WHITE PAPER

Shifting Perspective:

FROM REMEDIATING TO AVOIDING BREACHES

Balbix

Shifting Perspective:
FROM REMEDIATING TO AVOIDING BREACHES

Executive Summary

The vast majority of cybersecurity approaches, techniques, and solutions to date have been about preventing attacks or exploits as they occur, or rapidly finding and mitigating breaches after they've happened. Reactive tools and controls are typically point-in-time assessments and not only that, these periodic scans generally produce a large number of alerts and events that are difficult to act on as they are not prioritized and without business impact.

But in today's threat environment, eliminating risk and avoiding breaches requires enterprises to transition from focusing their resources and efforts on putting out fires to transforming their security practice to predictively and proactively controlling breaches. As the threat of attack continues to increase exponentially, the need for more proactive tools and technologies has rapidly expanded. The challenge is making breach risk assessment and control simple to operationalize and accessible to businesses that lack the team necessary to manually analyze the attack surface, or the budget to deploy a plethora of controls for the security problem. Or if you are an enterprise with a Security Operations Center (SOC), the challenge is to increase the productivity and effectiveness of managed or augmented SOC service teams to reduce the time spent on reviewing logs and alarms or remediating breaches and focus more on proactively preventing or minimizing new breaches.

In this paper, we will provide a deeper look into existing cybersecurity practices, their shortcomings, and the urgent need to avoid breaches altogether and not just mitigate them after the fact.

The challenge is making IT risk assessment and planning simple to operationalize and accessible to businesses that lack the security team necessary to manually analyze the attack surface, or the budget to deploy a plethora of controls for the security problem.

Current cybersecurity initiatives are mostly reactive

In recent years, cybersecurity has emerged as a top concern for enterprises worldwide, driving significant investment in procuring new security products and services. However, nearly all new security spending and effort is directed toward detecting an attack in progress or responding to one that has already occurred. While putting out security "fires" is an essential practice, the best way to build a secure enterprise is not necessarily by hiring a lot of firefighters (incident response teams) or purchasing all possible anti-fire equipment (controls such as firewalls and endpoint security). Instead, consider "fire-proofing" your infrastructure and understanding your risk at all times.

Borrowing some terminology and thinking from the military, let's consider an actual cyberattack by an adversary to be a "boom." Then

the practices and products pertaining to cybersecurity can be mapped to three phases centered around their operations with respect to the point of boom. Left of Boom phase would include controls and planning to predict breach risk, Boom phase would encompass controls to detect and stop attacks in progress, and Right of Boom phase would include tools and controls for incident response, triage, and security operations. (**Figure A**)

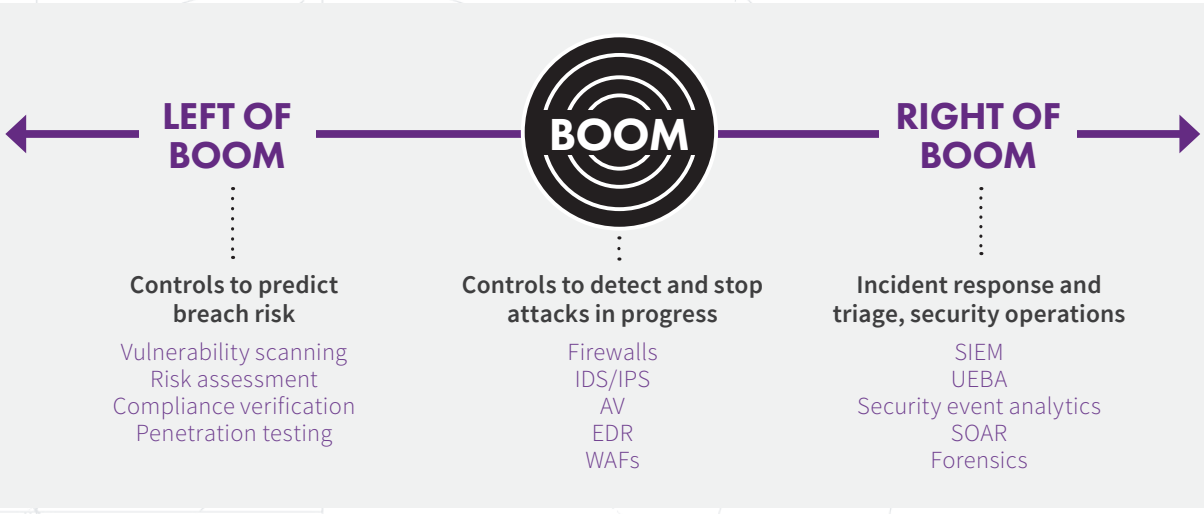
As the threat of attack continues to increase exponentially, the need for Left of Boom tools and technologies has rapidly expanded as many more businesses are at risk of suffering a breach.

Investing in Left of Boom controls can drive extreme value and efficiency

In recent years, there has been an explosion of awareness and interest in security controls (Boom) and security operations (Right of Boom) areas. There has been some fantastic innovation in next-generation firewalls and endpoint controls, using technologies such as virtualization, security event analytics, AI, and workflow automation. Several tens of billions of new security spending and investor value has been created in the last five years with new technology. While there is no dearth of products and innovation in the Boom and Right of Boom areas, there has been a marked lack of innovation in Left of Boom technologies. But tackling the Left of Boom phase has a very high value – it can inform and direct every aspect of your security practice, driving value and efficiency.

