Maximize Qualys’ Value

Scott Frederick

Director, Enterprise Security, Vulnerability Management

Ameritas
fulfilling life

Scott Frederick

Director of Vulnerability Management, Ameritas

14 years with the company

Roles included:
Infrastructure and Security Architect, Technical Systems Architect, Enterprise Security Director

CISSP Certified

Ameritas
fulfilling life.

Ameritas®

Ameritas Mutual Holding Company and its affiliated subsidiary companies include Ameritas Life Insurance Corp. and Ameritas Life Insurance Corp. of New York.

Founded in 1887, Ameritas offers a wide range of insurance and financial products and services to individuals, families and businesses.

These products and services include life insurance; annuities; individual disability income insurance; group dental, vision and hearing care insurance; retirement plans; investments; asset management; and public finance.

Company Founded:

1887

Headquarters:

Lincoln, NE

Industry:

Insurance and Financial Services

Note:
This presentation is considered TLP (Traffic Light Protocol): White; Information can be shared freely, as it is not considered sensitive.

Ameritas' 2024 Corporate Theme...

- We grow by delivering more **value** to more customers
- We deliver more value by prioritizing the work that makes the most **impact**
- We are motivated by our **purpose**, which is fulfilling life

... as implemented by the VM Team

Value

- Produce meaningful deliverables
- Maximize existing licensed software

Impact

- Risk-based prioritization
- Measure effectiveness

Purpose

- Well-defined deliverables and expectations
- Review frequently and adjust

Solving Problems with Qualys' Capabilities

How can we maximize the value of our existing Qualys modules?

Simplify Risk Prioritization and Reporting

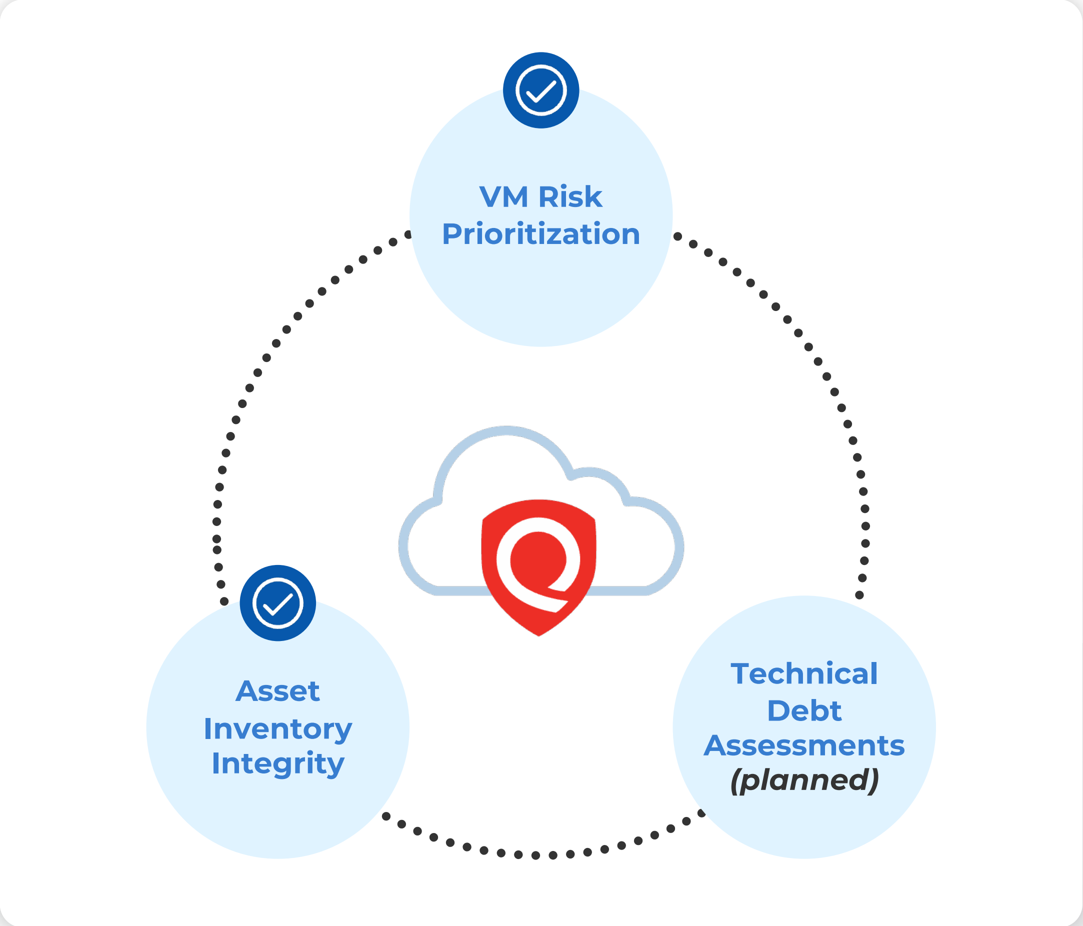
Maximize use of Qualys Detection Score and Qualys' Threat Research Unit

Improve Asset Inventory Integrity

Maximize capabilities of Qualys' CyberSecurity Asset Management (CSAM), TotalCloud, and Container Security Modules

Support Technical Debt Assessments

Planned - Integrate Asset Criticality Score (ACS) and TruRisk Score into the Technical Debt assessments

