Progress®

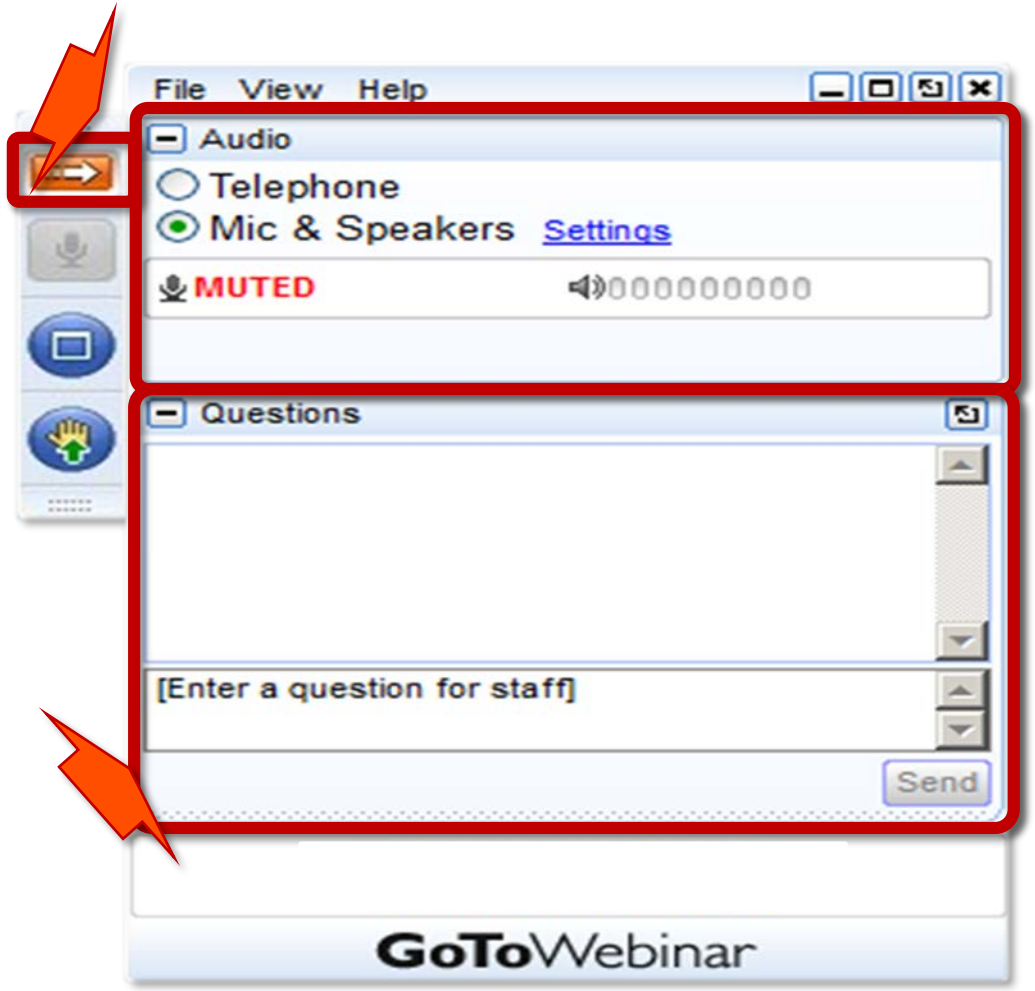
Enterprise Security in Data Access

Jim Silhavy, Software Engineering Manager

Brian Derwart, Principal Software Engineer

Phil Prudich, Principal Software Engineer

Audio Bridge Options & Question Submission



ogress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Progress®

Enterprise Security in Data Access

Jim Silhavy, Software Engineering Manager

Brian Derwart, Principal Software Engineer

Phil Prudich, Principal Software Engineer

Agenda

- Data Access Security Landscape
- Deep-Dive into Data Access Security
- How Progress configures and tests these complex environments
- DataDirect Security Vulnerability Policy

