TRENDING TOPIC FOR CISOs:

Why You Need to Consolidate Cybersecurity Tools

Balbix®

{Fig A}

{Fig B}

If you were to take a 10,000 ft view of your organization's current security posture, would you see *Figure A* or *Figure B*?

Chance are, your answer is **Figure A**. This is because most organizations have a security posture that is a mishmash of security point products that have been deployed in the quest to address security “projects”.

Let’s take cybersecurity visibility and risk assessment as an example. Need inventory visibility? Let’s buy Product X. Need a vulnerability management tool? Deploy Product Y. Need security posture reporting to the board of directors? Go for Product Z.

This project-oriented approach to security visibility is one where teams are focused on completing security projects off of to-do lists without having any real insight into whether or not these projects have a meaningful impact on your organization’s security posture. This usually involves deploying products from a bunch of different vendors without realizing that these are all point solutions that don’t interoperate in any meaningful way.

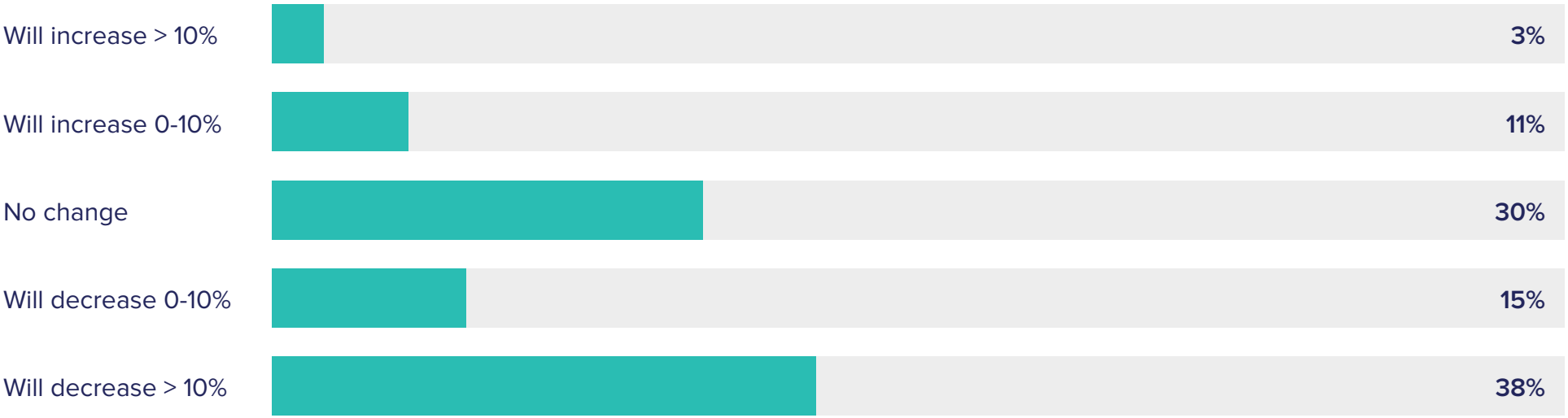
What this really means is that your security visibility practices and products are too narrowly focused to be completely efficient and effective. As a result, you are devoting most of your efforts on fixing indicators of compromise (IOC) alerts, patching, and chasing commitment biases, without really knowing the answers to questions like which of your assets are most critical, what threats are active right now, and which assets are most vulnerable to what kinds of attack vectors. The bottom line is that your security posture investments may not be aligned with how attacks can potentially occur and how you can be adequately prepared and cyber-resilient in your security posture.

Contraction in cybersecurity budgets

Now with the changing macroeconomic climate and the toll taken by recent events, leaders in every function, including information security, will be asked to make cuts. The extent of those cuts remains to be seen, but in a recent live survey of more than 150 cybersecurity leaders, more than 50% responders said that they expect their cybersecurity budgets to be cut over the next 6 months.

As a leader, you are probably already thinking about how you'll continue to get results with less budget and a smaller team. You realize that you can't afford to continue to dedicate time, resources and budget toward fixing problems without having a clear understanding of how those actions reduce the company's overall cyber-risk. Your existing security practices need to be evaluated with a fresh lens to enable you to do more with less and maximize your cybersecurity program efficiency.

How do you expect your budget to change over the next 6 months?