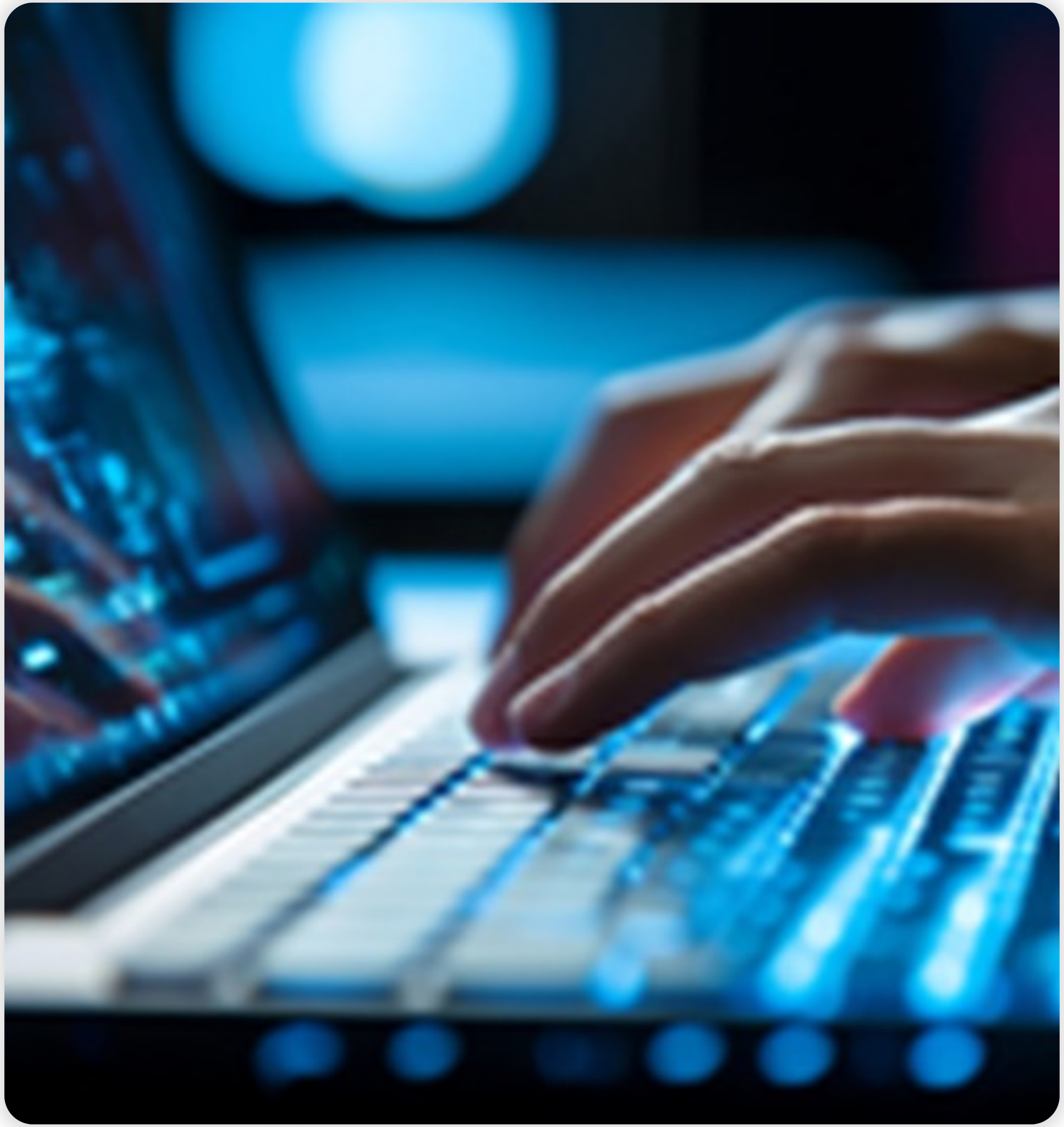


VM Risk Prioritization
Asset Inventory Integrity
Technical Debt Assessments *(planned)*

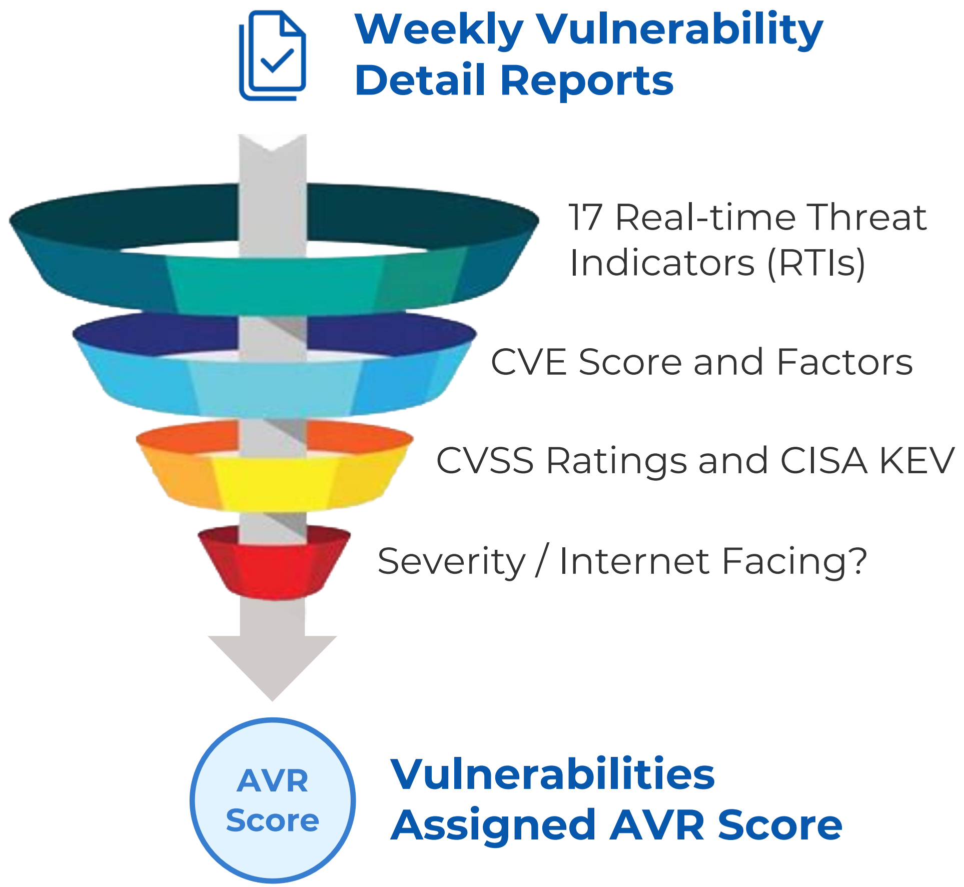
Simplified Risk Prioritization

Maturing our risk prioritization approach by leveraging the Qualys Detection Score (QDS)...