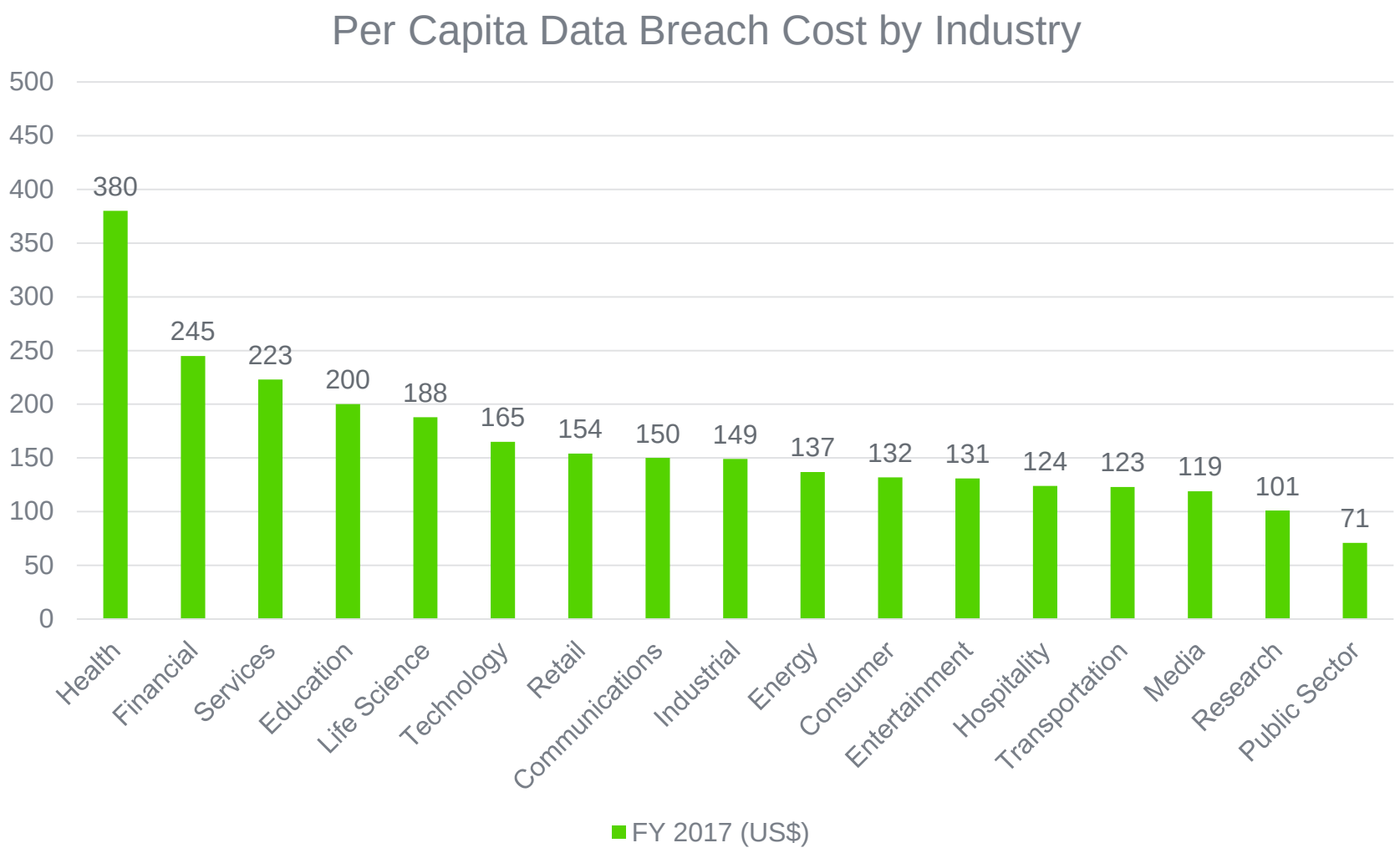
© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Data Access Security Landscape

$2.1 Trillion

Cost of Data Breaches by 2019

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.



Source: 2017 Ponemon Cost of Data Breach Study

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Enterprise Data Access Security is Highly Complex

1

Misuse of Credentials

Threats from within the organization and ex-employees

2

Security Breaches

Phishing, Malware, DoS... Ex: Poodle, Freak, Beast, etc.

3

Compliance Needs

HIPAA, FEDRAMP, SOX, FIPS 140-2 etc.

4

Data Privacy Laws

GDPR, FCRA, GLBA, COPPA, etc.

