brinqa

Proactive Security Series

# The 2025 Guide to Risk Operations

# EXECUTIVE SUMMARY

Conventional vulnerability and risk management programs struggle to keep pace with organizational growth and technology changes. They are mired in manual processes and inefficiencies, leading to fragmented visibility across infrastructure, cloud, and application security teams. They are caught in an endless loop of reacting to the next security incident with no end in sight, while the biggest source of security incidents and breaches - exploitable known vulnerabilities - sit unaddressed across the attack surface of an organization. When managed proactively, addressing these vulnerabilities reduces the number of incidents and time wasted reacting to them.

The lack of cross-communication and shared tooling across various security teams, exacerbates this problem, duplicating efforts. It's not that the teams fail to identify vulnerabilities, but manual processes create friction in remediation, leading to an impossible backlog to overcome. Steps from identifying the right owners for remediation to aligning on the urgency impede the process. This misalignment leads to friction and a slowdown in remediation times, hindering the ability to gain business buy-in for necessary security measures.

To meet new SEC mandates on reporting, organizations need to undergo a fundamental shift in their approach to security – they need to take more proactive measures. Against this backdrop, there is a solution, which is to implement a Risk Operations Center (ROC). A ROC isn't a single technology or vendor solution but a holistic way of re-imagining how the business handles vulnerability and cyber risk management. It unifies and streamlines the vulnerability management process, fosters cross-communication, and aligns security initiatives with business objectives. It provides a more precise, comprehensive approach to cyber risk, ensuring that vulnerabilities are efficiently managed and the business impact is clearly communicated to all stakeholders.

This shift is about improving defenses beyond the focus on responding once an exploit has occurred. It is about enhancing the organization's overall risk posture in a way that resonates with security teams and business leaders. By implementing a Risk Operations Center, businesses escape the never-ending loop of crisis-management security, adopting a proactive business-oriented security lifecycle.

# TABLE OF CONTENTS

THE OPPORTUNITY

THE APPROACH

# INTRODUCTION

Businesses today have many tools at their disposal to identify and detect the vulnerabilities that affect their organization. These tools, owned by multiple teams, generate massive volumes of disjointed data and fail to convey the full picture of organizational risk. With cloud adoption and rapid growth, mapping vulnerabilities to the right owners and conveying the urgency of remediation becomes almost impossible with current tools. The tools communicate technical risk well but fail to deliver on the business impact, slowing down remediation efforts.

This dynamic environment demands a strategic, proactive response, particularly in light of recent directives from regulatory bodies like the SEC, which underscore the critical need for robust and responsive security strategies. Cyber risks' ever-growing complexity and scale require a solution transcending manual efforts and traditional practices. It is no longer sufficient to reactively address security incidents as they arise; organizations must anticipate and neutralize threats before they materialize from the exposures that already exist within the organization.

The Risk Operations Center (ROC) approach directly addresses these challenges, helping organizations take control of their vulnerability management holistically. A Risk Operations Center is not a tool or a process; it's a modern methodology encompassing cybersecurity. A ROC aligns proactive security measures with detection and response strategies, typically associated with a Security Operations Center (SOC). In this sense, the ROC can be seen as the proactive counterpart to the SOC, focusing on preventing threats before they materialize, while the SOC handles the detection and response aspects. This relationship between the ROC and SOC is vital to a comprehensive and effective cybersecurity strategy. It transforms the security posture from purely reactive to a combined proactive and reactive approach, moving isolated efforts into an integrated, strategic framework.

This whitepaper guides you through the intricacies of a ROC, illustrating how this innovative approach effectively mitigates risks cost-effectively and operationally efficiently. It explores a ROC's technical foundations and strategic implementations, showcasing its role as an indispensable asset in the modern cybersecurity arsenal.

Section 1

# The Opportunity

# OPERATIONAL CHALLENGES IN VULNERABILITY MANAGEMENT

Vulnerability management is fraught with challenges in aligning assessment results with business priorities. Increased tooling has improved detection, leading to overwhelming volumes of security findings, creating enormous backlogs and slow remediation times due to difficulties prioritizing and responding at scale. This is complicated by exposure assessments inability to accurately categorize severity levels due to a lack of context, creating a misalignment between IT security teams and business units.

## Ineffective Resolution and Prioritization Processes

Tooling has improved detection capabilities, creating a flood of information for security teams to manage and prioritize, leading to an overwhelming backlog. Effectively distinguishing between critical and lower-priority threats takes work, prolonging timeframes for mitigation. These delays are compounded by unclearly mapped ownership and responsibility, dragging out decision-making.

Unfortunately, solving this problem is not as easy as throwing more resources at it. Organizations are already struggling with a scarcity of security professionals and constrained remediation team capacity, making it harder to tackle all the vulnerabilities they face effectively. This scarcity of resources leads to inefficiencies that ripple across various departments, wasting valuable time and effort across the business.

For security teams, especially risk analysts, this translates into an overwhelming workload and the inability to adequately address the most critical threats. Similarly, IT and development teams, the primary owners of remediation tasks, find their allocated time for security bugs consumed by an endless cycle of vulnerabilities, diverting their attention from other business-critical development and IT tasks.

> "Brinqa is at the heart of our Risk Operations Center. We developed and implemented a vulnerability remediation strategy with the insights Brinqa provided, initially focusing on our crown jewels and working our way down the priority list."
>
> **Jim Desmond, CISO, Asurion**

## Misaligned Focus in Vulnerability Assessment

There's an overemphasis on the CVSS score of security findings while neglecting to consider their potential impact on business operations and reputation. This approach prioritizes threats based on their technical aspects rather than their impact on the business. It creates a disconnect between what IT security teams and business units perceive as critical threats. The information in these assessments frequently comes from disjointed sources across various security domains like vulnerability and risk management, application security, and cloud security. This lack of integration results in fragmented visibility and hampers the ability to conduct accurate and comprehensive risk assessments.