Ameritas®
fulfilling life®



Simplified Risk Prioritization - Legacy Approach



Weekly Vulnerability Detail Reports

17 Real-time Threat Indicators (RTIs)

CVE Score and Factors

CVSS Ratings and CISA KEV

Severity / Internet Facing?

Vulnerabilities Assigned AVR Score

Home-grown Calculation

- Required 30+ files downloaded
- Full refresh weekly to stay current
- Developed prior to release of TruRisk's QDS

Ameritas Vulnerability Risk (AVR)

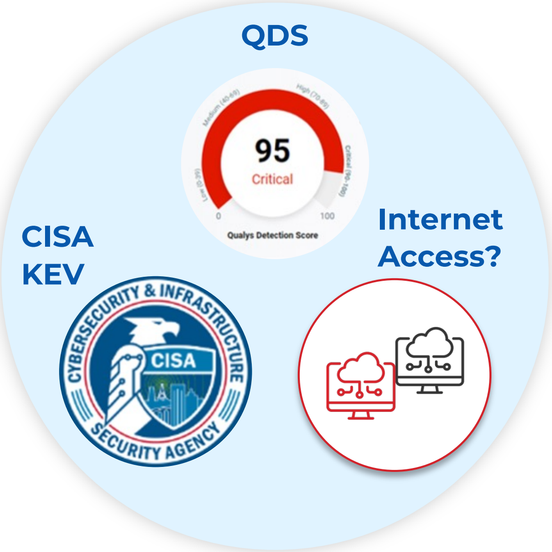
- Qualys RTIs were central to prioritization
- Vulnerabilities assigned an AVR Score
- AVR Score drove Risk Priority Band assignment

Numerous Downsides

- Significant commitment of time to maintain
- Required extensive regression testing
- Changes required broad communications
- Risk Band assignment not representable in native Qualys dashboards

Simplified Risk Prioritization – QDS-based

Simplified Prioritization Approach



- What is the Qualys Detection Score (QDS) for this Vulnerability?
- Are any associated CVEs listed on CISA's Known Exploited List?
- Do the impacted assets have access to the Internet?

Simplified QDS-based Calculation

- QDS replaced complex in-house calculation
- Risk Priority Bands are easily represented in Qualys Dashboards and Reports
- Countless hours saved over legacy approach

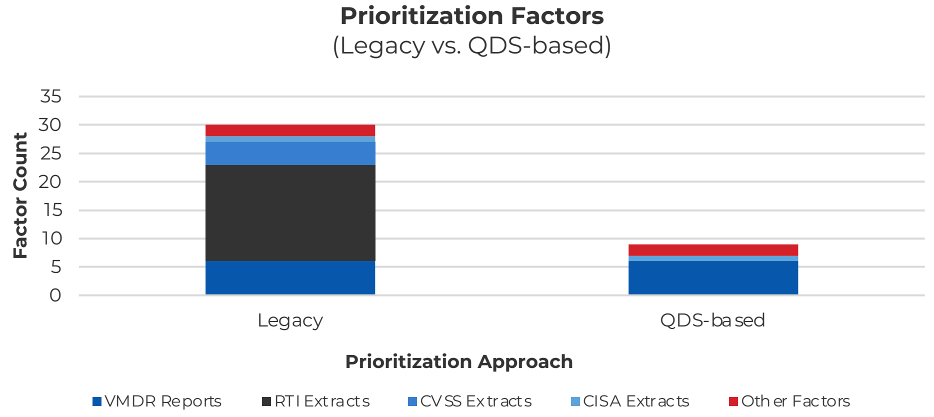
Supported by External Expertise

- Qualys' Threat Research Unit (TRU) is our trusted source for threat analysis
- Eliminates the need to justify threat and remediation priorities

Enterprise-wide Adoption

- Vulnerabilities grouped into Risk Priority Bands
- Integrated into Risk Management's controls and practices
- Fully embraced by Enterprise; included in Board of Director reports

Simplified Risk Prioritization and Reporting – Benefits (1 of 3)



Risk Priority Band	Internet Facing	CISA Known Exploited CVE	Qualys Detection Score (QDS) Inclusive	Recommended Remediation Timeline	Comments
0	Yes	Yes	0 - 100	15 days	Internet Facing: Yes CISA KEV: Yes QDS: Any
1	Yes	No	70 - 100	30 days	Internet Facing: Yes CISA KEV: Yes QDS: High and Critical
2	No	Yes	70 - 100	30 days	Internet Facing: No CISA KEV: Yes QDS: High and Critical
3	Yes	No	40-69	45 days	Internet Facing: Yes CISA KEV: No QDS: Medium
4	No	No	40-69	75 days	Internet Facing: No CISA KEV: No QDS: Medium
5	Any	No	0-39	As Possible	Internet Facing: Any CISA KEV: No QDS: Low

