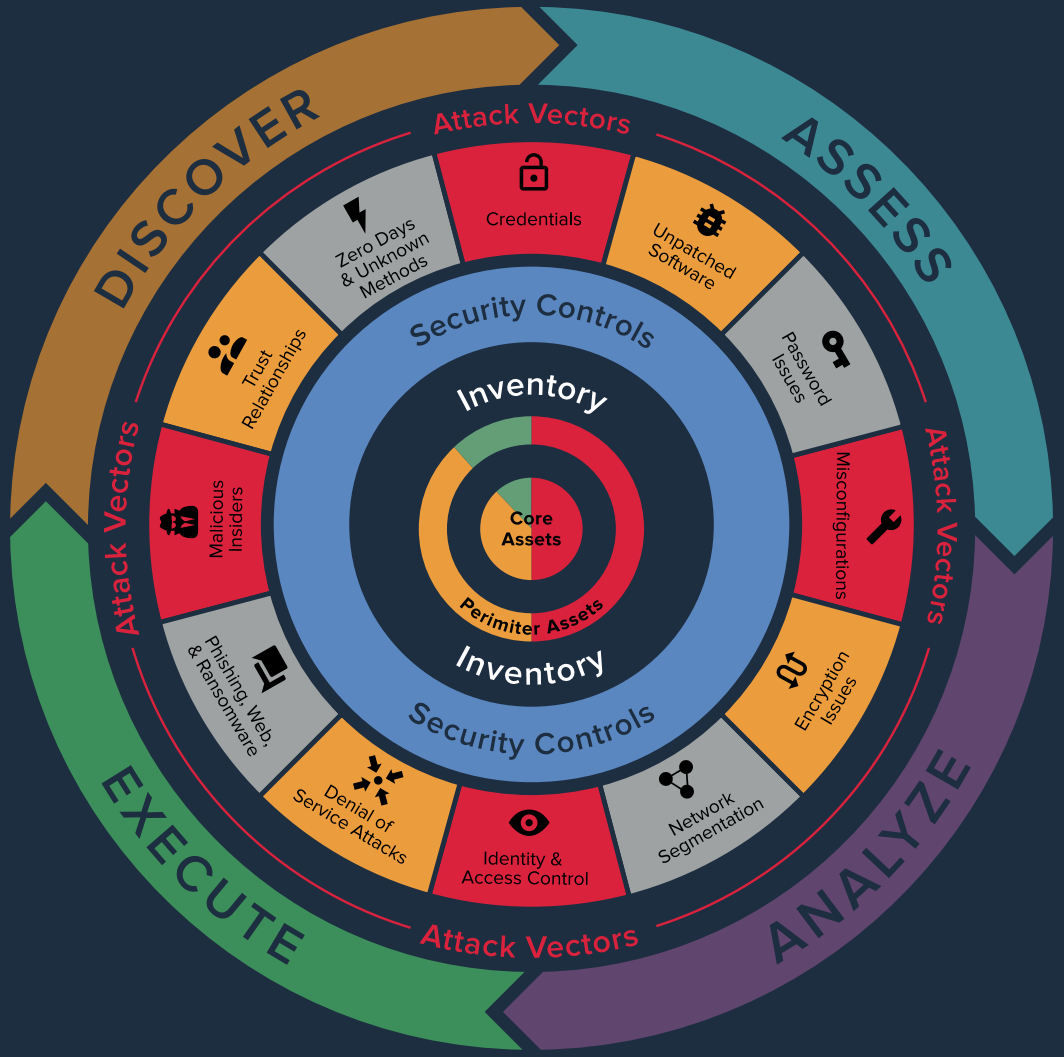
3 Essential Tools for CISOs to Assess and Report on Breach Risk

As a CISO, you need to assess and report on your enterprise's breach risk in a number of situations. You may be a new CISO trying to get a quick handle on what you have inherited and where to begin. Or you may be a seasoned pro who reports on a periodic basis to your company's audit committee or board of directors. A successful approach to assessing breach risk begins with an accurate overview of your security posture.