Enterprise risk assessment and planning technologies, such as GRC, rely extensively on manual processes, and are episodic (typically done 1-2 times a year). Essentially, such systems are just some math calculations, pie-charts, and reports on top of questionnaires filled by humans, and lead to an incorrect notion of "paper" cyber-risk that is very different from the real on-network breach risk.

Figure A



Another related practice, vulnerability assessment (VA), is the enumeration of systems likely to be compromised from just one attack vector – unpatched software. VA is rules-based and unable to learn new targets or attack methods by itself. VA is also episodic, with periodic scans generally producing a large number of alerts and events that are difficult to act on as they are not prioritized and without business context. VA tools work mostly on managed devices, and have limited coverage of the vast and rapidly expanding enterprise attack surface. For example, vulnerability assessment does not tell you anything about the risk to your business from weak passwords and shared passwords, or incorrect or incomplete implementations of encryption. Similarly, VA cannot tell the difference between an unpatched primary domain controller and an unpatched lab server.

What *all* businesses need, is a smart system of automated risk assessment, which learns the context of your business, and then continuously analyzes the complete attack surface with little or no human effort and prescribes the necessary tactical and strategic mitigations to eliminate risk.

Medium-sized businesses need to start Left of Boom

As the threat of attack continues to increase exponentially, the need for Left of Boom tools and technologies has rapidly expanded. Solutions once employed only by large enterprises and government agencies are becoming increasingly applicable for mid-size enterprises and even SMBs. The challenge is making breach risk assessment and planning simple to operationalize and accessible to businesses that lack the team necessary to manually analyze the attack surface, or the budget to throw a kitchen sink of controls at the security problem. If you are the Chief Information Security Office (CISO) at a company that has revenues of several hundred million to several billions, and a small security team of less than five, you can't simply try to replicate the controls and operations of a top Wall Street bank. It would be an insurmountable challenge for you to keep your business secure without a robust strategy. And innovative Left of Boom approach and tools can help you with this plan.

Large enterprises need to upgrade their Left of Boom thinking

Everyone, even organizations with a mature security posture, should systematically and continuously assess whether all required controls are present and functioning, and if there are any important gaps, or any non-working or sub-optimal controls. New Left of Boom technologies have the potential of bringing the risk and security practice in your organizations together and enable you to eliminate the gap between "paper" risk and on-network breach risk and maximize your security ROI.

Using automation to identify and predict your breach risk is key

What *all* businesses need, is a smart system of automated breach risk assessment, which learns the context of your business, and then continuously analyzes the complete attack surface with little or no human effort and prescribes the necessary tactical and strategic mitigations to minimize risk. There is a lot of business value in using automation to identify all that

might go wrong from a cybersecurity standpoint, prioritizing these indicators of risk (IoR), and taking proactive steps to mitigate the risk. This would lead to better coverage, hopefully no breaches resulting from attacks, a cybersecurity team focused on the top priorities that need to be addressed, and a robust security posture at a fraction of the cost/time.

Avoiding breaches through prediction and proactive mitigation

Gartner and other analysts also recognize the overwhelming and urgent need for Left of Boom thinking. One such approach is breach avoidance – a proactive approach that starts with putting the right tools in place to comprehensively assess the breach risk from all your IT assets across all attack vectors, coupled with an understanding of external threat risk. Then prioritizing the actions you need to take to mitigate the risk and finally applying prescriptive fixes to patch each action item.

Breach avoidance will modernize risk assessment for the era of hyper-threats, cloud, BYOD, IoT and the distributed enterprise, leveraging emerging technologies such as artificial intelligence to make assessment automated and continuous. Left of Boom thinking when properly implemented can be predictive, prescriptive and preventative.

In today's threat environment, eliminating risk and avoiding breaches requires enterprises to transition from focusing their resources and efforts on responsively putting out fires to transforming their security practice in the Left of Boom area. Companies adopting Left of Boom thinking will gain a competitive advantage in managing and mitigating breach risk efficiently, gaining better resilience and simplified compliance.

A new solution for avoiding breaches

The Balbix breach avoidance platform, BreachControl™, helps your enterprise avoid breaches by providing continuous and real-time risk prediction, a prioritized list of actions, and prescriptive fixes for each action.

Let Balbix show you how you can plan for, predict and prevent cyber-disasters!

3 Steps to Breach Avoidance

1

Predicting Breaches

Assess breach risk across all IT assets and all attack vectors and incorporate external threat data, to predict breach scenarios.

2

Prioritizing Actions

Prioritize mitigation actions based on business risk to obtain an actionable list based on risk.

3

Prescribing Fixes

Generate prescriptive and clear recommendations of actions to reduce the time-to-fix and prevent a breach from occurring.

Balbix

3031 Tisch Way, St 800
San Jose, CA 95128
866.936.3180

info@balbix.com
www.balbix.com