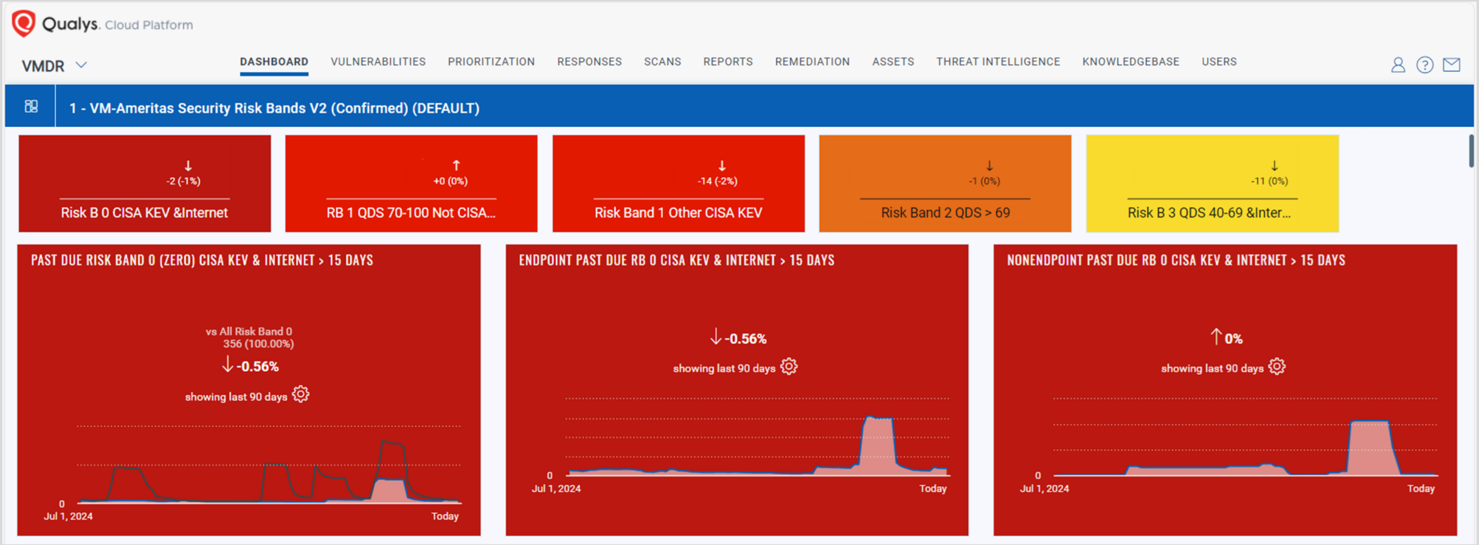
Fewer Factors/Less Complexity/Improved Accuracy

- Data files reduced by 67%; saving 2 hours weekly
- Reduced calculation errors and rework
- Elimination of custom calculation maintenance; saving countless hours

Leverages Trusted External Experts

- Foundational to Ameritas’ Risk Management controls
- External expertise reduces biases and internal challenges
- IT meetings reduced from 4 hours to .75 hours monthly

Simplified Risk Prioritization and Reporting – Benefits (2 of 3)



1 - VM-Ameritas Security Risk Bands V2 (Confirmed) (DEFAULT)

↓ -2 (-1%)	↑ +0 (0%)	↓ -14 (-2%)	↓ -1 (0%)	↓ -11 (0%)
Risk B 0 CISA KEV &Internet	RB 1 QDS 70-100 Not CISA...	Risk Band 1 Other CISA KEV	Risk Band 2 QDS > 69	Risk B 3 QDS 40-69 &Inter...

PAST DUE RISK BAND 0 (ZERO) CISA KEV & INTERNET > 15 DAYS

vs All Risk Band 0
356 (100.00%)
↓ -0.56%
showing last 90 days

ENDPOINT PAST DUE RB 0 CISA KEV & INTERNET > 15 DAYS

↓ -0.56%
showing last 90 days

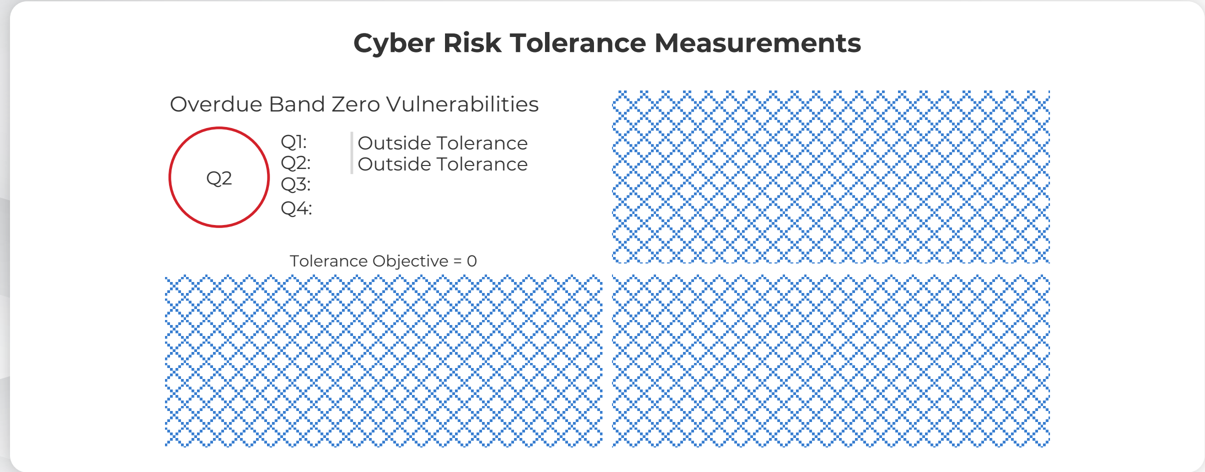
NONENDPOINT PAST DUE RB 0 CISA KEV & INTERNET > 15 DAYS

↑ 0%
showing last 90 days

Represented with Dashboards

- All prioritization factors within Qualys Platform
- Widgets allow segregation based on Risk Priority Band and Age
- Near real-time reporting on risk bands

Simplified Risk Prioritization and Reporting – Benefits (3 of 3)



