Measuring Corporate Risk with Retina CS Enterprise Vulnerability Management

April 2015
Table of Contents

Executive Summary............................................................................................................................................... 4
Critical IT Security Exposures.............................................................................................................................. 4
Corporate Risk Calculation .................................................................................................................................. 4
Protecting Your Castle.......................................................................................................................................... 5
Asset Risk Calculation ........................................................................................................................................... 6
Network Map by Smart Group ............................................................................................................................... 8
Calculations: Summarized Methodology ........................................................................................................... 9
Conclusion.............................................................................................................................................................. 10
About BeyondTrust ............................................................................................................................................. 10
This document contains information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of BeyondTrust.

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.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this white paper.

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.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

For the latest updates to this document, please visit: http://www.beyondtrust.com
Executive Summary

Vulnerabilities in your IT environment can wreak havoc on your business operations. These common weaknesses can be exploited by a variety of external and internal threats, from malicious individuals and “hacktivists,” to criminal hacking syndicates and nation states. The need to proactively address vulnerabilities is accentuated by requirements for always-on business services, cloud-based computing, and regulatory compliance. It’s therefore critical to design and implement a comprehensive security management strategy to ensure business continuity.

BeyondTrust’s vulnerability management solutions enable organizations to monitor and document IT weaknesses for a “near-real-time” view into asset risk and its implications for business operations. This risk can be monitored by individual assets or in logical groups, such as by application, operating system, geography, or even business function.

BeyondTrust solutions ensure that exposures to critical business processes and applications are monitored and managed at the enterprise level. This enables security resources to be managed as part of an overall IT resource management strategy and allows operations staff to better support the company’s key business objectives.

Critical IT Security Exposures

IT security is clearly the key business issue of today. The words “threat” and “attack” are commonly used as if they connote some monolithic evil that awaits every organization’s infrastructure. In fact, there are many kinds of threats and many modes of attack, and they can originate both inside and outside the organization. Their impacts are diverse and can include:

- Proprietary information loss
- Loss of system availability
- Loss or corruption of data or applications
- Loss of productivity
- Regulatory non-compliance
- Damaged customer relations / brand image

Corporate Risk Calculation

With Retina CS Enterprise Vulnerability Management, BeyondTrust has created a revolutionary methodology for expressing the risk of IT assets deployed throughout the organization. The solution assesses multiple security vectors and calculates a risk for each asset. This risk can be expressed in terms of a logical “Smart Group” within the solution such that the overall assessment of a business unit, geography, or custom container can be compared to other entities within your environment. The overall expression of risk is calculated based on four high-level vectors:
• **Vulnerability** – The quantity and severity of vulnerability audits identified by Retina or the PowerBroker Endpoint Protection Suite. Measurements are based on such factors as a lack of proper patch maintenance on a host or compliance issues related to current corporate security policy and best practices.

• **Attacks** – A direct measure of actual attacks – as flagged by BeyondTrust’s PowerBroker Endpoint Protection Suite – and their severity. The solution looks at how assets in the corporate environment are being exposed to threats and what type of threats challenge their integrity to perform business functions and protect data.

• **Exposure** – A measure of how open a system is to an attack. This is based on the number of open ports, shares, services, and users a host contains; the lack of protection such as a firewall or anti-virus solution; and the presence of any illegal or unnecessary applications that have been installed.

• **Threat** – A measure of potential danger to an asset from sources that may regard it as a worthy target, based on user-defined criteria and/or system role.

Based on the technical translation to business terms, organizations can have a direct method for understanding the asset’s security posture from raw technical data to business impact.

**Protecting Your Castle**

A simple analogy can provide a better understanding of this approach. Consider each asset in your environment to be a castle. Its construction, defenses, location and treasure are all factors for any impending attack. The castle walls protect an inner sanctum containing a treasure of gold (data, business operations, etc.). Armies (hackers, worms, etc.) are attempting to breach the castle walls and penetrate the inner sanctum to get the gold or disrupt the castle’s normal operations. In this case, the security vectors would be defined as:

• **Vulnerabilities** indicate how easy it is for the inner sanctum to be breached and how simple it would be to gain access to the gold.

• **Attacks** are represented by arrows, bombs and breach attempts on the walls and inner sanctum.

• **Exposures** reveal the extent to which the castle walls and openings can be attacked, and how poorly the castle’s periphery is protected.

• **Threats** are the lurking enemy armies on the hills surrounding the castle, who are priming for attack.
Sitting atop these four vectors is the essential *Criticality* of the castle itself; in other words, how valuable and important the castle and inner sanctum are in terms of value and importance to the empire. (See Figure 1)

**Note:** *Criticality* is not a security vector in itself. It is a weight applied to each of the four security vectors during raw assessments and internal calculations. It is variable and included in the calculation of each of the four primary risk vectors.

