TAG CYBER

AUTOMATING CYBERSECURITY POSTURE ASSESSMENT: AN OVERVIEW OF THE BALBIX PLATFORM

EDWARD AMOROSO, TAG CYBER

Balbix®

AUTOMATING CYBERSECURITY POSTURE ASSESSMENT: AN OVERVIEW OF THE BALBIX PLATFORM

EDWARD AMOROSO

Establishing cybersecurity posture is an important step toward mitigating the cyber risks to an enterprise. Automation is the best approach for such assessment—one that builds on existing foundational security methods. The Balbix[1] Security Cloud is shown to automate this cybersecurity posture assessment process effectively.

INTRODUCTION

A major goal for enterprise security teams is to identify the attack surface that malicious adversaries can exploit. Such identification is the first step in mitigating cyber risk, and while the process might be simple to define, it is much tougher to implement. Modern enterprise infrastructure typically includes a complex mix of on-premises, cloud, SaaS, and hybrid infrastructure connected via proprietary and off-the-shelf software apps.

The process of defining all relevant vulnerabilities (or lack thereof) for a given attack surface is often referred to as the *security posture*. As one might expect, this has traditionally been achieved using a combination of scanning tools, asset databases, penetration test results, and other security tool output. Aggregation of this data has typically been done manually, often using proprietary algorithms and methods.

In this report, we explain how cybersecurity posture assessments can be automated. This is an important objective because it can establish a more continuous view of posture and will greatly reduce the possibility for coverage or completeness deficiencies. The commercial *Balbix* platform is used to illustrate how such a practical, automated assessment can be done in an enterprise context.

SECURITY POSTURE FOUNDATIONS

The challenge of establishing security posture can be visualized by mapping the assets of an organization against potential attacks. The two-dimensional structure that emerges is further complicated by the consequences, expressed in terms of financial loss,[2] that can result from a compromise. The result is a three-dimensional structure with a massive number of asset-attack-consequence mappings.

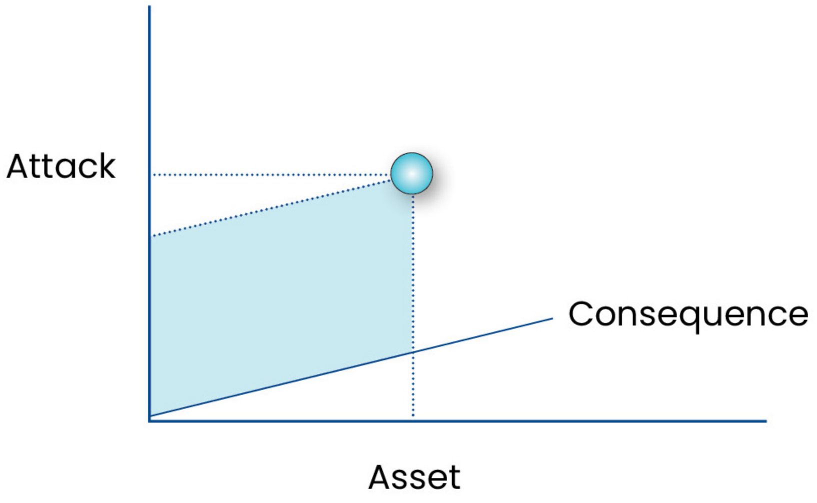


Figure 1. Mapping Assets, Attacks, and Consequences

The goal of gaining visibility into the present and ongoing status of cybersecurity controls is obviously not new. The primary means by which this goal has been addressed in the past includes familiar methods, many of which remain useful, but none of which have properly met the challenge. Since these traditional methods play a role in more evolved strategies for posture assessment, it is worth briefly reviewing the benefits of each.

Breach Simulation

One way to demonstrate the effectiveness of internal controls is to test them continually. To that end, so-called breach and attack simulation (BAS) tools have emerged to help enterprise teams determine the effectiveness of deployed security systems and tools. BAS implementations typically involve placement of active agents on either side of a control to continually test its ability to block attacks.

The advantages of a BAS approach include automated operation and continuous coverage. The disadvantages include limited flexibility and difficulty expanding to include more complex attack campaigns. Ultimately, BAS solutions are likely to find their way into a target security architecture, either as stand-alone platforms or as functional components of a more comprehensive protection architecture.

Vulnerability Scans

An additional major aspect of security posture assessment involves scanning networks, systems, and other resources for evidence of exposure. Operating a security scanner is perhaps the most familiar and traditional aspect of vulnerability detections and, as such, it is not only a requirement in every framework, but is also a major expectation of executives, board members, and other influencers.

