EBOOK

brinqa

It’s Time for a New Approach to Vulnerability Management

How to apply a risk-based approach to infrastructure, application and cloud security findings to achieve effective vulnerability management

WHY IS VULNERABILITY MANAGEMENT MORE CRITICAL THAN EVER?

Because the attack surface you need to protect is expanding exponentially. Because digital business is growing nonstop.

No one ever claimed that enterprise vulnerability management was easy. Practitioners know just how challenging it is — particularly as organizations scale — to manage all of the vulnerabilities that exist and develop across an increasingly diverse set of assets. This eBook examines how VM teams should apply a risk-based vulnerability management approach across application, traditional infrastructure, and cloud security to achieve effective risk reduction.

Brinqa hosted a webinar titled Reframing Vulnerability Management: How to Apply a Risk-Based Approach featuring three accomplished security professionals who have experienced the many challenges of leading enterprise vulnerability management teams. Those experts — who all use Brinqa as the foundation for their risk-based vulnerability management program — shared their insights during a wide-ranging discussion about the most challenging aspects of enterprise vulnerability management.

On the webinar panel were Martin Karel, global security vulnerability management product lead at Nestlé, and Steve Hawkins, director of security architecture and engineering at Cambia Health Solutions. Leading the discussion was Ravi Pentapaty, former senior director of security architecture at Warner Bros. Discovery and now cybersecurity evangelist for Brinqa.

This eBook captures and expands on the valuable insights these webinar panelists provided on how to run a successful vulnerability management program, including:

- Why vulnerability management needs to be reframed
- Practical advice on where to start and pitfalls to avoid
- How Brinqa enables security teams to reframe vulnerability management

WHY VULNERABILITY MANAGEMENT NEEDS TO BE REFRAMED

Effectively managing cyber risk as the technological landscape evolves rapidly and digital transformation continues unabated is a daunting responsibility. Many days it can seem impossible.

After all, identifying, measuring and managing an always-growing and changing attack surface is intense work that consumes security teams. And, as if that weren't enough of a burden, to be successful, these teams must convince various internal stakeholders to provide the resources required to actually mitigate vulnerabilities.

Ownership complexity in today's enterprise security landscape has evolved quickly. It wasn't long ago that container security might not have been on the agenda for most VM teams. Same with API security or securing a continuous integration and continuous deployment (CI/CD) pipeline. But as the number and types of security risks VM teams face expand, achieving and maintaining visibility, particularly at large enterprises, is a never-ending process.

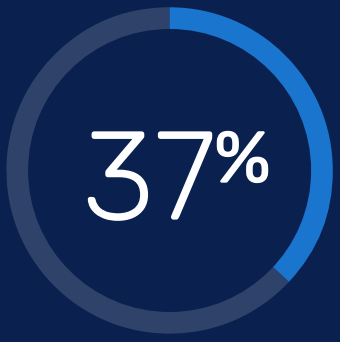
The issue of "who owns what" in the enterprise environment, according to Pentapaty, puts constant pressure on VM teams. "The key challenge in VM is what I call the 'unknown unknowns.' We don't know what we don't know, so there's a constant discovery process as to what's actually in our environments. Then there's the discovery and the security risks that might be associated with those unknowns."

Just a few years ago, for instance, API security tools weren't on the radar of most VM teams, but now practitioners are painfully aware of these and other emerging risks. A new industry segment has quickly appeared related to API security tools. That's just one example, but as each new focus area appears, it requires people, processes and technologies to manage the risk it introduces.

The webinar kicked off with a poll question to an international audience of security professionals:

"What is the biggest challenge you are facing in your VM program?"

The top three responses were:



OWNERSHIP COMPLEXITY

POOR ASSET VISIBILITY

EXPLOSION OF TOOLS & FINDINGS

As organizations continue to deploy intricately interconnected new technologies, risk rises exponentially.

That's the environment in which today's VM practitioners must operate.

Cambia Health Solutions, a multibillion-dollar healthcare company serving the northwestern U.S., has been on a journey to get the foundational components of VM in place, according to Hawkins. "Things like proactive patch management, getting scanning deployed broadly and deeply across our enterprise. And working diligently to develop a solid understanding of the assets involved and their significance to the business," he said.