Cyber Risk Tolerance Measurements

Overdue Band Zero Vulnerabilities

Q2

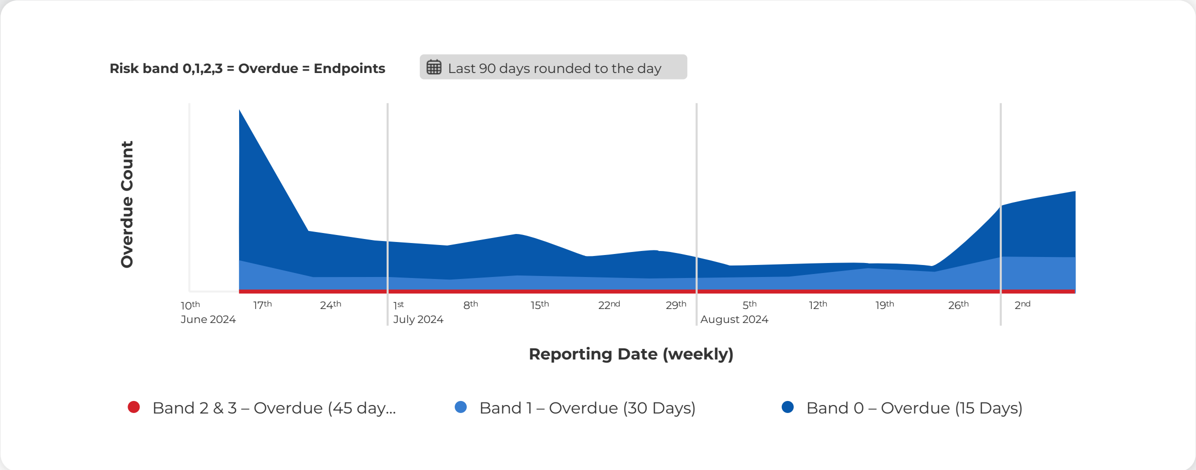
Q1:	Outside Tolerance
Q2:	Outside Tolerance
Q3:	
Q4:	

[redacted]

Tolerance Objective = 0

[redacted]

[redacted]



Concise Board-level Risk Reporting

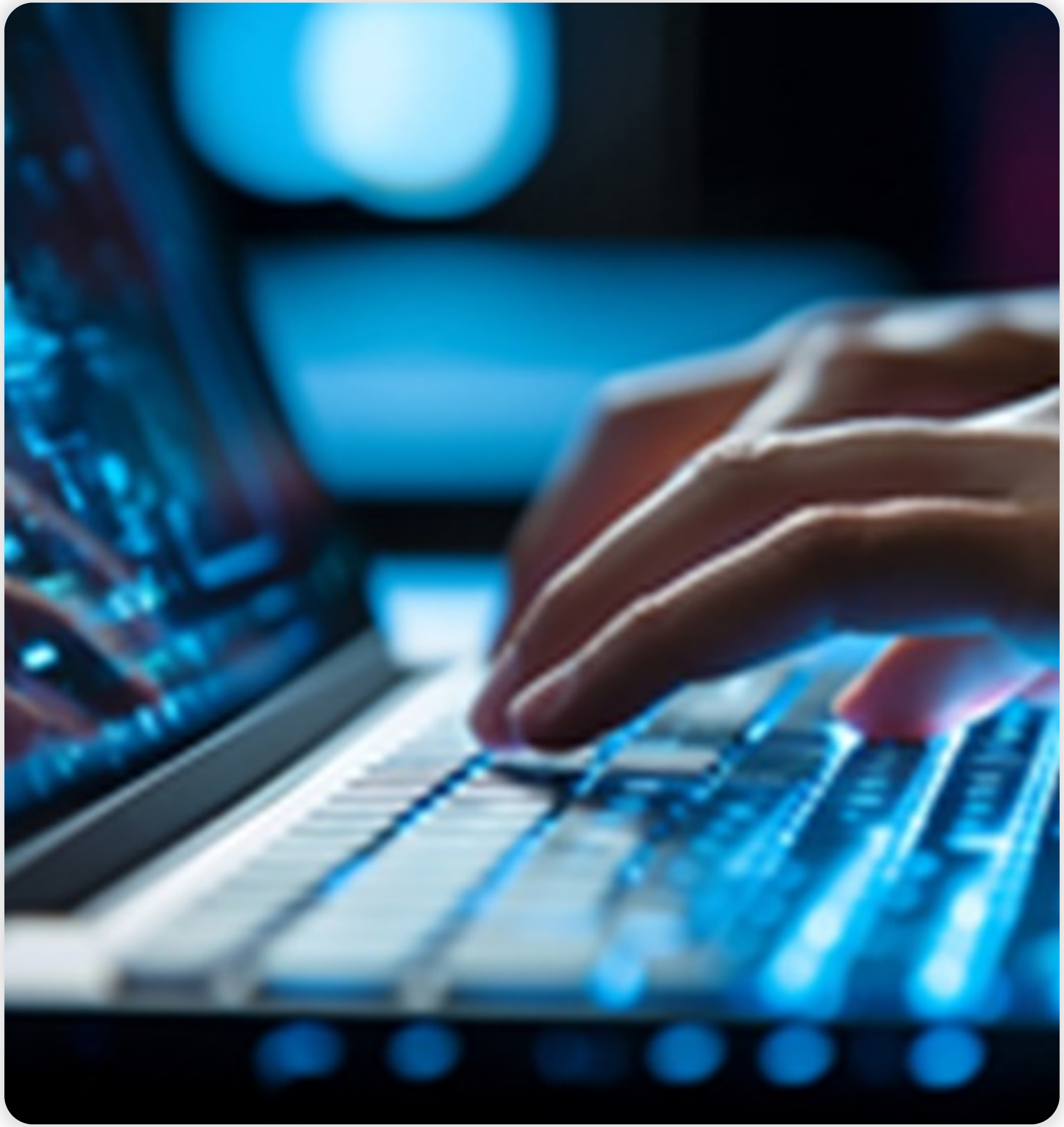
- CISO reports on four key risk indicators (KRIs) for Ameritas, tracking risk reduction over time
- Overdue Risk Band 0 instance count, powered by QDS, is one of these four KRIs
- Report preparation time reduced from hours to minutes

