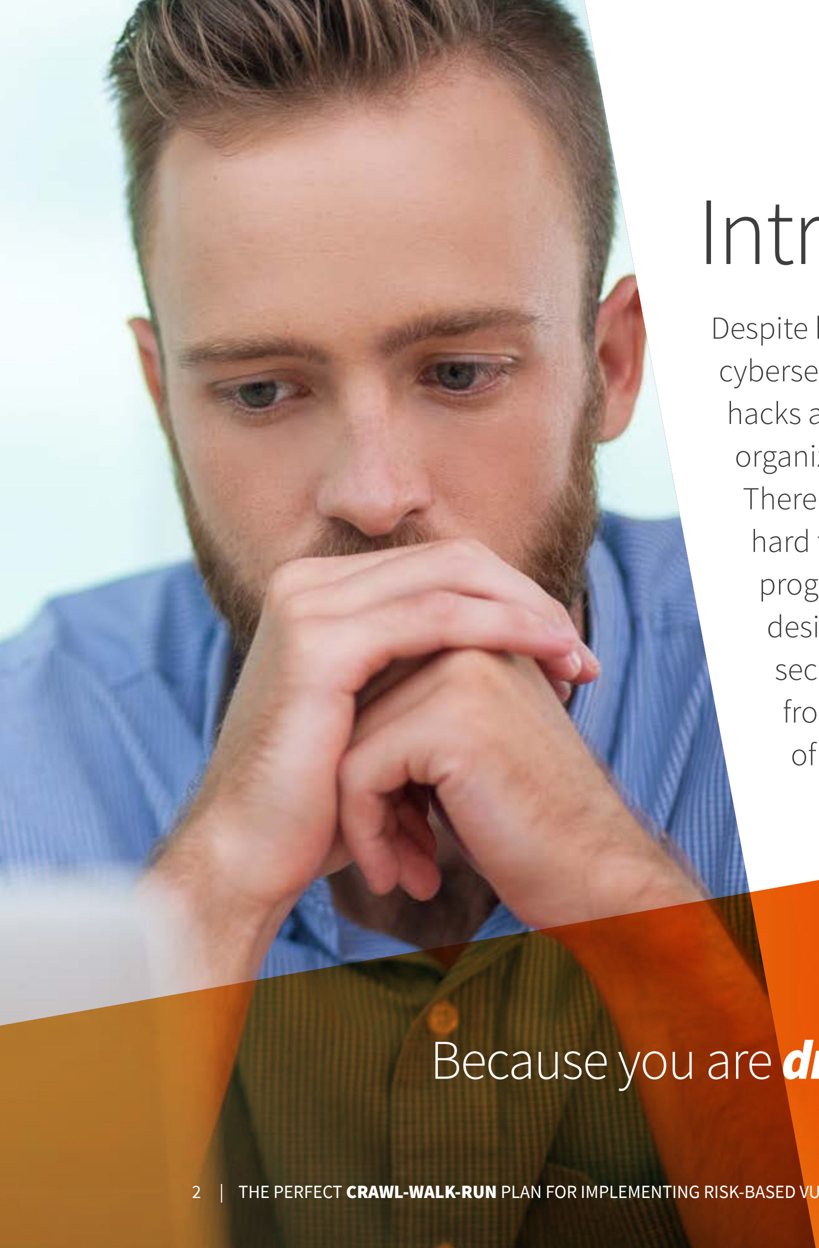
Balbix®

The Perfect Crawl-Walk-Run Plan for Implementing Risk-Based Vulnerability Management



Introduction

Despite hundreds of security products and billions of dollars a year cybersecurity spend (expected to top $100 billion by 2020), breaches and hacks are in the news every day. Cybersecurity is a tough problem because organizations have a massive and exponentially growing attack surface. There are myriad of ways by which networks can be breached, and it is very hard to keep up with the attackers. An enterprise vulnerability management program is the cornerstone for any modern cybersecurity initiative and it is designed to help security teams proactively understand and improve their security posture to avoid breaches and protect the business from brand + reputation damage and loss of customer trust.

Know why your vulnerability management program is not up to snuff?

Because you are ***drowning in data*** but ***starving for insights***.

Understanding and acting on data output from your vulnerability assessment scanner is a critical component of your vulnerability management program. However, if your scanner is spewing out vulnerabilities in the thousands every time a scan completes, your team is bound to be overwhelmed and struggling with how to proceed. This inability of security teams to address the vulnerabilities in a timely manner (due to vast number of action items) is a significant shortcoming of the traditional vulnerability management program.

