Strengthening Web Application Security:

IDB Bank's Journey with Qualys WAS

Beatrice Sirchis
Vice President, Application Security
IDBNY

IDBBANK
It's personal

Our Vision

We aspire to be the best bank for our clients by putting their needs first, offering unwavering personal service, trusted relationships and the expertise of our people.

Enabling factor for business success.

Beatrice Sirchis

Vice President, Application Security

Background includes:

- Network Engineer
- Security Engineer
- Security Architect and Project Manager
- CISO of Affiliate Subsidiaries at Discount Bank in Israel

IDB Bank

More than 70 years of personal service and sophisticated financial solutions.

IDB Bank offers personalized and comprehensive solutions for protecting and preserving your wealth.

1935
Company Founded

New York, NY
Headquarters

Rapid Business Growth Through Web App Security

Cybersecurity to position the Bank as a leader in digital innovation

Web Applications & APIs exist in on-prem and multi-cloud environment

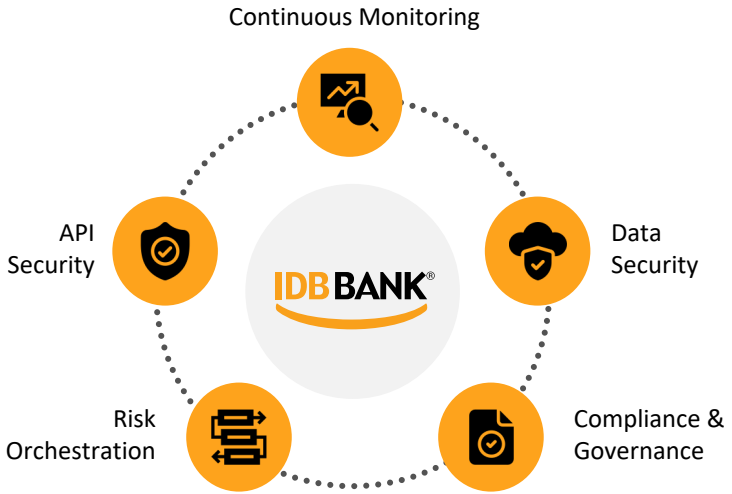
- Internal/external, prod/non-prod, critical/non-critical

Implementation of advanced solutions

- Web Application Scanning
- Secure Code Reviews
- OWASP's Application Security Verification Standard (ASVS)

Data security for sensitive financial data protection as a competitive differentiator.

Compliance with stringent regulations like NYDFS, PCI DSS, to expand into new markets or offer new products with minimal risk.



Critical Requirements

Comprehensive Vulnerability Detection for both internal and external web applications to identify critical and high-risk vulnerabilities

Continuous Scanning to ensure no new vulnerabilities arise due to application changes

Non-Intrusive Production Scans during off-hours to prevent any disruption to production systems

Flexibility with custom dashboards, compliance with OWASP Standards and tagging to classify applications

Central Reporting to consolidate vulnerability data across all web apps for senior management

Shared platform across IT, Security, Internal Audit, and Risk Management Teams.

How We Use Qualys Web Application Scanning (WAS)

Start With Full Visibility Into Web App Inventory

Discover Every Web App Across All Environments

Visibility Of Complete Asset Inventory

- Internal and External Apps
- Cloud and On-prem Apps
- Production and Non-Production Apps

Prioritize with Complete Context

- Improve App Visibility for Web App Security Program
- Prioritize using
  - External vs. internal
  - Critical vs. non-critical applications
- **Monitoring different asset types** (e.g., Internet-facing, internal, non-prod).
- **Align IT & Security Teams, Application Owners**