The primary advantage of vulnerability scans is the familiar, mature data output that can support existing security and compliance programs. Most participants in enterprise security expect and understand this data, so scanning is essential in this context. The primary disadvantage is that scan data is prone to gaps in coverage and significant misinterpretation by executives and other stakeholders.

Penetration Tests

Penetration testing is also an effective means for identifying security vulnerabilities, especially ones that are subtle and not easy to find. For many years, enterprise security teams have relied on expert white hat hackers to probe, scan, and explore visible infrastructure with the goal of finding exploitable errors before a malicious adversary might find them and cause real consequences.

The advantage of penetration testing is that it is good at identifying the presence of security issues. That is, in environments where it is not generally accepted that exploitable holes exist, penetration testing can provide clarity. The biggest problem with penetration testing, however, is that it is an insufficient means for demonstrating the absence of problems. Not finding something during a penetration test doesn't mean that it doesn't exist.

Crowdsourced Testing

Finally, the use of vetted hackers (e.g., bug bounty) to help identify vulnerabilities has been an important component of an enterprise security posture assessment program. Since techniques, skills, and insights can vary so much between expert testers, having a large group of such individuals targeting a given system is a major advantage that offers depth of coverage and scope that cannot be reached by an individual.

The advantage of crowdsourced testing is the wide range of skills that can be harnessed to identify exploitable vulnerabilities. A drawback, however, is that considerable time and effort is required to properly vet and manage the ethical hackers. This workload can be mitigated through partnership with a capable commercial vendor, but it nevertheless represents a considerable hurdle.

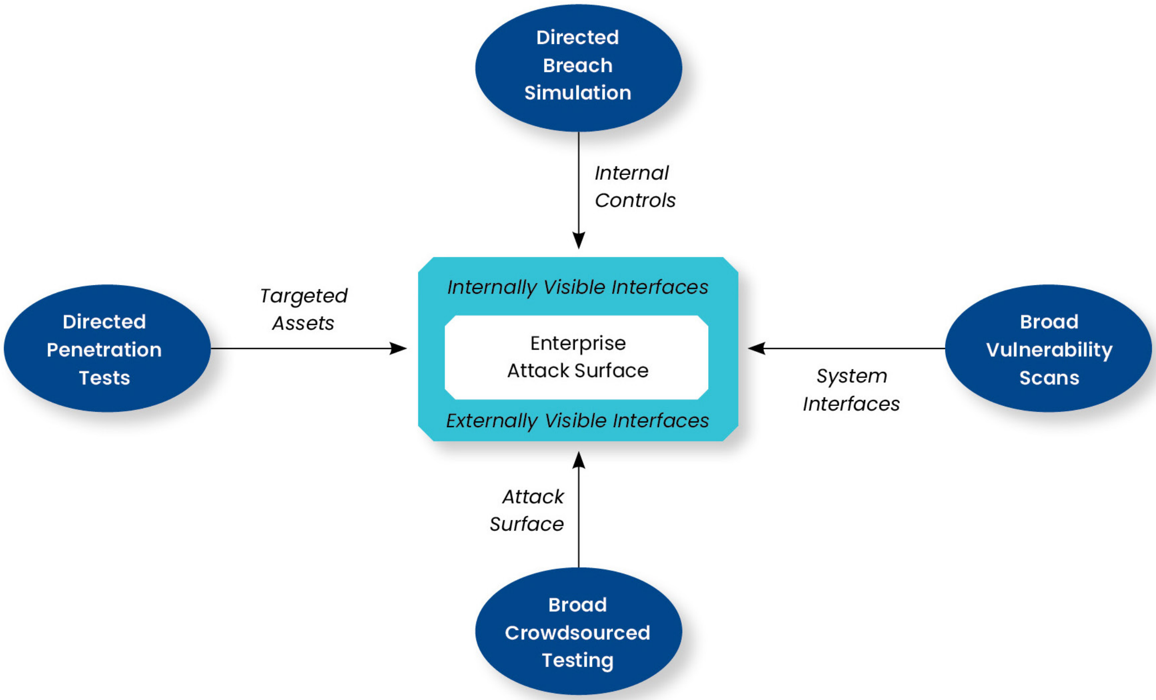

Directed Breach Simulation
Internal Controls
Directed Penetration Tests
Targeted Assets
Internally Visible Interfaces
Enterprise Attack Surface
Externally Visible Interfaces
Broad Vulnerability Scans
System Interfaces
Attack Surface
Broad Crowdsourced Testing

Figure 2. Common Traditional Methods for Identifying Security Posture

The challenge with these various methods is that while they each provide some degree of visibility into security posture, they remain disparate and uneven in terms of their automated or manual control. In the next section, we introduce a commercial platform from Balbix that uses automation as the basis for establishing an accurate, scalable view into the security posture of an organization.