You need to know your threat landscape and the risk appetite of your execs and the board. Then you need to assess current security controls and their effectiveness and identify top risks and their relevance to your organization. What is the most effective way to do that?

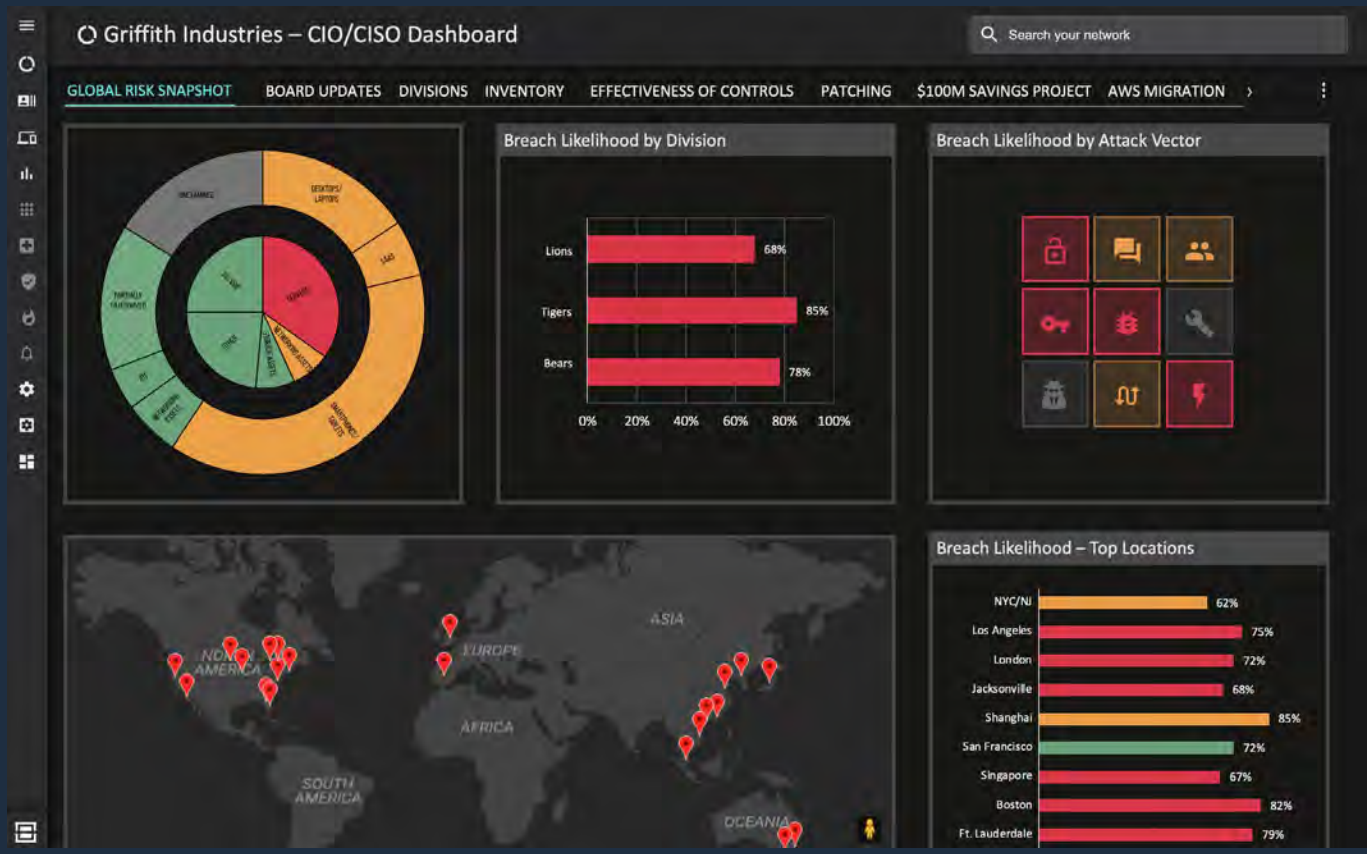
Here are **3 tools** that you absolutely need in your arsenal to achieve clarity and demonstrate using concrete data that all the right actions are being taken to manage cyber risk. This will also enable you to formulate your cybersecurity operating plan which is aligned with the business and will be able to demonstrate progress in a data driven way.