This is one of the main reasons why you are unable to stay up-to-date with your patching and as a result, chances are that your periodic scans will return the *same* list of vulnerabilities each time.

4 Reasons Why Organizations Struggle with Patching

1. Overwhelming number of alerts with too many vulnerabilities to patch

2. Lack of prioritization to focus the security team's efforts towards patching most critical issues

3. Small, resource-constrained teams, with not enough people

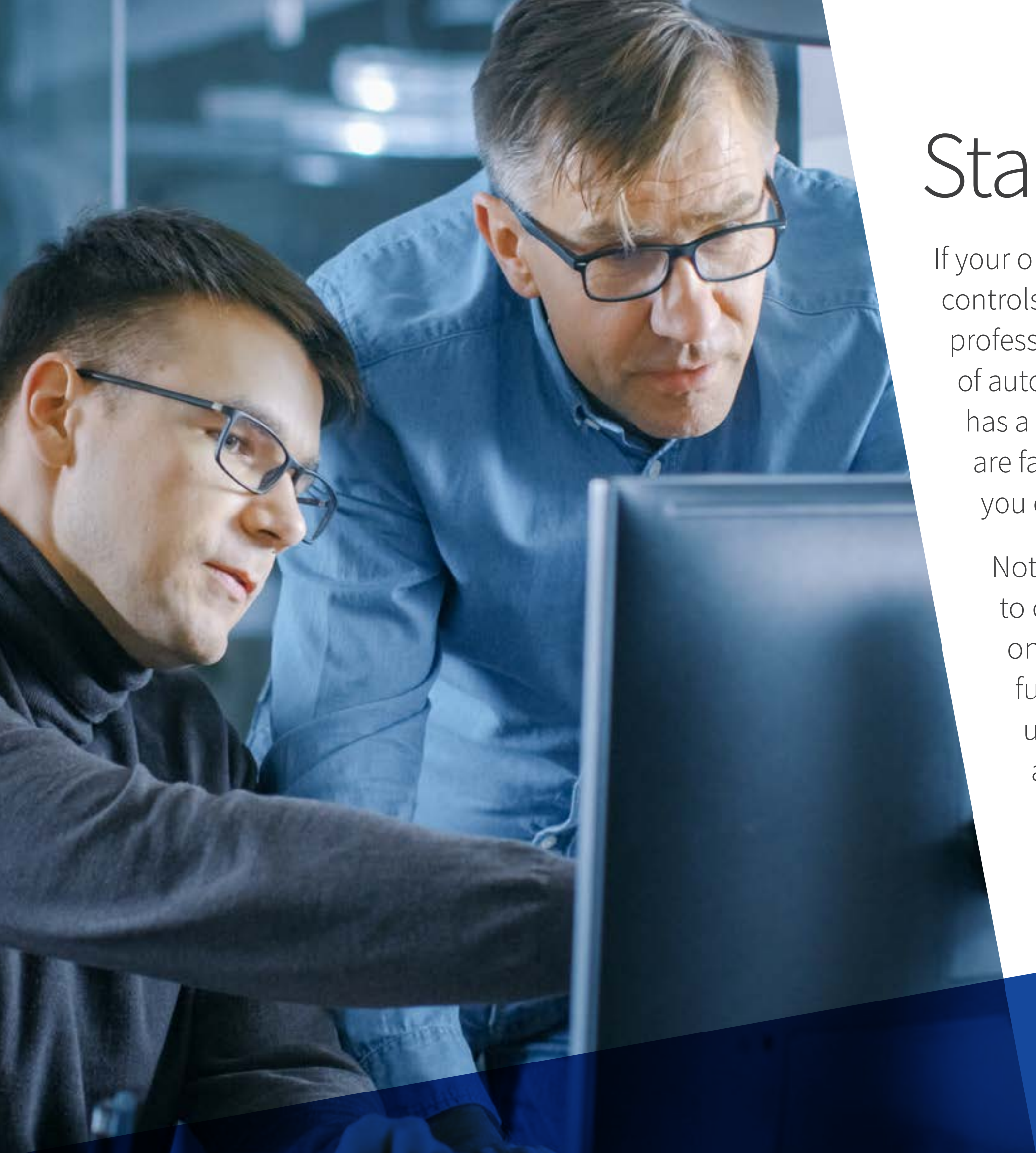
4. Lack of guidance on HOW to fix the issues

> "***99%*** of the vulnerabilities exploited by the end of 2020 will continue to be ***ones known*** by security and IT professionals ***at the time of the incident***."
>
> —Susan Moore, Smarter with Gartner

Enter risk-based vulnerability management

In order to truly enhance security posture and improve resilience, organizations need a risk-based vulnerability management approach that not only identifies vulnerabilities across all assets, but also prioritizes the action items based on business criticality and actual risk by understanding the context around each vulnerability and the enterprise asset that it affects. And then, it offers prescriptive fixes to address the issues. Armed with this information, security teams can be better equipped to tackle the open vulnerabilities head-on and start closing them.