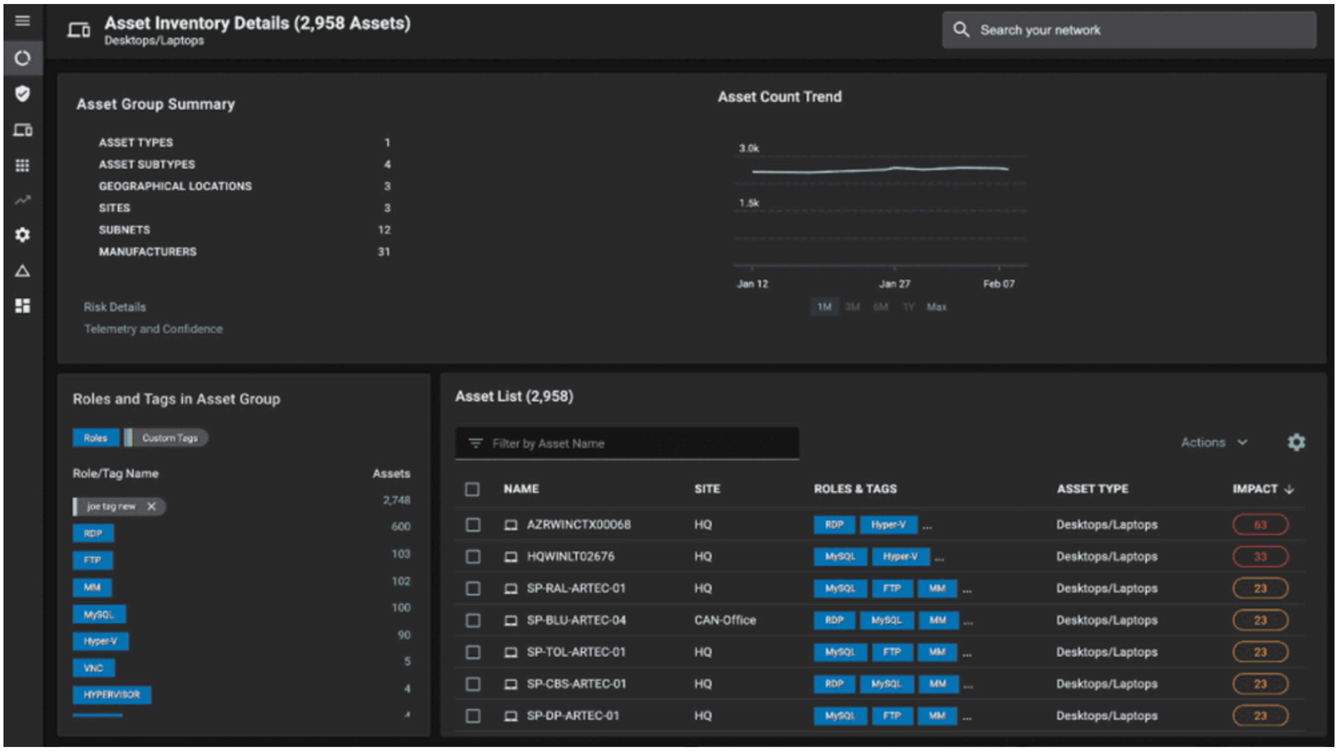
CASE STUDY: BALBIX APPROACH TO AUTOMATED SECURITY POSTURE

The commercial Balbix platform provides for cybersecurity posture automation. It was created to complement existing vulnerability management and related security posture capabilities deployed into the enterprise, while also addressing the major challenges and shortcomings that such functions have typically exhibited in practice for most security teams. Some teams will find that Balbix can replace their existing posture tools.

Automated Asset Discovery

The first goal of the Balbix platform is to address the ongoing challenge of inaccurate and incomplete asset inventories. Without clarity around the specific devices, apps, endpoints, and other resources in use across the enterprise, it becomes impossible to have a complete measure of security posture. This challenge is further driven by the consistent change that occurs even for those assets for which an inventory has been established.

Balbix addresses this requirement through automated, continuous monitoring of the enterprise, including traffic flows, to discover assets. The types of assets that emerge from this task include on-premises and cloud-based devices, applications, systems, and services, including managed and unmanaged assets. Fixed and mobile systems, including Internet of Things (IoT) devices are also included in the asset discovery capability.



