Warranty
This document is supplied on an "as is" basis with no warranty and no support.

Limitations of Liability
In no event shall BeyondTrust be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

Disclaimer
All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. BeyondTrust is not associated with any other vendors or products mentioned in this document.
Table of Contents

Executive Summary ............................................................................................................................................... 4
Differentiator #1: Visibility and Reporting to Prioritize Remediation .......................................................... 5
Differentiator #2: Increased Vulnerability Management Efficiency ............................................................... 6
Differentiator #3: Enterprise Scalability ......................................................................................................... 7
Differentiator #4: Zero-Gap Coverage .......................................................................................................... 8
Analysts and Experts Agree ............................................................................................................................ 9
Critical Vulnerability Management Capabilities .......................................................................................... 10
BeyondTrust Vulnerability Management Solutions ....................................................................................... 11
  Enterprise vulnerability management .............................................................................................................. 11
  Network security scanning .............................................................................................................................. 11
  Cloud-based vulnerability assessment ............................................................................................................ 11
  Web application vulnerability assessment ..................................................................................................... 11
  Centralized management, policy, reporting and analytics ............................................................................ 11
Conclusion ................................................................................................................................................... 12
About BeyondTrust ...................................................................................................................................... 13
Executive Summary

Despite widespread deployment of vulnerability management technologies, many security professionals still struggle to decide how best to protect their organizations, achieve compliance, and communicate risk enterprise-wide.

The fact is, most vulnerability management solutions do little to help security leaders put vulnerability and risk information in the context of business. Saddled with volumes of rigid data and static reports, the security team is left to manually discern real threats and determine how to act upon them. How can security teams deliver security risk information in context in order to take appropriate action?

In this white paper, BeyondTrust seeks to demonstrate just that – how we have helped our customers overcome these challenges with the Retina difference – four key differentiators that separate BeyondTrust from other solution providers in the market using data and real feedback from our 2015 customer survey conducted by TechValidate.
Differentiator #1: Visibility and Reporting to Prioritize Remediation

Security administrators today are inundated with data – recommended patches, vulnerabilities, risk scores, and more – with very little tangible guidance on what to do with that data. Often lacking is actionable information – beyond just the data – to help prioritize what to focus on first. This lack of context puts security administrators in a difficult position. How do you ensure you’ve protected your enterprise without spending hours poring over vulnerability reports? Prioritization is the key to helping IT teams deliver protection that scales.

In a survey of more than 90 customers, those customers indicated that the visibility and reporting that Retina provided helped to prioritize remediation.

This differentiator was important to Genscape, Inc., the leading global provider of real-time data and intelligence for commodity and energy markets. Genscape was looking to:

- Gain visibility into exposures across multiple layers of infrastructure
- Profile previously unknown assets on the network
- Understand the operational implications of vulnerabilities
- Report risk to IT administrators, management and/or auditors
- Identify and prioritizing remediation tactics
- Patch / update assets with greater efficiency

After looking at competitive solutions, including Rapid7 and Tenable, they turned to BeyondTrust. In the words of Mike Sartuche, Director of Security and Network Infrastructure, “BeyondTrust has allowed us to identify assets that are vulnerable to the latest threats as soon as they hit like POODLE, Heartbleed, and others. It allows us to prioritize the remediation process and the reporting is top notch.”

Retina CS delivers deep analytics and reporting to multiple stakeholders, ensuring that all teams have the information and views they need to effectively manage application and asset risk. A dashboard interface simplifies reporting, helping teams indicate the type of information needed.

Need more evidence? Check out the Retina CS report summary.
Differentiator #2: Increased Vulnerability Management Efficiency

In vulnerability management, efficiency is measured by rates of detection, rates of false positives, and rates of remediation. IT teams gauge a vulnerability management solution’s efficiency by whether it helps them quickly find and remediate the most critical instances.