Enterprise security posture

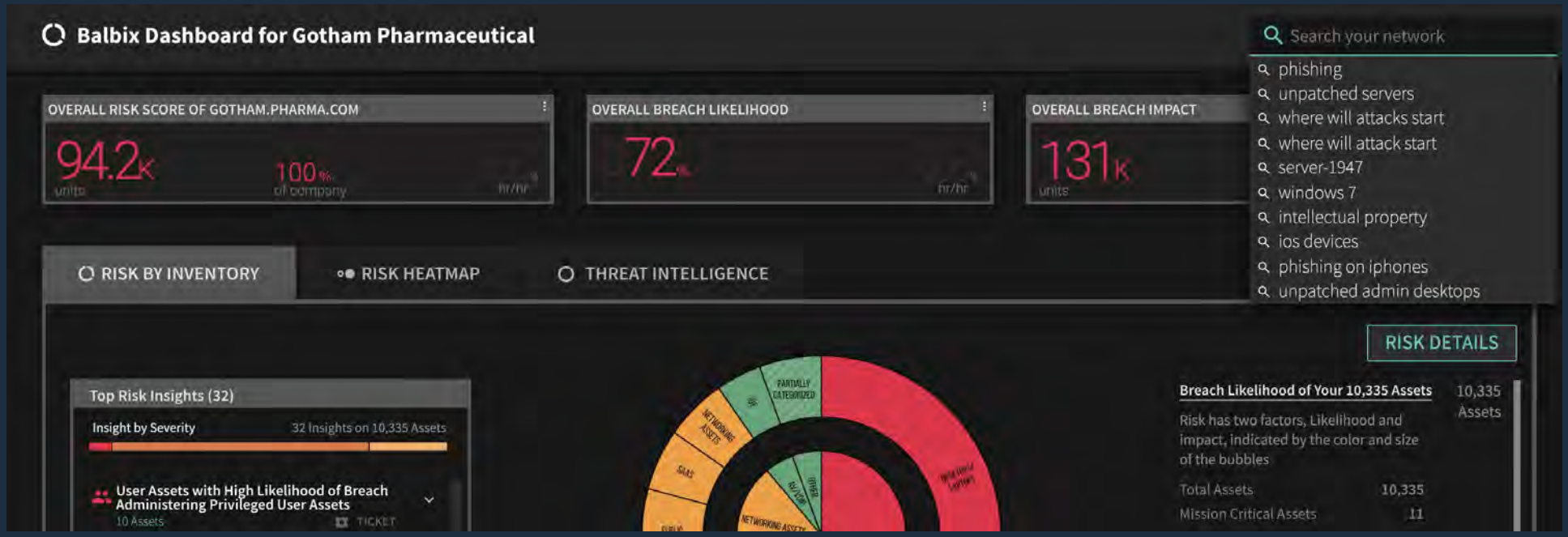
Custom Dashboards

An essential component of your job is to provide progress updates in your cyber risk reporting. These updates provide information on the status of your security initiatives and the changing threat landscape. To get this information about your programs, you need various types of risk dashboards. These can enable you to summarize your entire risk management program in a series of widgets and present information like the current status of your threat landscape and its implications, cyber risks based on business units and measured through risk indicators specific to that business unit, implementation status, and actual impact on risk reduction through a series of charts, graphs and analyses like timeseries and trendlines. To support effective decision making, optimally designed dashboards allow you to drill down from the group-level risk status to individual business units—and finally to the vulnerable assets underlying particular threats.