Ownership complexity, poor asset visibility and the explosion of tools and findings were all cited by webinar attendees, demonstrating how most organizations struggle with all three challenges.

"At Nestlé, we are working to centralize vulnerability management for our global organization," said Karel from the Swiss-based food and beverage giant. "We started this years ago as a part of our security operations center, so all of these challenges resonate with us. I suspect it's the same for all big companies and most likely organizations of many types and sizes."

> We don't know what we don't know, so there's a constant discovery process as to what's actually in our environments."
>
> – Ravi Pentapaty,
> Cybersecurity Evangelist
> Brinqa

SUCCESSFUL VM STARTS WITH VISIBILITY INTO YOUR ASSETS

Poor asset visibility was the second-biggest challenge for webinar attendees. Knowing what assets exist in your organization is the critical first step to reducing risk.

"Without good contextual data, getting the right information to the right people is impossible."

Let's expand on the visibility issue by looking at the bigger picture of organizational environments and how they affect VM success. Every company, from its technology landscape to its cybersecurity risks, is different. The environments of the three panelists — Nestlé, Cambia Health Solutions, and Warner Bros. Discovery — have different types and levels of risk.

Developers and engineers at Warner Bros. Discovery are empowered to create applications that appeal to users and generate a high level of traffic, according to Pentapaty. That requires tens of thousands of workstations and thousands of cloud accounts, virtual machines, container workloads, web applications, and the like. Deploying that much technology makes visibility more challenging.

The story is similar at Nestle, which has a few hundred thousand workstations, tens of thousands of servers, and hundreds of factories with all possible types of devices, according to Karel.

He said the move to the cloud means the company has to have visibility into all possible cloud models with all cloud vendors, along with thousands of websites supporting the company's many global brands.

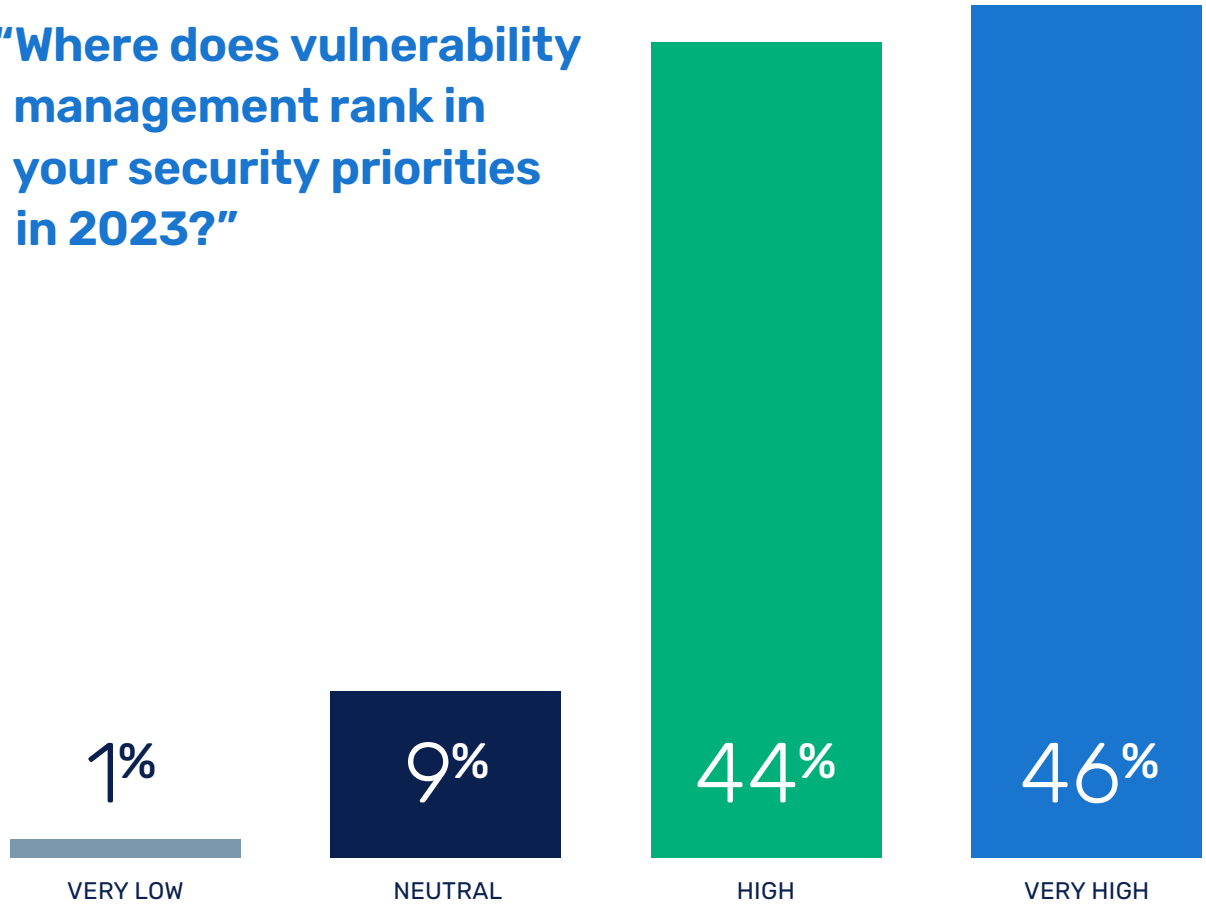
Cambia Health Solutions is smaller than the first two companies, but with thousands of endpoints and servers, it certainly has its challenges ensuring visibility. "We're hybrid like most companies. We have our own data center and cloud operations. Whether it's AWS, EC2, containerized workloads, or serverless functions such as AWS Lambda or Google Cloud, flaws can exist everywhere. Like traditional computers, those platforms can have unsupported run times or out-of-date libraries. So you must ensure you have good contextual data on all of them."