In a survey of more than 80 customers, those customers indicated that the vulnerability management efficiency increases gained by using BeyondTrust Retina were a competitive differentiator. This differentiator was important to BMC, the global software solutions company, who was looking to:

- Reduce the risk of security breaches
- Shrink the attack surface
- Reduce security data overload
- Meet compliance regulations
- Tighten operational practices
- Integrate with other solutions

BMC chose BeyondTrust Retina CS over McAfee, Qualys and Tripwire (Belden). In the words of Saurabh Verma, Security Officer, “BeyondTrust Retina has made our security lives pretty comfortable as it’s a one stop solution for us as we scan, detect, and patch vulnerabilities effortlessly. Kudos to BeyondTrust Retina.”

Retina CS addresses every phase of the vulnerability management lifecycle – from assessment to remediation – eliminating the need for multiple, sometimes overlapping, solutions to address vulnerability management risks. All BeyondTrust vulnerability management solutions are included in the BeyondInsight IT Risk Management platform for unified reporting, analytics, policy and management across the environment. This approach delivers efficiency and cost savings.

Need more evidence? Check out the sample vulnerability management policy to help guide the maturity of your vulnerability management program.
Differentiator #3: Enterprise Scalability

IT organizations must conduct scans across dispersed, heterogeneous environments with maximum performance and minimum service interruption. To achieve that objective, their vulnerability management solutions must be architected for anything from simple deployment to management of networks with multiple firewalls, IDS/IPS, VLANS and disparate locations. BeyondTrust Retina CS delivers on this customer requirement.

In a survey of more than 100 customers, those customers indicated that BeyondTrust’s enterprise scalability was a competitive differentiator versus other options in the vulnerability management market. As evidence, take a look at the quote from a system administrator from a Large Enterprise Security Products and Services Company below.

This differentiator was also important to Standard Bank of South Africa, one of South Africa’s largest financial institutions, who was looking to:

- Gain visibility into exposures across multiple layers of infrastructure
- Profile previously unknown assets on the network
- Report risk to IT administrators, management and auditors
- Identify and prioritize remediation tactics

After evaluating McAfee, Qualys and Tenable, they chose BeyondTrust Retina CS. In the words of Andrew De Lange, Engineer, “The drive for more efficient patch management has increased tenfold since our implementation. We are the trusted source the company looks to for all kinds of data collected in our scans, not just vulnerabilities.”

The Retina CS console provides a centralized management, reporting and analytics solution across the enterprise’s assets and endpoints. Retina CS includes Smart Rules to logically group, alert, report, assess, and govern under role based application control (RBAC). Additionally, Retina CS can create a compliance scorecard, present risk ratings, and create reports on benchmarks and deviations. Targeted reports are available for audiences ranging from security and IT administrators to executives and compliance auditors.

You just can’t match this level of enterprise scalability anywhere in the industry. To learn more, check out the Retina CS product review conducted by Frost & Sullivan.
Differentiator #4: Zero-Gap Coverage

IT organizations understand that one of the simplest ways to maintain a strong security posture is to ensure coverage of the IT infrastructure – no virtual machine, database, server or application can exist on the network without vulnerability management coverage – no gaps allowed. However, without the right solution, it’s becoming increasingly difficult for IT organizations to put a zero-gap policy into practice. As enterprises grow, so does its IT infrastructure complexity. It only takes the exploitation of one asset’s vulnerability to compromise a network.

In a survey of more than 80 customers, the overwhelming majority of those customers indicated that BeyondTrust Retina CS reduced their security exposure by up to 25%. Customers indicated that Retina’s zero-gap platform coverage was a competitive differentiator versus other options in the vulnerability management market.

This differentiator was important to VCU Health System, a leading research hospital and medical center in Virginia, who was looking to:

- Scan remote assets or other offline/air-gapped systems
- Profile previously unknown assets on the network
- Understand the operational implications of vulnerabilities
- Report risk to IT administrators, management and auditors
- Identify and prioritize remediation tactics
- Patch/Update assets with greater efficiency

After evaluating McAfee and Rapid7, VCU Health chose Retina CS. In the words of Peter Ring, systems administrator, "Retina has given us a security view we had never had. We use it extensively on all of our servers, both in the DMZ and internal. We also use it on any external servers we are responsible for."