With Balbix, you can create and manage custom dashboard to highlight data relevant to you. You can create multiple types of dashboards to show either the status of various aspects of your job such as inventory by geo location or a detailed list of risk insights, progress towards your goals. If your job involves overseeing other risk owners, you can add comparator dashboards which enable you to compare metrics by site or by assets types, and more.

These dashboards are also customizable for individual roles. For example, business unit heads should be able to view data and metrics related to their own business unit, while the CISO should be able to aggregate the dashboard output across business units, functions, and entities.



Natural Language Search

If you needed to quickly list all your enterprise assets susceptible to Wannacry, how long would it take your team to do it? If you wanted to list of critical servers using expired or self-signed certificates, how easy would that be? How about getting an inventory of all your assets with access to intellectual property? Having access to a natural language search functionality to query your security posture for components of interest is a powerful tool at your disposal.

This would enable you to ask questions about your asset inventory to understand every type of device on your network, the vulnerabilities that put your enterprise at risk, and narrow down to business critical assets with a highly severe vulnerability if you needed to.

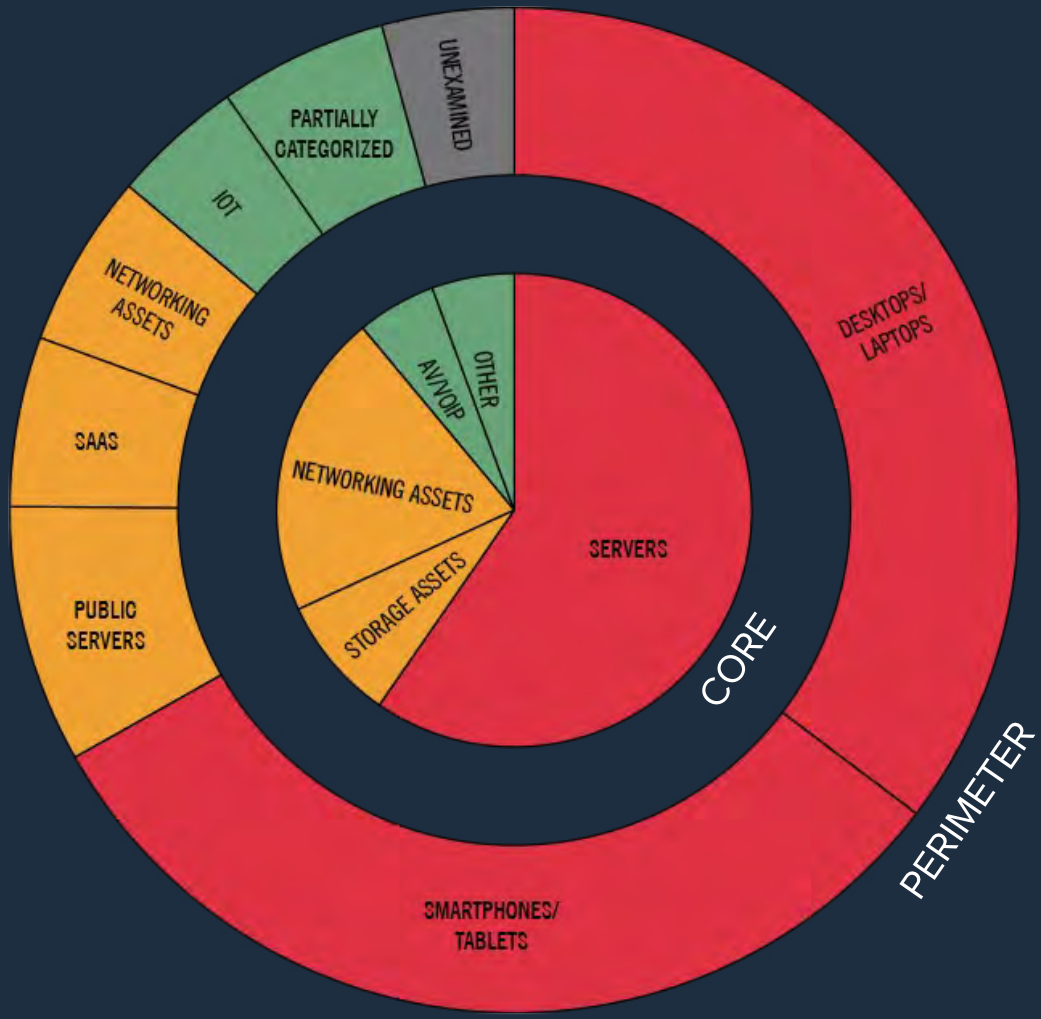
With Balbix, you can get answers to questions about your inventory, security posture or breach risk using natural language search. Customers can query their inventory using IT vocabulary, e.g., “windows servers in london”, combine security and IT terms to find “unpatched switches in NYC”,or search by CVE number, e.g., “CVE-2017-0144”, or its common name “wannacry”. Using higher level queries like “where will attacks start”, “assets with intellectual property”, and “risk to customer data” is also possible.