5

Variety of Solutions

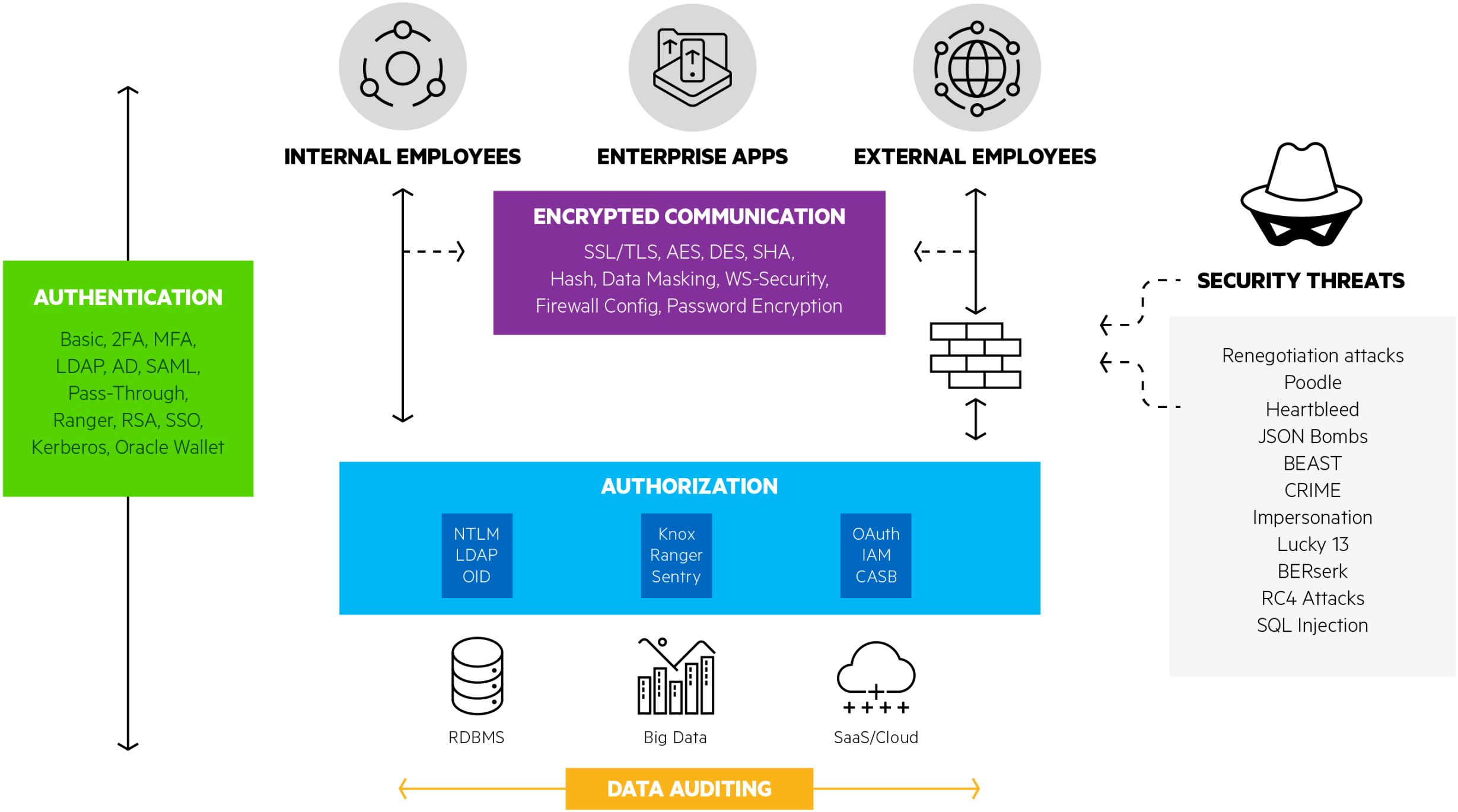
Enterprises adopt different technologies to solve the same problem. Ex: Kerberos, NTLM

6

Hybrid Environment

Security needs to be managed in the cloud, on the perimeter and on-premises

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.


