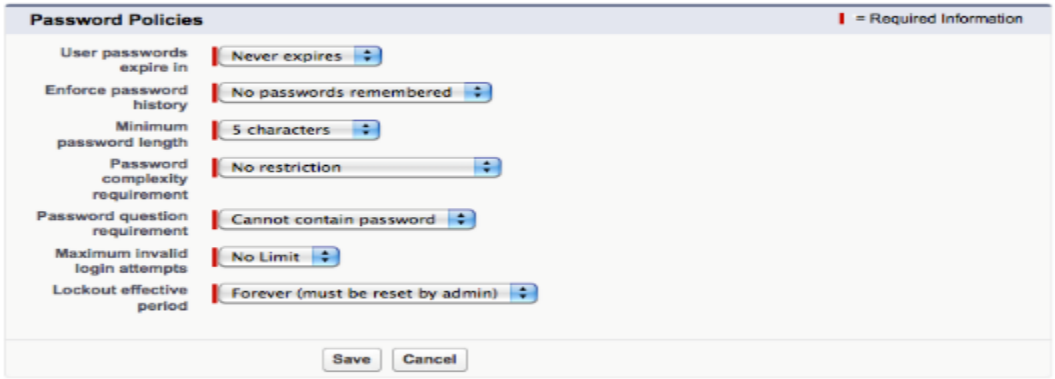

Security Health Check Application

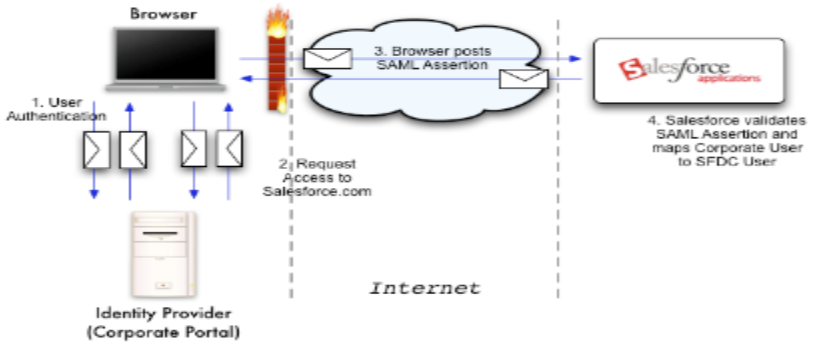
CLOUDBYZ

Authentication Options

- Salesforce.com native
- Delegated Authentication
- SAML 1.1 and SAML 2.0







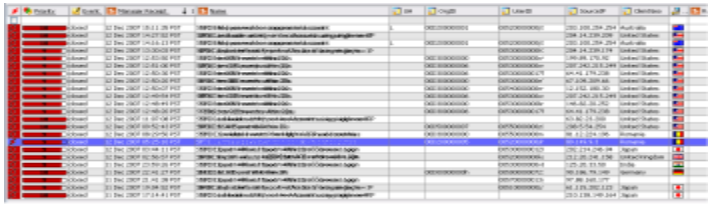
Encryption/Data Protection Options

force.com cloud infrastructure

Option	Description	Used When	Advantages	Challenges
Encrypted Custom Fields	Standard functionality: field contents are encrypted via 128-bit AES encryption; user perm required to view the actual data within salesforce; keys are manageable within salesforce	The exact data values are needed for the use of some functionality in salesforce.com and can be seen by select, logged in end users	• Encryption and Key Management are native functionality • Can be included in Reports, Search Results, Validation Rules, Apex Scripts	• Not availble for Standard Fields • No Search, Filtering, use in Workflow • Limit 175 characters • Fields still accessible by administrators • ECFs are always editable, regardless of whether the user has the correct perm
Apex Crypto Class	Provides algorithms for creating digests, message authentication codes, and signatures, in Apex code, as well as AES 128 – 256 bit encryption and decrypting information	Needing to encrypt larger fields or documents within salesforce or making encryption/decryption part of a larger business process and not automatic like with ECFs	• Native functionality that is fully extensible and customizable via additional Apex code • Can generate your own initialization vector or have salesforce do it for you	• Custom code, but leverages standard Apex functionality
Data Masking	Only part of a sensitive piece of data is stored in salesforce (e.g. last 4 digits of SSN or credit card number)	Typically with Call Centers: some part of the sensitive information is needed in the case management or identity verification process for a caller; end users should never know the whole value	• Sensitive data is "de-sensitized" before it gets to salesforce and rendered benign while still being able to support the business process	• None, if this is the proper use case and the unmasked values can still support their needed function