So, here's the key question—***how do you get started*** with risk-based vulnerability management?



Starting to crawl

If your organization has yet to implement modern security controls and practices, and you have zero to a few security professionals on staff you need converged security products, lots of automation, and simple prescriptions. If your organization has a traditional vulnerability management tool deployed, you are familiar with the problems listed above. In both the cases, you can start smart with risk-based vulnerability management.

Not unlike other technology transformations, it's best to crawl before you try to walk or run. This is really the only way to build a strong and resilient bridge to your future state. The initial phase of your journey involves understanding vulnerabilities, assessing breach risk, and prioritizing actions to move toward a predictive, proactive, and effective risk-based vulnerability management program.

The **Crawl** Plan

Here are five recommended steps:

First, make sure that you have visibility into all of your assets (users, apps, and devices).

Start scanning for vulnerabilities regularly.

Monitor more than just unpatched software systems – add scanning across other attack vectors.

Prioritize vulnerabilities based on business risk, taking into account the business impact and context of each asset.

Get a patching strategy in place and patch, patch, patch.

Ready to walk

The next phase of your journey allows you to tighten the reins on your vulnerability management program and enhance your capabilities. This phase is for organizations that are getting to or are already in a “security-mature” state. Your organization has a security budget, you have an army of people using a broad range of security controls. Everything is logged, and in theory, analyzed.

The **Walk** Plan

To truly make your vulnerability management program effective and risk-based, you need to consider the following:

Discover new inventory in real-time and keep your inventory list up-to-date. Deploy continuous, real-time scanning of each asset in your inventory.

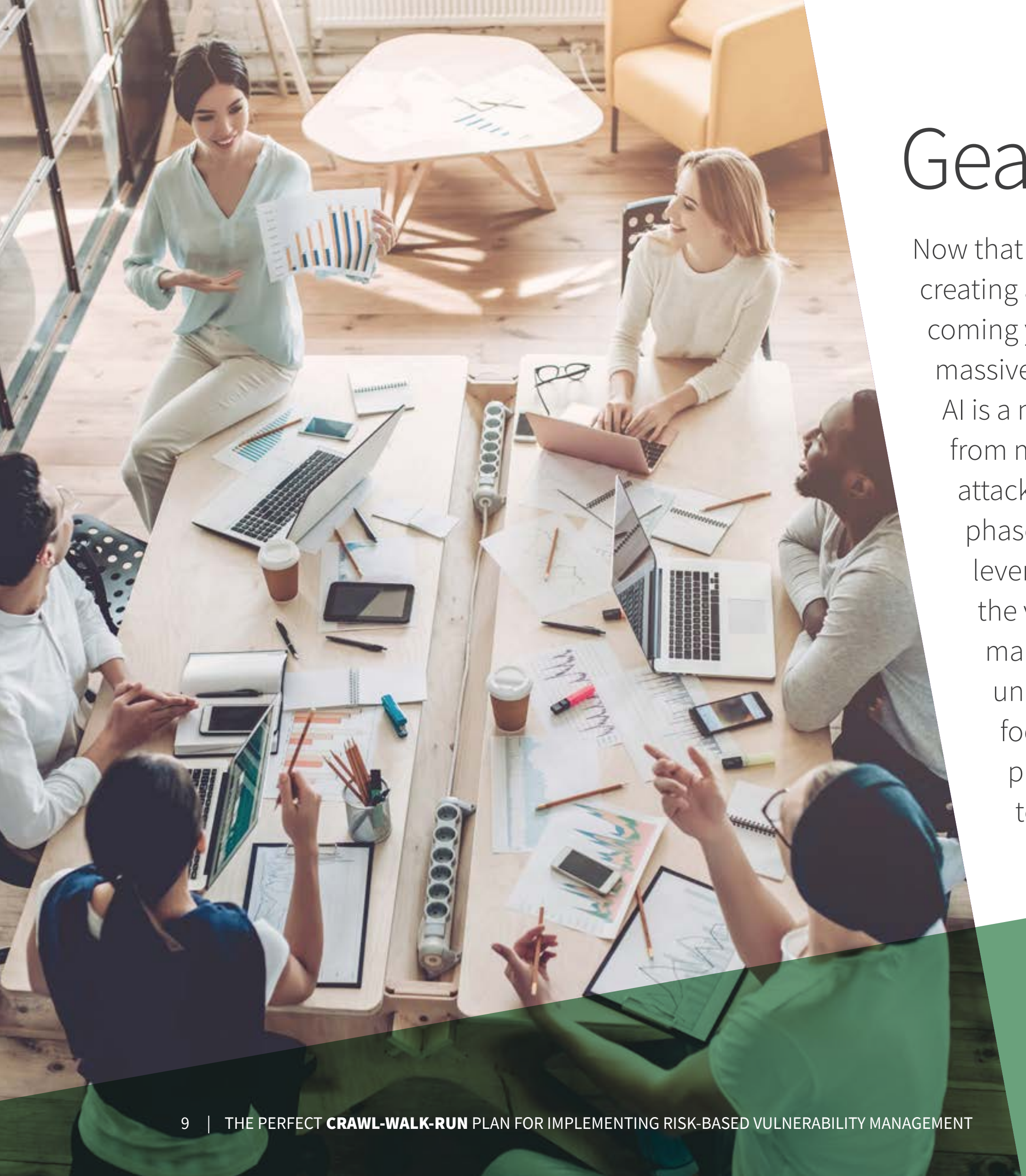
Monitor inventory across broad range of attack vectors, not just unpatched software.