Despite the differences in the industries and sizes of the panelists' businesses, there are many common lessons that VM professionals working at any organization can recognize and learn from. The challenges apply to startups with 10 or 20 employees to giant corporations with thousands of people and massive infrastructures.

THE VITAL ROLE OF VULNERABILITY MANAGEMENT

The growing importance of vulnerability management reflects organizations' need to address all the weak spots in their attack surfaces. That's true of organizations of all types and sizes, but especially enterprises with significant asset inventories.

"Where does vulnerability management rank in your security priorities in 2023?"



That 90% of respondents said vulnerability management ranks "very high" or "high" among their priorities is unsurprising. Security teams know they have a tremendous amount of work on their plates. The question is, how can they successfully manage this rapidly expanding burden? Let's turn to our panel of experts for insights.

PRACTICAL ADVICE FROM EXPERT PRACTITIONERS

"Being risk-based means we're focusing the time and energy of our vulnerability management team on the areas of our company with the greatest risks," said Pentapaty.

That practical approach means that if you identify a critical vulnerability on a development server behind three firewalls, the organization should focus its resources on higher priorities. "For example, with a risk-based approach, a path reversal vulnerability on an externally facing web server presents a much greater risk to the organization and should be prioritized for response."

At Cambia, the approach to being risk-based began with the goal of becoming good at keeping software up to date. "We met with teams and asked, 'What do you need to be good at this?' And we created the conditions our people needed to become good at dependency management," said Hawkins. "Once you update your dependencies, 90% of the risk is off the table, so you can apply risk-based vulnerability management against the business-critical vulnerabilities that represent the greatest risk to the organization."

For Nestlé, with its large, diverse environment, the vulnerability management team emphasizes achieving maximum visibility on the "right areas" of the organization. "Our priority is to have visibility on the assets that are likely to have the greatest number of vulnerabilities," said Karel. "We have a very strong process around hot or burning vulnerabilities that we understand and those that are exploited in the wild."

"Our trade intelligence team provides constant feeds that inform us about attack vectors and related information."

As these expert insights show, there is no one-size-fits-all approach to risk management. Every organization must dedicate time to focusing on the risks that matter most to the business. That means you need to evaluate your attack surface holistically across security programs.

As Pentapaty put it, "If you're being hit with a number of brute-force and password-spraying attacks and then you suddenly see an uptick in authorization to operate (ATO) attacks, it makes sense to turn up the volume on those areas of your websites. That's why active telemetry is so important for determining what (and where) the greatest risks are at any point in time."

...apply risk-based vulnerability management against the business-critical vulnerabilities that represent the greatest risk to the organization."