Internal Apps
Agent, Scanner, Sensors

Cloud Apps
Monitor Apps on Cloud

External Apps
Qualys Internet scanner

APIs
API discovery and testing

Continuous Vulnerability Scanning

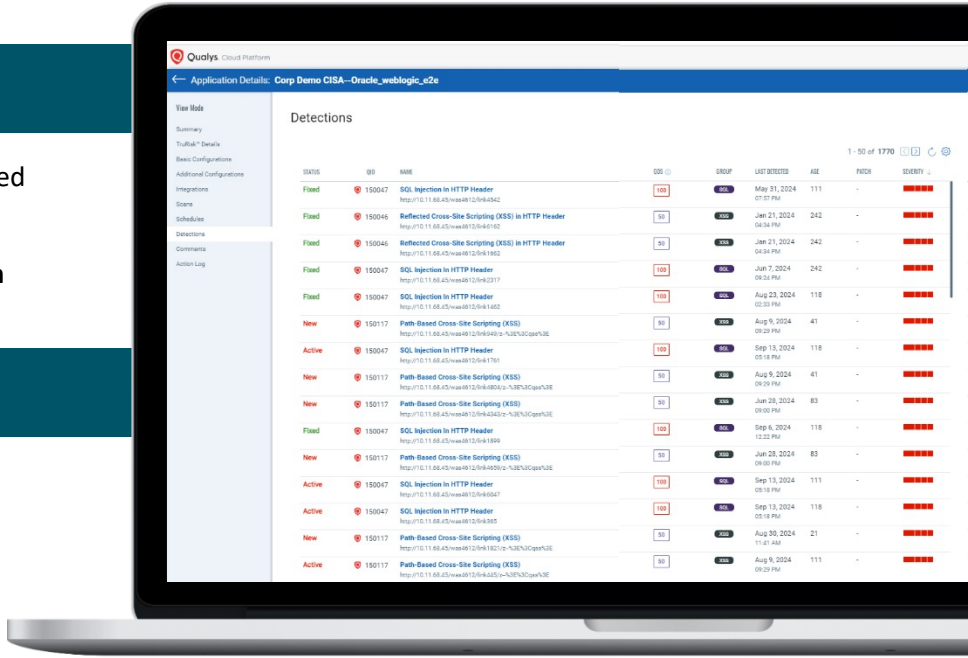
Identify Risks for New and Upgraded Applications

New and upgraded applications onboarding

- New & upgraded applications, both **internal** & **external**, are scanned to remediate **high** and **critical** vulnerabilities **prior to go-live**
- Import **Burp XML files** into Qualys WAS for a **single source of truth**

App changes can bring new vulnerabilities

- **Continuous periodic scanning** of applications to address **critical** and **high-risk vulnerabilities**
- Ensures that any changes made to applications are **detected** and **analysed**