Simplifies Operational Risk Reporting

- Consistently tracking risk over time
- Focus remediation efforts on the highest threats

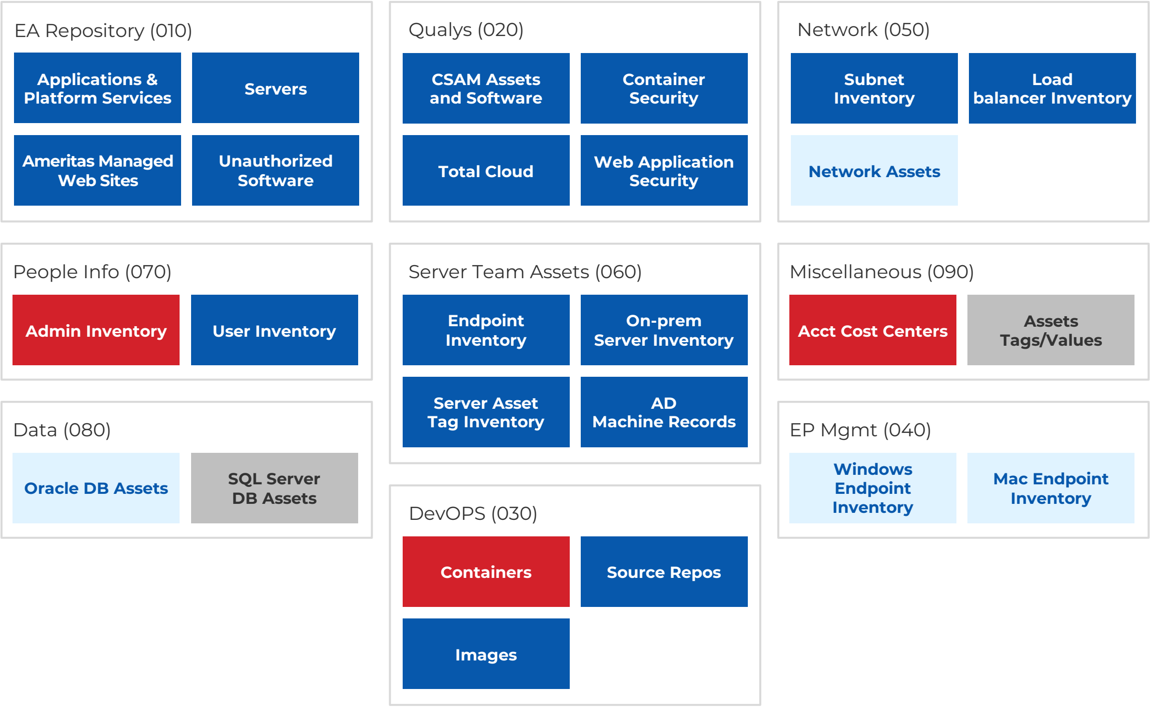
Improved Asset Inventory

Leveraging Qualys' discovery capabilities to serve as our "source of truth" for asset inventory...



Ameritas®
fulfilling life®

Asset Inventory – Legacy Silos



EA Repository (010)
- Applications & Platform Services
- Servers
- Ameritas Managed Web Sites
- Unauthorized Software

Qualys (020)
- CSAM Assets and Software
- Container Security
- Total Cloud
- Web Application Security

Network (050)
- Subnet Inventory
- Load balancer Inventory
- Network Assets

People Info (070)
- Admin Inventory
- User Inventory

Server Team Assets (060)
- Endpoint Inventory
- On-prem Server Inventory
- Server Asset Tag Inventory
- AD Machine Records

Miscellaneous (090)
- Acct Cost Centers
- Assets Tags/Values

Data (080)
- Oracle DB Assets
- SQL Server DB Assets

DevOPS (030)
- Containers
- Source Repos
- Images

EP Mgmt (040)
- Windows Endpoint Inventory
- Mac Endpoint Inventory

- No authoritative source for asset inventory
- Too many existing agents and sensors
- No comprehensive CMDB

Departmental inventory silos

- Each department and team has own inventories
- Different formats and storage platforms
- None met standards to be “source of truth”

No centralized inventory view

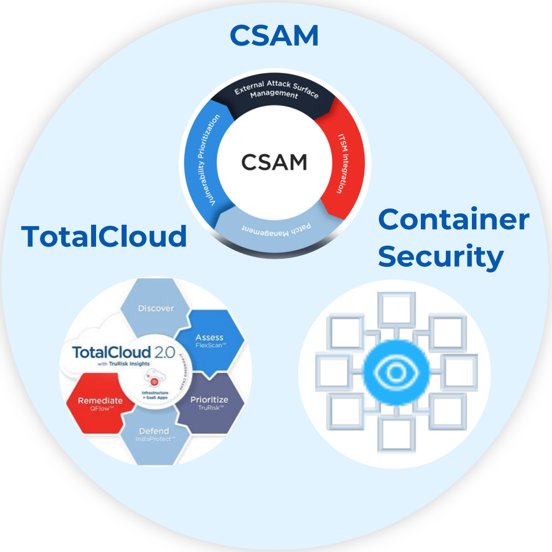
- No common data dictionary or definitions
- No true CMDB or dependency information
- No reconciliation processes between disparate repositories

Packaged solutions were considered

- Required yet additional scanning agent
- Required significant levels of customizations
- Required additional operational personnel

Improved Asset Inventory Integrity

Inventory Source of Truth



- Accurate asset inventories are crucial for vulnerability management
- Comprehensive visibility helps prevent security gaps and reduces risk

Create "source of truth" inventory

- Qualys discovery data most complete source for "active" assets
- Core Qualys data ingested central database
- Asset context added from other sources
- No additional discovery agents required