Asset Inventory Details (2,958 Assets)

Desktops/Laptops

Asset Group Summary

ASSET TYPES	1
ASSET SUBTYPES	4
GEOGRAPHICAL LOCATIONS	3
SITES	3
SUBNETS	12
MANUFACTURERS	31

Asset Count Trend

Roles and Tags in Asset Group

Role/Tag Name	Assets
joe tag new	2,748
RDP	600
FTP	103
MM	102
MySQL	100
Hyper-V	90
VNC	5
HYPERVISOR	4
	4

Asset List (2,958)

NAME	SITE	ROLES & TAGS	ASSET TYPE	IMPACT
AZRWINCTX00068	HQ	RDP Hyper-V ...	Desktops/Laptops	63
HQWINLT02676	HQ	MySQL Hyper-V ...	Desktops/Laptops	33
SP-RAL-ARTEC-01	HQ	MySQL FTP MM ...	Desktops/Laptops	23
SP-BLU-ARTEC-04	CAN-Office	RDP MySQL MM ...	Desktops/Laptops	23
SP-TOL-ARTEC-01	HQ	MySQL FTP MM ...	Desktops/Laptops	23
SP-CBS-ARTEC-01	HQ	RDP MySQL MM ...	Desktops/Laptops	23
SP-DP-ARTEC-01	HQ	MySQL FTP MM ...	Desktops/Laptops	23

Figure 3. Balbix Platform – Discovered Asset Details

Data is discovered in the Balbix platform using a library of connectors that can handle two primary scenarios: *streaming connector*-based collection of data in motion, and *snapshot* connector-based collection of data at rest. Both take advantage of available interfaces including data dumps and application programming interfaces (APIs) to ingest the data necessary to build accurate inventory views.

Continuous Cybersecurity Asset Management
Once a complete picture of security posture has been created for the entire attack surface, the obligation emerges to manage and maintain the asset inventory and associated context in a unified manner based on automated platform support. The Balbix platform includes support for vulnerability and risk management workflows to ensure that assets are managed continuously to provide accurate security posture even as the attack surface evolves.

The collected data is used to categorize and manage assets based on their visible attributes, including internet protocol (IP) addresses, domain name system (DNS) information, and other signals that can be used to identify entities. The technique used by Balbix to normalize the accurate asset inventory view is called *host enumeration logic*, which supports stateful, intelligent de-duplication, sanitization, and other data clean-up tasks.

Such tasks must be performed at all levels of the technology stack, each of which will provide a different type of asset-related information. Layer 7 analysis, for example, will be useful to extract application-level information about assets, whereas layer 3 and 4 analysis will be useful to extract information about packet headers and protocol behaviors. The goal is to combine this collection into a unified view of the discovered asset.

Risk-Based Vulnerability Management
A major problem reported by enterprise teams is the large volume of alerts that is collected by typical vulnerability management and scanning tools. It is common for the number of alerts to become so high that security teams cannot maintain proper categorization, handling, and mitigation. This situation is ironic, because the success of vulnerability management programs is often measured based on the numbers of alerts generated.