You can also use Balbix’s natural language search to define groups and assign them to specific owners. Groups and owners can be organized in multiple hierarchies to reflect the organizational structure of your enterprise. With these powerful search capabilities, you can look for gaps in ownership and use this to further refine your setup.

Risk Heatmaps

A risk heatmap is a visual representation of cyber risk data where colors are used to connote meaning. Risk heatmaps are an excellent tool to provide an instant overview of your security posture. However, there is a caveat. If your risk heatmap presents a point-in-time picture of your security posture, then it is not useful as the data is likely outdated since it doesn't account for changes in your asset inventory, threat landscape, and network. A risk heatmap that is continuously updated in real time tells a different story.

There are several types of risk heatmaps. Balbix provides one that maps your IT asset inventory by type (core vs perimeter, desktops, laptops, IoT, BYOD, servers, cloud assets, etc.) and risk associated with each of those categories.



Supporting the Data-driven CISO

Your cybersecurity jobs consist of many activities, tasks and linked workflows. You may rely on several tools, which are often not integrated with each other. Decisions need to be made at many points, and often the data to make an informed decision is not available. In addition, there are critical obstacles that cause some parts of your jobs to be tedious, time consuming and/or error prone. With these 3 essential tools in your back pocket, you can effectively and efficiently assess and report on your organization's breach risk. Balbix can help make your cybersecurity jobs easier and more effective. Let us show you how.

Understand your attack surface

Balbix continuously observes your extended enterprise network inside-out and outside-in to discover the attack surface and analyze hundreds of millions (or more) of data points that impact your risk. Organizations can track their inventories in real-time and stay current on security issues affecting business critical devices, software, and other assets.

Get an accurate read on your risk

Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. Analysis of all possible breach scenarios—the various combinations of attack starting points, target systems and propagation paths—and precise determination of the riskiest scenarios is key. This real-time risk model is surfaced to relevant stakeholders in the form of highly visual drill-down risk heat maps and Google-like natural-language search. You can ask questions like "where will attacks start" or "what is the risk to customer data," and get a relevant, highly visual answer, along with drill-down details on how to mitigate the risk.

Obtain prioritized action items with prescriptive fixes

Balbix generates a prioritized list of actions that will affirmably reduce risk. Security posture issues with the greatest risk are addressed first before working down the list of smaller contributors. For each issue, responsible owners for the corresponding assets are identified and then prioritized tickets containing all relevant context are generated and assigned to these owners. Progress is closely tracked and fed back to relevant stakeholders.

LEARN MORE

Balbix®