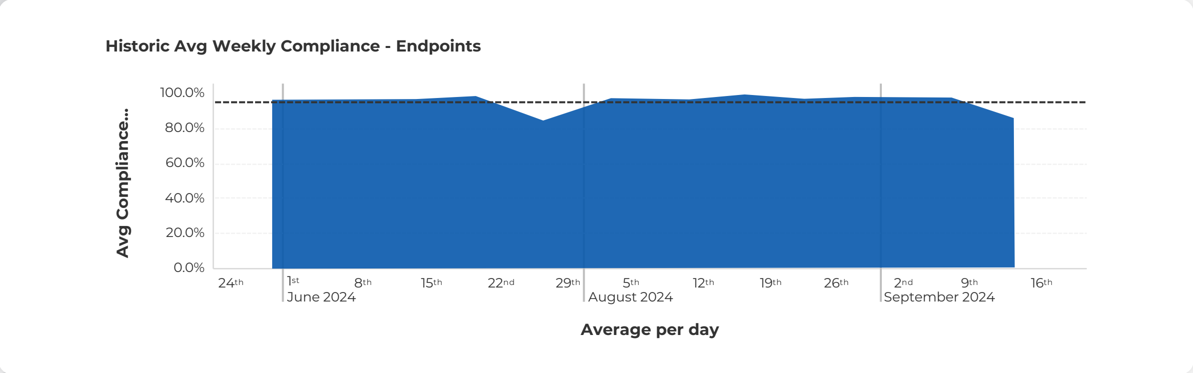
Measuring inventory integrity

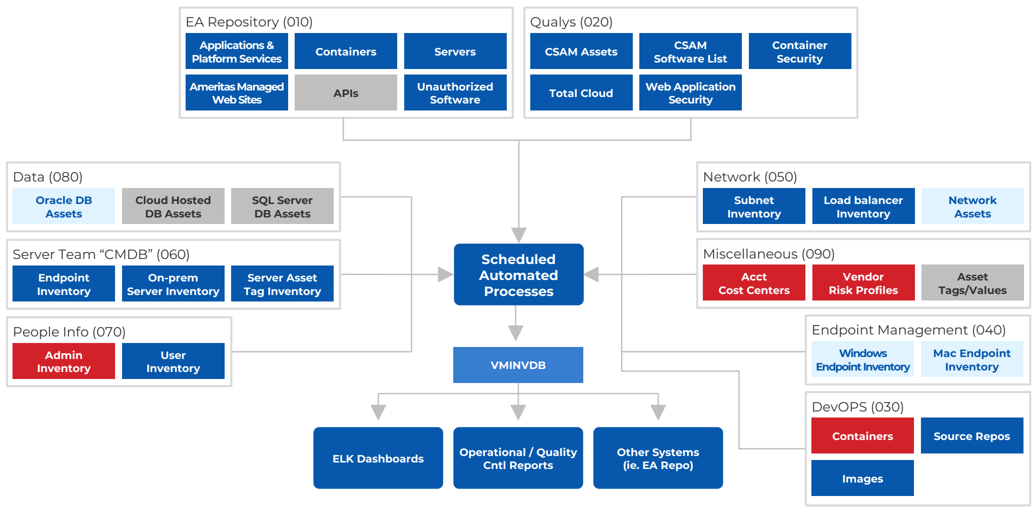
- Qualys-sourced inventory used to validate other systems
- Key required attributes are inspected
- Report on inventory integrity deficiencies

"Downstream" integrations

- Inventory database sourced to maintain Enterprise Architecture's Repository
- Planned integration with ITSM Service Management Platform
- Supports centralized topical Elastic dashboards

Improved Asset Inventory Integrity – Benefits (1 of 2)





EA Repository (010)
- Applications & Platform Services
- Containers
- Servers
- Ameritas Managed Web Sites
- APIs
- Unauthorized Software

Qualys (020)
- CSAM Assets
- CSAM Software List
- Container Security
- Total Cloud
- Web Application Security

Data (080)
- Oracle DB Assets
- Cloud Hosted DB Assets
- SQL Server DB Assets

Server Team "CMDB" (060)
- Endpoint Inventory
- On-prem Server Inventory
- Server Asset Tag Inventory

People Info (070)
- Admin Inventory
- User Inventory

Network (050)
- Subnet Inventory
- Load balancer Inventory
- Network Assets

Miscellaneous (090)
- Acct Cost Centers
- Vendor Risk Profiles
- Asset Tags/Values

Endpoint Management (040)
- Windows Endpoint Inventory
- Mac Endpoint Inventory

DevOPS (030)
- Containers
- Source Repos
- Images

Scheduled Automated Processes

VMINVDB

- ELK Dashboards
- Operational / Quality Cntl Reports
- Other Systems (ie. EA Repo)

Historic Reporting of Key Asset Integrity

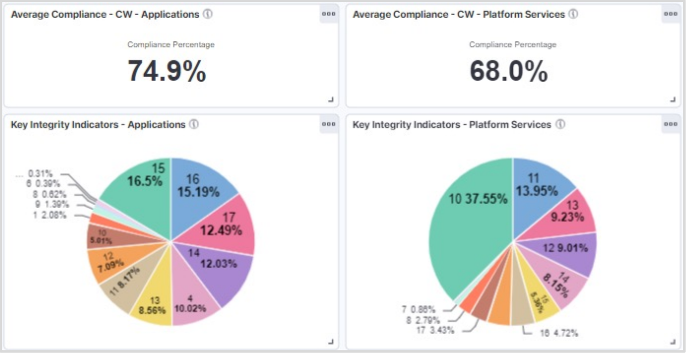
- Evaluate integrity compliance against 99% Key Performance Indicator (KPI) target
- Focused remediation based on trend analysis

Comprehensive Inventory

- Consolidated information from 30+ sources
- Delivers broad contextual relationships

Ameritas
fulfilling life.