Assess existing mitigation controls and use this information to prioritize vulnerabilities.

Use a layered risk model to understand the actual business risk.

Focus on patching the most critical vulnerabilities using patching guidance and prescriptive fixes.

To properly measure risk, a layered risk model is the best approach that should consider inherent likelihood of breach for each asset, global threats prevalent at the time, and existing mitigating controls deployed in the enterprise to come up with an accurate risk picture.



Geared to run

Now that you can tie vulnerabilities to risk, you are essentially creating a sense of order around the data and observations coming your way. Considering that your attack surface is massive and hyper-dimensional, automation and use of AI is a necessity (as analyzing thousands of observations from monitoring your enterprise assets across potential attack vectors is not a human scale problem). In this phase, machine learning and AI-based technology are leveraged to parse through all the data collected by the vulnerability management system. Vulnerability management is also moved beyond just scanning for unpatched software vulnerabilities, broadening your focus to include other attack vectors such as phishing, malware, DDoS, malvertising, to name just a few.

The **Run** Plan

If you have made it this far, you are ready to reap the complete set of benefits of risk-based vulnerability management. Your risk-based vulnerability management program is running like a well-oiled machine and now you can:

Create your risk-based vulnerability management mandate across all stakeholders and then monitor how it is being followed.

Be proactive and integrate results into your SecOps, AppSec, and other proactive security tools.

Compare your program against peers in your industry to assess how well you are doing.

Track mean-time-to-patch diligently to quantify your enterprise's improvement over time.

Communicate risk reduction and program success to all levels, including board of directors using metrics, charts, trending graphs and quantified business benefits.

In this phase, your focus has shifted to high-level strategy, leadership, actionable metrics, and effective communications. It's important that you champion your program's business benefits and strategic value across the enterprise up to the highest levels. If you have created an effective risk model, you can now prioritize vulnerabilities based on business risk. Machine learning and AI help make the overall process manageable. Security teams can keep up while focusing on mitigating the most significant issues first. In short, you are now in a position to protect your organization from the most urgent threats, proactively avoid breaches, and raise your organization's cyber-resilience and security posture.

Do it **now**.

Get ahead of the game

It is unlikely that the number of attacks will abate over time. On the contrary, there is every reason to expect that their number will continue to grow. In fact, with the growing attack surface and increasing number of potential targets as we constantly increase the connections of various assets to the Internet, breaches are inevitable.

The only way to stop reacting to attackers and get ahead of the game is to be proactive about the security of your IT assets. Investing in emerging technologies that use AI and deep learning algorithms to enable risk-based vulnerability management by monitoring your environment and predicting your breach risk is an effective strategy. With prediction of breaches and insights into potential breach propagations, organizations can move towards a more robust security posture. Then, with a prioritized list of action items and prescriptive fixes for these action items, vulnerabilities can be fixed and closed before they can be exploited.

Balbix BreachControl™, the risk-based vulnerability management platform, enables organizations to transform their security posture and avoid breaches by continuously discovering and monitoring all points in your attack surface, analyzing this information to predict likely breach scenarios, and helping you take appropriate mitigation steps by producing a prioritized list of actions items and prescriptive fixes to address the issues.

Learn more about ***Balbix BreachControl*** now.

Balbix®