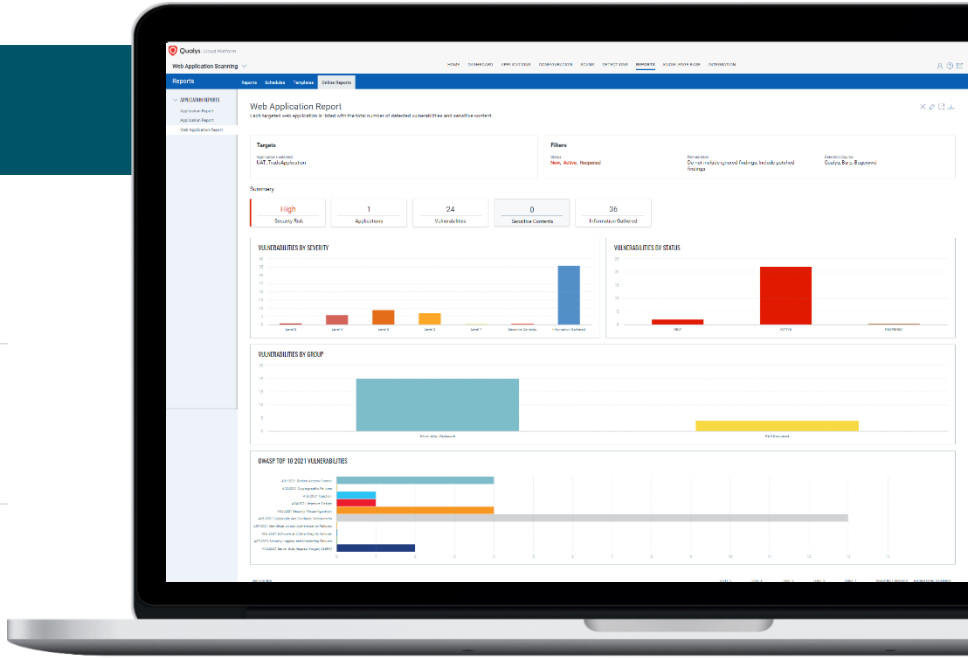


Non-Production Scanning

To Fix Vulnerabilities Before Production Deployment

Web application security extends beyond production environments

- Periodic scanning of non-prod applications **before moving to production**
- **Increased vulnerabilities** in non-prod trigger engagement with IT owners
- IT stakeholders receive **regular scan reports via email** without direct access to Qualys



IDB BANK
It's personal

Scanning Profiles & Schedules

For Comprehensive Application Scans

Leveraging scanning profiles tailored to the needs of each application environment

Key scan profiles include

- OS Scanning
- Spring4Shell Vulnerability Scanning
- Log4Shell Vulnerability Scanning

Non-Production Specific Testing

- **Denial of Service (DoS) tests** only executed in non-production environments to avoid production risk
- Can be conducted at any time, including during working hours

Production Scans

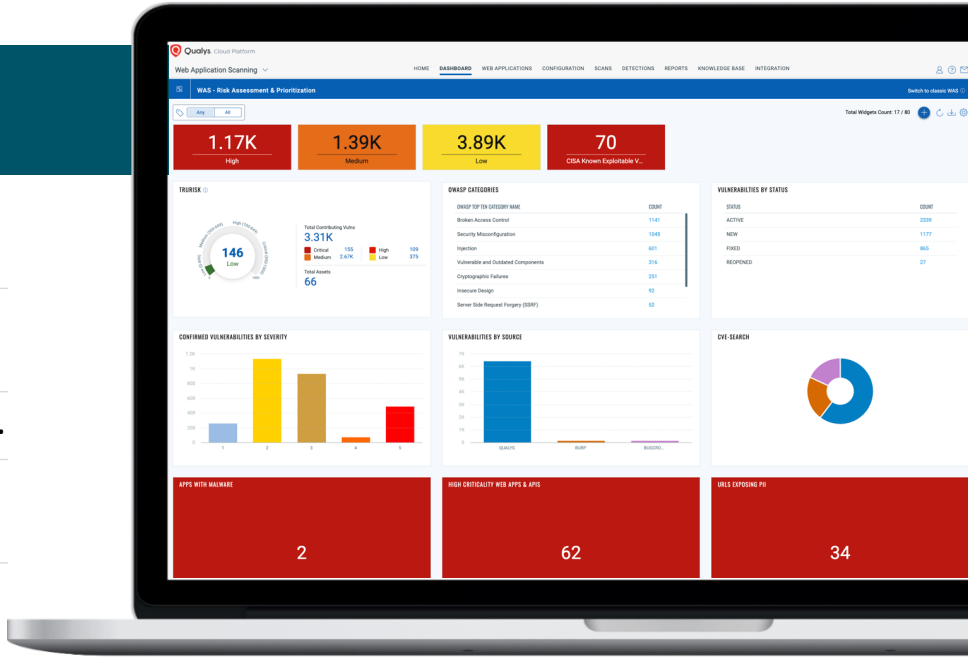
- Run outside of working hours to avoid any potential operational impact

Dashboards, Reports & KPI Tracking

For Stakeholder & Executive Communication

Defined dashboards & reports for both security teams, IT/application owners & executives.