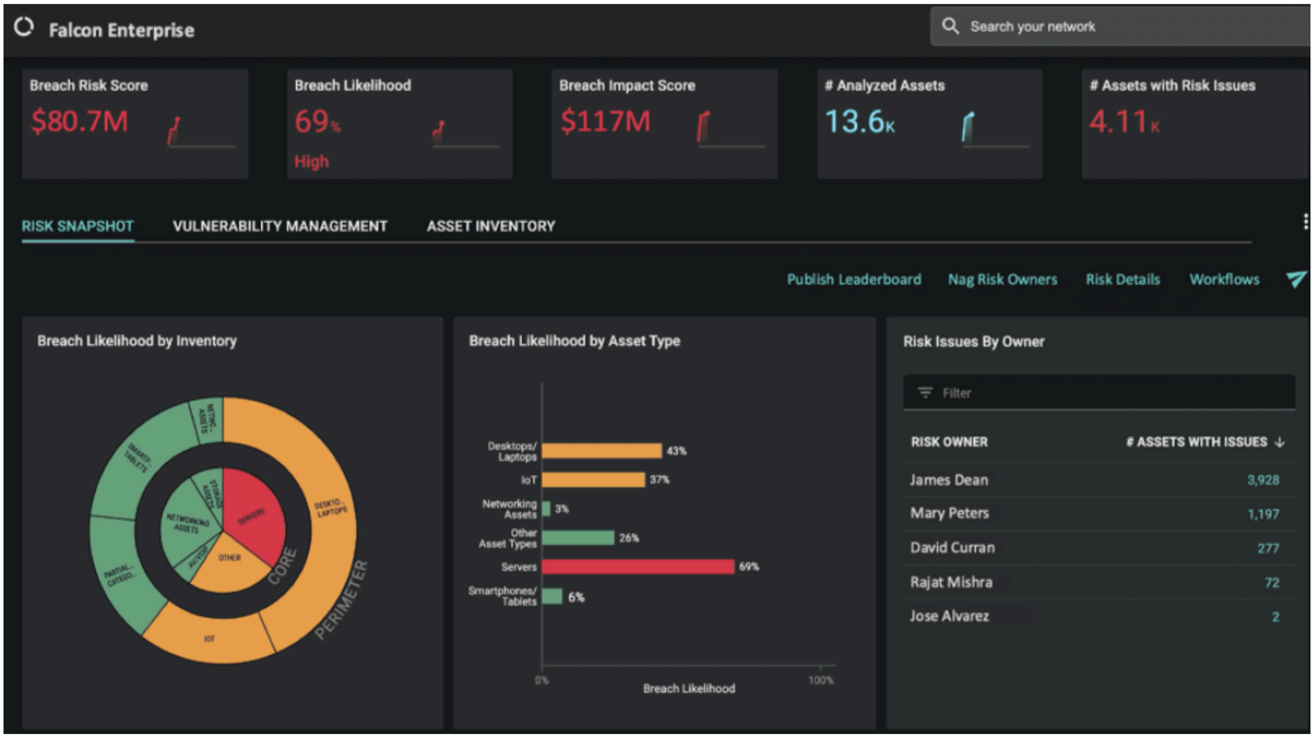
The Balbix platform handles the volume of vulnerability management by ingesting and analyzing data from a massive number of security-related sources. These sources include vulnerability assessment tools, security scanning platforms, threat and vulnerability feeds, BAS tools, penetration testing results, crowdsourced security test output, endpoint controls, and more.

Enterprise Vulnerability Prioritization
Prioritizing vulnerabilities requires attention to relevant factors, most of which will vary in intensity between environments. The Balbix approach involves establishing five major categories of factors—severity, threat, exposure, criticality, and controls—so that enterprise teams can organize the best mitigation strategies. Such mitigation can start with those vulnerabilities that can have the greatest negative impact to critical assets.

Ultimately, the goal is to identify a breach likelihood calculation, which is a computed summation of the individual attack vector computations. Such analysis is complemented by probabilistic graph models which estimate the vulnerability levels associated with the various risk scenarios. Collectively, these computations and values provide an organization with an accurate understanding of their security posture.

Cyber Risk Quantification in Dollars

The goal of accurately establishing a quantitative measure of security posture for the organizational attack surface requires use of a risk formula that makes sense to the local domain. To avoid multiple equations, formulas, and other metrics, the Balbix platform defines a consistent cyber risk equation that can be used across all assets and over all aspects of the organization to identify a meaningful posture assessment.



Breach Risk Score $80.7M

Breach Likelihood 69% High

Breach Impact Score $117M

Analyzed Assets 13.6K

Assets with Risk Issues 4.11K

RISK OWNER	# ASSETS WITH ISSUES ↓
James Dean	3,928
Mary Peters	1,197
David Curran	277
Rajat Mishra	72
Jose Alvarez	2

Figure 4. Balbix Platform—Risk Quantifications

The Balbix platform automates the calculation of risk in dollars. While this is certainly not a new strategy in enterprise cybersecurity, the specialized artificial intelligence models integrated into the platform support the calculation of risk trending, breach likelihood, breach impact scoring, breach likelihood by inventory, and more. These are presented in a visual display that is easy to share with both practitioners and executives.

Cyber Risk Visibility and Board Reporting

The final goal of the Balbix platform is to ensure that enterprise security teams have the best available tools for reporting and explaining vulnerability and risk posture to the organization. This must include reports for senior executives including board members as well as colleagues with more detailed understanding of security programs. Such reporting must cover the entire attack surface and must account for continuing change.

Most executives will tend to focus on the impact of potential breaches, because this represents the most direct consequence of cyber risk to business operations. Balbix supports detailed impact modeling that uses impact estimates based on several factors, such as prior information, contextual impact modeling based on current usage, volumes, and interactions.

ENTERPRISE ACTION PLAN

It is recommended that enterprise teams act immediately to review, address, and improve their cybersecurity posture assessment. This is best done using an automated platform that can unify existing posture-related tools such as scanning and security testing. As suggested above, the Balbix platform provides excellent support in this regard and should be included in source selection plans.

[1] See https://www.balbix.com/.

[2] See https://www.fairinstitute.org/ for information on how the FAIR (Factor Analysis of Information Risk) model supports consequence analysis based on financial impacts.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Balbix, Inc. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.