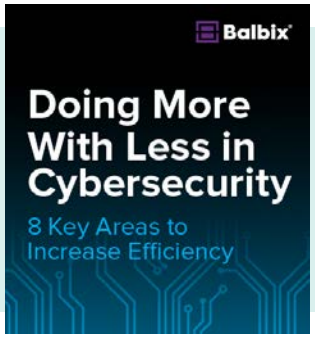
Consolidation is the need of the hour

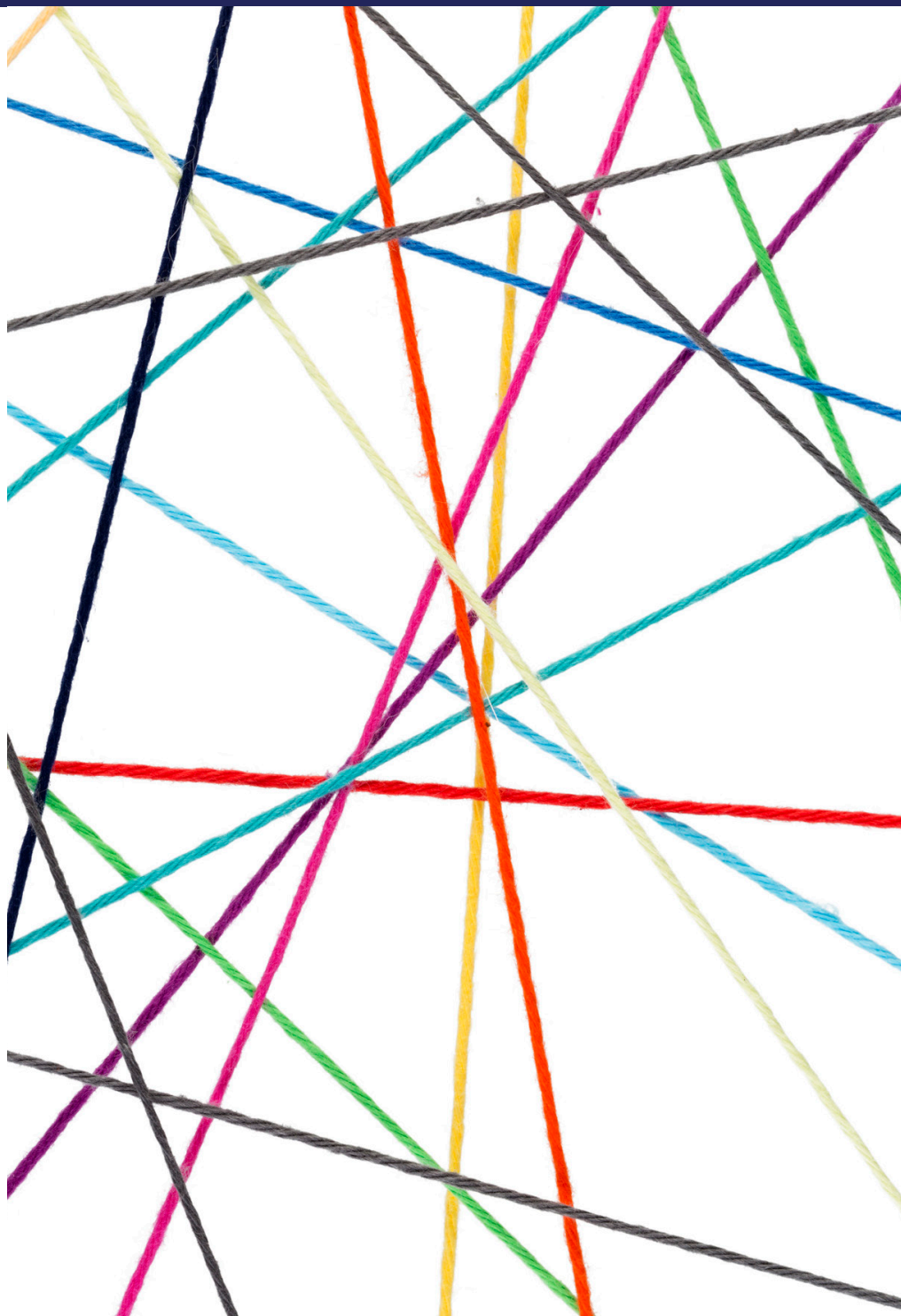
One way to maximize cybersecurity program efficiency is to consolidate various cybersecurity point products so that you are no longer spending money and team effort on something that's not meeting your needs anymore. Balbix is a comprehensive AI-powered cybersecurity platform that can help consolidate your inventory, vulnerability management, and cyber-risk reporting (and many other "features" offered by other tools) into one.

With Balbix, customers are able to maximize their cybersecurity program effectiveness and efficiency by measuring and monitoring their attack surface, consolidate their security program by finding security and IT tools that are no longer effective and providing their team information that makes daily workflows much more efficient.

Maximize security program efficiency

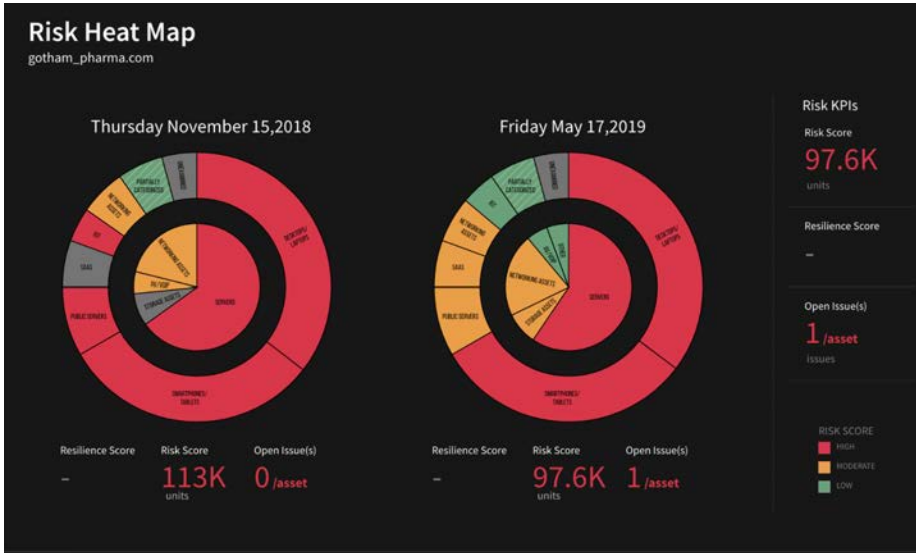
Learn more





How Balbix can help

The Balbix platform analyzes your entire attack surface in order to obtain a more accurate view of breach risk, compute a risk score for the enterprise, then compare that score against peer organizations. Not only will this allow for more transparency in the company's security posture, but it will increase the business' security teams efficiency and reduce risk by seeing which actions need to be taken in order to improve your security posture.



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®