- **Target: 0** - Tracking **critical/high-risk vulnerabilities on external web applications**
- **Target: 0 before production** - Monitoring **critical/high-risk vulnerabilities** on **internal applications**
- **Third-Party critical component monitoring** like **Java, Apache, .NET.**
- Utilizing **OWASP dashboards** for compliance and security framework adherence
- Simplified reporting to **senior management** across all bank web applications



Prioritize Risks For Remediation

With Enhanced Visibility and Risk-Based Prioritization

Clear visibility into security posture based on where the application resides

Tagging applications by:

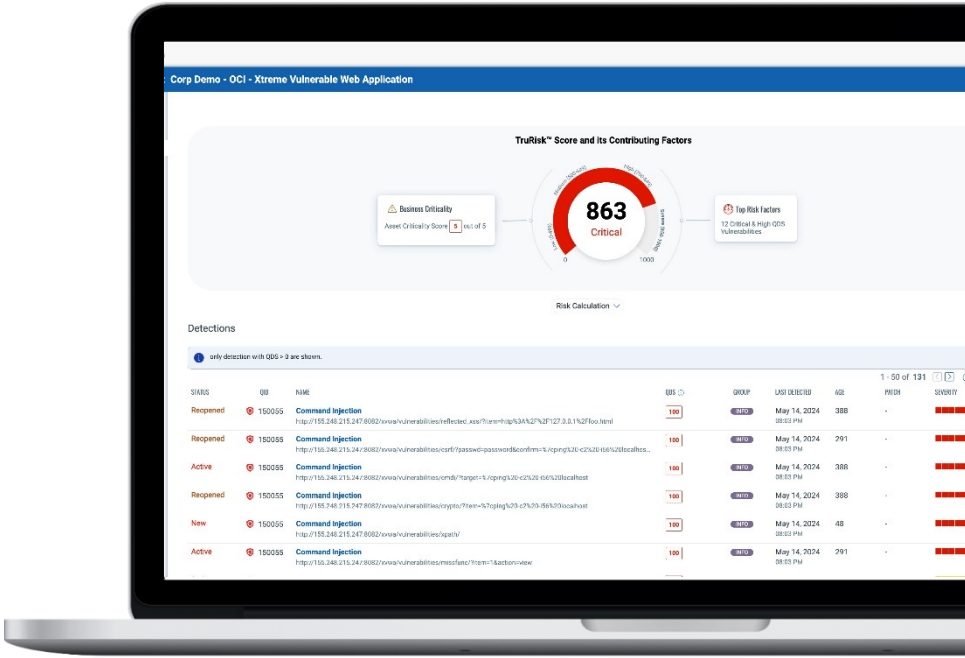
- **Environment** Production vs. Non-production
- **Exposure:** Internet-facing vs. Internal applications
- **Criticality:** Critical vs. Non-critical applications

Risk-Based Prioritization with TruRisk™

- Leveraging **Qualys TruRisk™ score** to prioritize vulnerabilities based on **actual risk**

Streamlined Remediation Process

- Vulnerabilities **are assigned to application owners**, with remediation progress monitored and reported to stakeholders



Future Roadmap to Promote Innovation

Qualys WAS as Single Source of Truth for Web Apps & APIs

Software Composition Analysis

Using SCA testing to identify more software components (**Java, .NET, Node.js**).

Automated remediation workflow

Automate export of vulnerabilities to **ServiceNow** for auto-assigning & remediation

API Scanning

Scan APIs, especially **MuleSoft APIs,** particularly with MuleSoft compliance support

Strategic Business Enabler To Drive Growth

by Aligning IT and Security Teams

100% Reduction in Critical and High-Risk Vulnerabilities in Production

Continuous scanning and remediation before applications go live, maintaining zero critical vulnerabilities in production

80% Increase in Vulnerability Detections Across All Environments

Increase in the identification of vulnerabilities across multi-cloud, on-premise, containers, APIs and more

80% Time Saved in Stakeholder & Executive-level Reporting

Less time spent on manual reporting, compliance and remediation tracking for stakeholders & executive teams.

Thank you