– Steve Hawkins,
Director of Security Architecture and Engineering
Cambia Health Solutions

HOW TO BEGIN REFRAMING VULNERABILITY MANAGEMENT

As the Chinese proverb says, "A journey of a thousand miles begins with a single step." That's not a bad way to describe the process of creating and operating an effective vulnerability management program.

"It's all about starting small," said Pentapaty. "Begin where you have IDS and IPS points in place. Then expand and mimic your success elsewhere in the environment. This approach works for a 10-person organization or a multinational with a million employees. Vulnerability management is challenging work that requires significant effort to be successful."

It's essential not to get discouraged when you launch or expand a VM program. "There's no book about how to run this kind of program," said Karel. "If you go to a course or ask business colleagues, they'll say 'scan everything.'"

Fortunately, he had prior experience in this area before he joined Nestlé.

"There were no tools to support such programs. Like many of you, we either had to work with an Excel sheet or build our own tools. Fortunately, I found a company that could support this model — Brinqa. I convinced my management that although the Brinqa approach is different, it will work for us. And it has, quite well."

Speaking of spreadsheets, Hawkins said Cambia hit a wall using the spreadsheet method and urgently needed a more modern approach. When the team managed vulnerabilities in a spreadsheet, as many organizations still do, the file became so large that analysts couldn't open it on their laptops!

"Brinqa enabled us to dig out of that hole," he said. "Now we have a place to do not only our formatted report cards, dashboards, etc., but we also have ad hoc search capability to drill in on things. Brinqa reporting is super fast and unlike anything else we tried before."

NEW APPROACHES TO TRADITIONAL PROBLEMS

The VM team at Nestlé developed a unique program to alert asset owners about vulnerabilities without needing to scan for them. Initially an intensely manual process, the company was able to automate it with Brinqa.

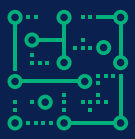
"We collect vulnerability intelligence from various feeds, enrich it with trade intelligence and calculate risk rating based on our own criteria. And then, we bundle vulnerabilities according to patching calendars and automatically create and send tickets to the patching teams.

"Brinqa enables us to do this without scanning or any extra effort. We increased the sophistication of this process over time, assigning the group of devices represented by their scope and so on. Now, as soon as vendors publish the vulnerabilities, our teams start working on patching. They know what their SLAs are because they receive the ratings immediately," he said.

The right technology is essential for your program to adopt a unified cyber risk lifecycle approach to vulnerability management.

Brinqa enables organizations to:

Model your attack surface, creating a single source of truth



Prioritize vulnerabilities with risk scoring and business context

Accelerate and improve the remediation process

Report risk in terms the rest of the business can understand and trust

KEY TAKEAWAYS

There are many facets and perspectives to how organizations of all types and sizes can reframe vulnerability risk management. The goal for every organization is consistent: Effectively address and overcome the many challenges associated with identifying and managing risk across your entire attack surface.

Here are three actions that will help you achieve that goal.

- Perform an inventory of your current security tools to ensure they provide the coverage you need across your entire attack surface.
- Collect the business context you need. Use this questionnaire to calculate your organization's business criticality score. Create your requirements — by following the cyber risk lifecycle — for managing cyber risks across infrastructure, application and cloud security.
- Use a platform like Brinqa to operationalize the cyber risk lifecycle across your business.

Not sure where to start?

Ask yourself these four questions:

1. Which groups will be involved in rolling out vulnerability risk management at all stages — initial rollout, later expansion, etc.?
2. How will you phase the coverage of the attack surface?
3. Where are you feeling the most pain right now when it comes to prioritizing and remediation?
4. How can you identify your best ROI opportunities for improving the operational efficacy of your vulnerability remediation efforts?

Brinqa is the only company that orchestrates the entire cyber risk lifecycle — understanding the attack surface, prioritizing vulnerabilities, automating remediation, and continuously monitoring cyber hygiene — across all security tools and programs. Brinqa Attack Surface Intelligence Platform is the source of truth for cyber risk. It empowers organizations to elevate the security conversation, hold risk owners accountable, identify security control coverage gaps, and manage and track all vulnerabilities in a single platform. Based in Austin, Texas. Brinqa is backed by Insight Partners. Learn more at **www.brinqa.com.**