INTERNAL EMPLOYEES
ENTERPRISE APPS
EXTERNAL EMPLOYEES
AUTHENTICATION
Basic, 2FA, MFA, LDAP, AD, SAML, Pass-Through, Ranger, RSA, SSO, Kerberos, Oracle Wallet
ENCRYPTED COMMUNICATION
SSL/TLS, AES, DES, SHA, Hash, Data Masking, WS-Security, Firewall Config, Password Encryption
SECURITY THREATS
Renegotiation attacks
Poodle
Heartbleed
JSON Bombs
BEAST
CRIME
Impersonation
Lucky 13
BERserk
RC4 Attacks
SQL Injection
AUTHORIZATION
NTLM LDAP OID
Knox Ranger Sentry
OAuth IAM CASB
RDBMS
Big Data
SaaS/Cloud
DATA AUDITING

Data Access Security in a Nutshell

Authentication

Ensure that an individual or application is who/what they claim to be

Authorization

Determine what actions a particular client can or cannot perform

Encryption

Protect sensitive data at all times – when at rest, in motion or in use

Data Auditing

Assess the quality, utility and security of data as it moves between systems

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Poll Question

- Where are you seeing increasing complexity with data access security?
  - Big Data and NoSQL sources
  - Enterprise databases such as Oracle and SQL Server
  - API Strategies
  - Hybrid Cloud and On-premises environments
  - Other

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Progress®

Deep-Dive into Data Access Security

Data Access Security Overview

Authentication

Anonymous
Basic
2FA
Kerberos
Single Sign-on

Authorization

Service-level
User vs Role-based
DB ,Table, Column
Read/Write
Data Masking

Encryption

SSL/TLS
Ciphers
Hash
Data Integrity
Data at Rest

Data Auditing

Logging
Monitoring
Alerts
Error Handling
Data Lineage

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Popular Enterprise Security Technologies

- Kerberos
  - Authentication
  - Authorization
  - Ticket management
- Active Directory
- LDAP
- NTLM (only for cross domain access)

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Relational Database Security Example

- Oracle Wallet
  - Manage DB credentials across multiple domains
  - PKI certificates
  - Encrypted database net service names
- Oracle Internet Directory
  - LDAP using Oracle database as storage
  - Authorization
  - Oracle Advanced Security uses OID for central mgmt of user credentials

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Cloud Data Security Technologies

- OAuth
  - Used as a means of providing access to web based resources
  - Not a true authentication protocol
  - Requests are directed to separate identity providers and if an access token is granted then access to the resource is granted
- OpenID
  - Authentication framework for establishing user identity

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Network Security Technologies

- Firewalls and Forward Proxies
  - Restrict points of access to network, network use policy enforcement, client anonymization
  - Problems for mixed cloud- and on-premises deployments
- Cloud Access Security Broker (CASB)
  - To network topology, like a proxy
  - Focused on cloud data
    - Authorization
    - Scan cloud data, enforce policies
    - Risk assessment
    - ML threat detection in some products

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Cloud Security Example

- Amazon AWS IAM
  - Identity and Access Management
  - User and Group Management
  - Authentication:
    - Passwords, key pairs, certificates, multi-factor
    - Integration with AD, Google, Facebook
  - Access Control
    - User and group permissions to control access to AWS resources
    - Granular control (EC2 instances or S3 buckets)

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Big Data Security Technologies

- HDFS File and Directory
- Single Node Security
- Cluster Security
  - Hadoop delegation
  - Apache Knox
  - Apache Ranger
  - Apache Sentry

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Encryption Technologies

- SSL/TLS - OpenSSL
  - Ciphers and Keys
  - Certificates and Trust
- Native
  - Oracle (Oracle Advanced Security)
  - IBM DB2 ("native encryption“, DATA_ENCRYPT)
  - MS SQLServer ("Always Encrypted“, Dynamic Data Masking)
- Password encryption
- Data Scrambling

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

How Progress configures and tests these complex environments

Starts with a Security-Minded Development Culture

- Security Scans – VeraCode
- Static Code Analysis – PREfast
- Fuzz Testing – SQL and Network
- Third-Party Vulnerability Tracking
- Engineering Vigilance

While there's no one tool or process that does everything, taken in combination, these provide a high level of confidence.