Security Monitoring

- Intrusion Detection Systems
- Arcsight Security Event Management
  - Devices, successful/failed logins, SU changes, etc.
- Application self monitoring
- Threat monitoring
  - SANS, CERT, OWASP, Cisco, F5, Redhat, etc..
- Continuous Perimeter Monitoring Service
- Third party monitoring of domain names, SSL certificates



Forensics Service

Customers have some basic tools (Admin Setup)

Login history log

Success/fail, source IP, Timestamps

Setup Audit Trail log

User, role, profile changes
Password policy changes
Mass deletes, transfers
Field level, page layout changes

Salesforce can provide Forensic web log analysis

Security Audits

- **ISO 27001 Certification**
  - International standard specifying requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System

- **SSAE-16 SOC2**
  - SSAE-16 (Standards on Attestation Engagements No. 16) attestation standard put forth by the Auditing standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) to evaluate the internal non-financial controls of a service provider.

- **SSAE-16 SOC3**
  - Effectiveness of controls relating to security, availability, processing integrity, privacy and confidentiality

Internal Vulnerability Assessments

Salesforce.com uses a multi-prong approach to ensure the software we release is secure.

- **Architecture Reviews**
  - Threat model features that are considered high risk.
- **Development**
  - Follow secure coding standards
  - All code prior to check in is reviewed.
  - Use code quality and security tools (Findbugs, Checkmarx.)
  - All developers receive annual application security training
- **Quality Engineering**
  - Use several black box analysis tools (Appscan, Paros, etc.)
  - All QE engineers receive annual application security training
- **Information Security**
  - Tests medium and high risk features.
  - Brings in third parties to perform code reviews (iSEC Partners, S&L)
  - Use Burp Suite and proprietary fuzzers

External Vulnerability Assessments

- MSSPs include WhiteHat, Solutionary, SPI Dynamics, Symantec
- Network Assessments and Application Assessments
- Assessments cover the following:
  - Cross-Site Scripting
  - Input validation
  - Buffer Overflow
  - SQL Injection
  - Directory Traversal
  - Parameter Overflow
  - Path Manipulation
  - Command Execution
  - Path Truncation
  - Character Encoding
  - Character Stripping
  - Site Search
  - Application Mapping
  - Automatic Form-Filling
  - Configuration Management
  - Proxy Support
  - Parameter Injection
  - Directory Enumeration
  - Authentication and Session Management
  - Web Server Assessment
  - HTTP Compliance
  - SSL Support and Strength
  - Certificate Analysis
  - Content Investigation
  - Spam Gateway Detection
  - Developer Comments
  - Absolute Path Detection
  - Error Handling
  - Permissions Assessment
  - Brute Force Authentication attacks
  - Known Attacks
  - Session Hijacking
  - Horizontal Attacks
  - Insecure Storage
- Executive Summaries available upon request

CLOUDBYZ

salesforce

ISV
PARTNER

Cloudbyz Inc is focused on building enterprise applications on force.com platform

www.cloudbyz.com | | info@cloudbyz.com | O: 630.748.8466

linkedin.com/company/cloudbyz

Facebook.com/cloudbyz

Twitter/cloudbyz

Plus.google.com/+cloudbyzinc

CLOUDBYZ