**Asset Risk Calculation**

The four security vectors described in the introduction have visibility within the solution as a calculated asset risk score. Individual assets have a numeric value that allows users to assess the risk to the organization and prioritize the highest-risk assets first. Throughout the rest of this paper, various depictions of these calculations will be covered and related to the security issues a business may face.

Based on the data model included in Retina CS Enterprise Vulnerability Management, a numerical value of 0 to 9.99 can be calculated for any asset to indicate its inherent risk. The higher the number, the higher the risk to the asset. A value of zero is when no risk is present or no data is available. The highest risk rating, 9.99, is assigned to assets that are just waiting to be compromised. When viewing an asset, this value is represented in the column labeled Asset Risk (See Figure 2):
Retina CS leverages the centralized BeyondInsight management, reporting and analytics console to summarize risk for all assets by color-coding the results and mapping them to risk scores. From this perspective, a user can see how asset risk applies to all systems within the environment. (See Figure 3)

- **Unknown** = 0, Grey
- **Low** > 0 and < 3, Yellow
- **Medium** >=3 and <6, Orange
- **High** >=6, Red

Retina CS also provides the asset risk score as a part of the Asset Report, which provides an up-to-date summary for all the devices within the specified Smart Group or IP range. (See Figure 4)
This chart accompanied by a Risk Statistics summary that offers a complete perspective of the assets. Details regarding each asset can be obtained via the user interface or any of the vulnerability reports. (See Figure 5)

![Risk Summary Statistics](image)

**Figure 5. Risk Summary Statistics**

Based on this table, the relative risk to the entire environment is low, but the open ports, shares, and vulnerabilities should be reviewed by security staff and system administrators.

**Network Map by Smart Group**

Retina CS can display assets and Smart Groups in a map format using the Asset Tab and Network Map function. This Java-based interface groups assets by various characteristics such as operating system, domain name, services, geography, and custom Smart Group. Figure 6 below illustrates this view and attack vectors for Vulnerability, Attack, Exposure, Threat and overall Risk Calculation.

![Network Map and Risk Vectors](image)

**Figure 6. Asset Network Map and Risk Vectors**
At a glance, we can see company XYZ (on the left in gray), based on a Smart Group, has four attribute groups that have assets at risk. The larger the circle, the more assets at risk an attribute group contains. The color indicates the risk to the group as documented above. After drilling in, the assets are illustrated by icons. Hovering a mouse over the group displays a pop-up that summarizes the asset or group’s overall risk.

This comprehensive view provides a common approach to assets in an environment. Displaying network maps by security risk is a unique concept in business. Retina CS considers all of the security data for an asset and provides a revolutionary method for documenting, reporting, and visualizing security risks throughout the enterprise.

Calculations: Summarized Methodology

The final risk vectors are calculated by the following algorithm:

A. Gather Raw Assessment Data
   For each asset, the solution gathers and/or calculates the “raw” assessment data over time.

B. Threshold and Normalize Data into Single Assessments
   For the multiple Audit and Attack Severities per asset, the solution merges each asset’s cumulative values to create a single summation value per asset.

C. Create Individual Asset Values by Scaling Against User-Defined Criticality Values
   For each asset, the solution calculates a 0-9 normalized Asset Value via an exponential mapping from user-defined asset Criticality. The idea is to take what users think an asset is worth (in a linear 0-9 sense) and adjust it for reporting purposes.

D. Scale Asset Value to 0 to 9 for All Variables Combined
   For each asset, the solution uses the Asset Values previously calculated to scale its summary assessment. This calculation is used to exaggerate assessments of high risk versus ones with low risks within the user interface.

E. Calculate Higher-Level Assessment Formulas per Asset
   For each asset, the solution uses advanced higher-level mathematical functions to calculate the final level values for graphical display within the solution.

F. Create Asset Value Weighted Averages for Attribute Groups
   For each Smart Group of assets, the solution creates weighted averages of the higher-level formula values, weighting by Asset Value to give more prominence to the most important machines in a group.

G. Calculate Final Risk Surface Value
   Finally, for all individual assets or Smart Groups, the overall risk “surface” can be calculated using the area formulas. This function is used to display data in the Network Map.
Conclusion

BeyondTrust has created a revolutionary methodology for expressing the risk of an asset in Retina CS Enterprise Vulnerability Management. The solution takes addresses multiple security vectors and calculates a risk levels for each asset. This expression allows an asset to be graded as to its inherent risk with respect to the enterprise. This risk can be expressed in terms of Attributes and Smart Groups within the solution such that the overall assessment of a business unit, geography, or individual asset can be compared to other entities within your environment.

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.