Improved Asset Inventory Integrity – Benefits (2 of 2)



Average Compliance - CW - Applications

Compliance Percentage

74.9%

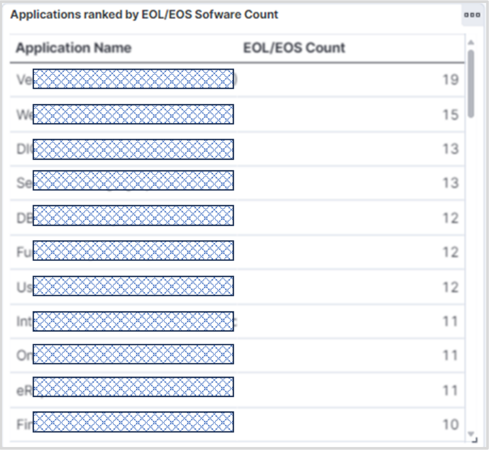
Average Compliance - CW - Platform Services

Compliance Percentage

68.0%

Key Integrity Indicators - Applications

Key Integrity Indicators - Platform Services



Applications ranked by EOL/EOS Sofware Count

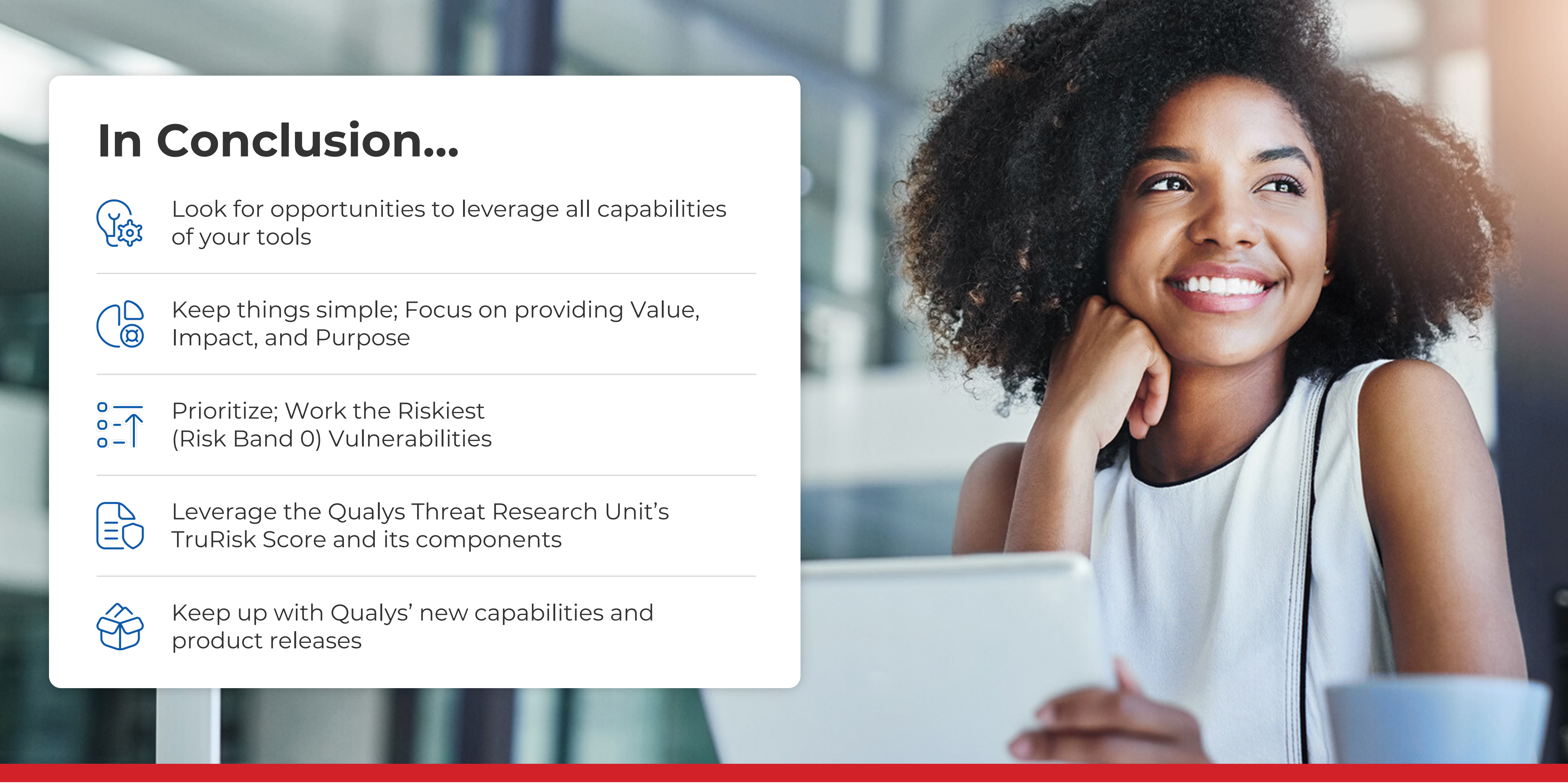
Application Name	EOL/EOS Count
[redacted]	19
[redacted]	15
[redacted]	13
[redacted]	13
[redacted]	12
[redacted]	12
[redacted]	12
[redacted]	11
[redacted]	11
[redacted]	11
[redacted]	10

Continual Inspection of Portfolio Integrity

- Granular reporting on asset property integrity
- Each Asset Type has a distinct set of mandatory properties

Business Applications use of EOL/EOS Software

- EOL/EOS counts summarized by Business Application
- Enables Tech Governance and Business Area Discussions



In Conclusion...

- Look for opportunities to leverage all capabilities of your tools
- Keep things simple; Focus on providing Value, Impact, and Purpose
- Prioritize; Work the Riskiest (Risk Band 0) Vulnerabilities
- Leverage the Qualys Threat Research Unit's TruRisk Score and its components
- Keep up with Qualys' new capabilities and product releases