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Starts with a Security-Minded Development Culture

- Security Scans – VeraCode
- Static Code Analysis – PREfast
- Fuzz Testing – SQL and Network
- Third-Party Vulnerability Tracking
- Engineering Vigilance

- *All JDBC drivers scanned weekly*
- *We fix all Very High, High, and CWE/SANS Top-25 issues found*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Starts with a Security-Minded Development Culture

- Security Scans – VeraCode
- Static Code Analysis – PREfast
- Fuzz Testing – SQL and Network
- Third-Party Vulnerability Tracking
- Engineering Vigilance

- *Compile-time analysis*
- *Exploitable violations detected:*
  - *Memory management*
  - *Pointer management*
  - *Initialization*
  - *Boundary*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Starts with a Security-Minded Development Culture

- Security Scans – VeraCode
- Static Code Analysis – PREfast
- Fuzz Testing – SQL and Network
- Third-Party Vulnerability Tracking
- Engineering Vigilance

- *Automated software testing technique*
- *Generates semi-valid inputs to expose problematic corner cases*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Starts with a Security-Minded Development Culture

- Security Scans – VeraCode
- Static Code Analysis – PREfast
- Fuzz Testing – SQL and Network
- Third-Party Vulnerability Tracking
- Engineering Vigilance

- *Track open source security, license compliance, and component quality risks*
- *Provide timely updates to avoid known vulnerabilities*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Starts with a Security-Minded Development Culture

- Security Scans – VeraCode
- Static Code Analysis – PREfast
- Fuzz Testing – SQL and Network
- Third-Party Vulnerability Tracking
- Engineering Vigilance

- *Trained developers*
- *Security as a differentiator*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Supported by a History of Testing Breadth

- 25-Years of Test Suite Evolution
- Comprehensive Testing Environment
- Robust Security Verification
- Industry-Specific API Tests

We invest in our testing environment so our partners don't have to, delivering continuous quality through comprehensive testing.

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Supported by a History of Testing Breadth

- 25-Years of Test Suite Evolution
- Comprehensive Testing Environment
- Robust Security Verification
- Industry-Specific API Tests

- *Millions of test cases for every modern connectivity scenario*
- *Strict ODBC, JDBC, ADO.NET and OData compliance*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Supported by a History of Testing Breadth

- 25-Years of Test Suite Evolution
- Comprehensive Testing Environment
- Robust Security Verification
- Industry-Specific API Tests

- *Windows, Linux, AIX, HP and more*
- *Relational, Big Data, Cloud and NoSQL*
- *Tableau, Power BI, Pentaho, Microsoft Office, and SQL Server Linked Server*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Supported by a History of Testing Breadth

- 25-Years of Test Suite Evolution
- Comprehensive Testing Environment
- Robust Security Verification
- Industry-Specific API Tests

- *TLS, Kerberos, Operating System and database-level authentication*
- *SSL and Kerberos configurations across platforms*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Supported by a History of Testing Breadth

- 25-Years of Test Suite Evolution
- Comprehensive Testing Environment
- Robust Security Verification
- Industry-Specific API Tests

- *J2EE CTS*
- *Microsoft LTM*
- *FIPS 140-2*
- *FedRAMP*

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Validated by SOC2 Certification

- Attests to Our Technical and Operational Maturity
  - Internal controls in place (e.g., security, availability, confidentiality) that meet industry best practices
  - Assessed by a recognized independent standards organization

- Provides a Transparent View into Our Organization
  - Important: data access is a critical function; if not done right, problems will find their way into your world
  - Necessary: to meet your vendor due diligence expectations

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Progress®

DataDirect Security Vulnerability Policy

Security Vulnerability Policy

Upon identification of any security vulnerability that would impact one or more Progress product(s), Progress will exercise commercially reasonable efforts to address the vulnerability in accordance with the following guidelines:

Priority *	Time Guideline	Version(s)
High Risk (CVSS 8+ or industry equivalent)	30 days	Active (i.e. latest shipping version) and all Supported versions
Medium Risk (CVSS 5-to-8 or industry equivalent)	180 days	Active (i.e. latest shipping version)
Low Risk (CVSS 0-to-5 or industry equivalent)	Next major release or best effort	Active (i.e. latest shipping version)

* Priority is established based on the current version of the Common Vulnerability Scoring System (CVSS), an open industry standard for assessing the severity of computer system security vulnerabilities. For additional information on this scoring system, refer to https://en.wikipedia.org/wiki/CVSS.

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Resources and Next Steps

- Explore our Security Matrix
- Learn what we do for ISVs, Financial Companies and Big Data Shops
- Talk to a Data Security Expert

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

QnA

© 2018 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Progress®