Retina CS provides zero-gap coverage, discovering and assessing any IT resource in the organization including network, web, mobile, cloud and virtual infrastructures. Having this zero-gap coverage reduces risk by ensuring that no assets are left unprotected.

Need more evidence? Check out the Retina CS’s platform coverage, including network vulnerability assessments, cloud vulnerability assessments, virtual environment scanning, web application vulnerability assessments, and mobile device scanning.
Analysts and Experts Agree

BeyondTrust’s approach to solving vulnerability management challenges has been validated by the industry as well as by our customers. Read what some of the most influential industry experts have to say:

1Gartner, Vulnerability and Security Configuration Assessment Solutions Comparison, Anton Chuvakin, 4.1.2014.
Critical Vulnerability Management Capabilities

Our 15+ years of experience in exceeding the vulnerability management needs of our customers tell us that there are critical capabilities that any solution in the market must include. Among them are those found in the table below. As you consider your vulnerability management tools, use this checklist to compare BeyondTrust to other solution providers.

<table>
<thead>
<tr>
<th>Critical Capabilities</th>
<th>BeyondTrust</th>
<th>Vendor B</th>
<th>Vendor C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover and assess <em>any</em> IT resource in the organization</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agentless and agent-based scanning whether assets are connected to the network or not</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting for COBIT, GLBA, HIPAA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST, PCI, SOX, and more</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share data with SIEM, GRC and other solutions</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import scan data from competitive solutions</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designed for simple deployment and management of networks with multiple firewalls, IDS/IPS, VLANS and disparate locations</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seamless patching for Microsoft and third-party applications</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Retina Enterprise Vulnerability Management

Vulnerability Management Lifecycle

Retina Capabilities

- Complete Risk Visibility
- Full Risk Context
- Comprehensive Threat Intelligence
- Flexible Deployment
- Ease of Integration
BeyondTrust Vulnerability Management Solutions

Enterprise vulnerability management

BeyondTrust Retina CS is the only vulnerability management software solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Retina’s results-oriented architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across disparate and heterogeneous infrastructure.

Network security scanning

BeyondTrust Retina Network Security Scanner is the most sophisticated vulnerability assessment solution on the market. Available as a standalone application or as part of Retina CS Enterprise Vulnerability Management, Retina Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.

Cloud-based vulnerability assessment

BeyondTrust BeyondSaaS is a cloud-based, external vulnerability assessment solution that gives you an attacker’s-eye view of your IT perimeter. The solution conducts fast, affordable security assessments of your public-facing network infrastructure and web applications, while delivering straightforward and accurate reports. As a result, you’re able to quickly identify perimeter vulnerabilities, clearly understand their potential impact, and decisively act to mitigate threats.

Web application vulnerability assessment

BeyondTrust Retina Web Security Scanner is a dynamic application security testing (DAST) solution designed for modern mobile and web applications built on new technologies such as REST, AJAX, JSON and GWT. With Retina Web Security Scanner, you get comprehensive application coverage and sophisticated attack capabilities, backed by the lowest false positive and false negative rates in the industry.

Centralized management, policy, reporting and analytics

BeyondInsight delivers a comprehensive view of the vulnerabilities that provide doors into an environment, as well as the privileges that present corridors to sensitive assets. The security team benefits from being able to correlate vulnerability information with user activity, while IT gains a clearer view of how privilege policies impact overall security. This fusion of asset and user intelligence enables IT and Security to collectively reduce risk across complex environments.
Conclusion

BeyondTrust Retina provides security professionals with vulnerability assessment and risk analysis in context. Retina enables teams to proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud and virtual infrastructures, and communicate that risk to operations and compliance teams to reduce risk.

We believe our differentiation in the vulnerability management market lies in the deep reporting and analytical insights, greater levels of efficiency, enterprise scalability and zero-gap coverage you gain with our solutions.

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Account Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.