Compounding this issue are the siloed nature of security assessments and the absence of a centralized approach. Vulnerability assessments, whether they pertain to infrastructure vulnerabilities, application security, or cloud security, are often conducted in isolation without meaningful consideration of the business impact. This separation leads to a failure in integrating business context, such as the value of affected assets, into risk assessments or the same vulnerability being reported numerous times across different tool sets.

Consequently, there's a lack of understanding among business stakeholders about the implications of cyber risks. This stems from a lack of a centralized system to measure and manage these risks, further exacerbating the problem and preventing the development of a unified view of the organization's security posture. This disjointed approach highlights the critical need for a more integrated, business-aligned strategy in vulnerability assessments and cyber risk management.

## Misaligned Focus in Vulnerability Assessment

There's an overemphasis on the CVSS score of security findings while neglecting to consider their potential impact on business operations and reputation. This approach prioritizes threats based on their technical aspects rather than their impact on the business. It creates a disconnect between what IT security teams and business units perceive as critical threats. The information in these assessments frequently comes from disjointed sources across various security domains like vulnerability and risk management, application security, and cloud security. This lack of integration results in fragmented visibility and hampers the ability to conduct accurate and comprehensive risk assessments.

Compounding this issue are the siloed nature of security assessments and the absence of a centralized approach. Vulnerability assessments, whether they pertain to infrastructure vulnerabilities, application security, or cloud security, are often conducted in isolation without meaningful consideration of the business impact. This separation leads to a failure in integrating business context, such as the value of affected assets, into risk assessments or the same vulnerability being reported numerous times across different tool sets.

Consequently, there's a lack of understanding among business stakeholders about the implications of cyber risks. This stems from a lack of a centralized system to measure and manage these risks, further exacerbating the problem and preventing the development of a unified view of the organization's security posture. This disjointed approach highlights the critical need for a more integrated, business-aligned strategy in vulnerability assessments and cyber risk management.

## Misaligned Focus in Vulnerability Assessment

There's an overemphasis on the CVSS score of security findings while neglecting to consider their potential impact on business operations and reputation. This approach prioritizes threats based on their technical aspects rather than their impact on the business. It creates a disconnect between what IT security teams and business units perceive as critical threats. The information in these assessments frequently comes from disjointed sources across various security domains like vulnerability and risk management, application security, and cloud security. This lack of integration results in fragmented visibility and hampers the ability to conduct accurate and comprehensive risk assessments.

Compounding this issue are the siloed nature of security assessments and the absence of a centralized approach. Vulnerability assessments, whether they pertain to infrastructure vulnerabilities, application security, or cloud security, are often conducted in isolation without meaningful consideration of the business impact. This separation leads to a failure in integrating business context, such as the value of affected assets, into risk assessments or the same vulnerability being reported numerous times across different tool sets.

Consequently, there's a lack of understanding among business stakeholders about the implications of cyber risks. This stems from a lack of a centralized system to measure and manage these risks, further exacerbating the problem and preventing the development of a unified view of the organization's security posture. This disjointed approach highlights the critical need for a more integrated, business-aligned strategy in vulnerability assessments and cyber risk management.

# OPPORTUNITY: CROSS-DEPARTMENTAL SECURITY COLLABORATION

No matter how good the visibility is into identified vulnerabilities and findings, the problems can never be efficiently resolved when security teams struggle to identify task owners and explain to them the risk. Teams waste time on 'administrative detective work,' expending time and resources to determine whom to prioritize ticket remediation to, slowing down the workflows and creating bottlenecks that hinder the overall effectiveness of the security operations.

## Lack of Broad Business Engagement

Unclear delineation of responsibilities leads to confusion within teams about their specific security roles, adversely affecting operational efficiency and the overall effectiveness of security measures. This results in fragmented vulnerability management and delayed threat response as coordination between departments breaks down.

Security problems are handled with a 'firefighting mentality,' where teams are primarily reactive, focusing on addressing major, critical issues as they arise with enthusiasm and urgency. While this approach can demonstrate immediate effectiveness, it's neither a sustainable nor effective long-term strategy, leading to burnout and an endless cycle of fires to manage. The only way to effectively end it is to integrate proactive security work, such as preemptively addressing pre-attack threat exposures. It is challenging as the firefighting mentality trains teams to see security as a diversion rather than a part of their responsibilities. Overcoming this mindset requires defining security in a way that makes sense to the business unit, showing risks in business terms, and fostering an organizational culture that understands the value of investing time in proactive security measures.

> "At Nestlé 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."
>
> **Martin Karel, Leader Nestle' Cyber Security Operations Center (CSOC)**

## Limited Engagement with Senior Leadership

The journey to embedding security into an organization's culture relies heavily on strategic direction and support from senior leadership. The challenge lies in effectively engaging these leaders in meaningful discussions about exposure management due to a significant misalignment between the security team's technical understanding and senior leadership's business-centric perspective.

The technical teams, proficient in their domain, struggle to articulate the business implications of cybersecurity threats in a way that resonates with executive decision-makers. They have the tools to provide visibility into vulnerabilities but fail to see the overall business impact, inhibiting their communication ability.

Senior leadership focuses on tangible returns and strategic investments and does not fully grasp the value and necessity of these initiatives without a clear and compelling presentation of their return on investment (ROI).

Security teams have the challenge of communicating the business impact of security issues while emphasizing the potential threats and opportunities that effective cybersecurity measures bring to the business. Security teams find it difficult to translate complex technical issues into terms that clearly convey the potential business impact, such as revenue loss, reputation damage, or regulatory non-compliance. Failing to do this results in misaligned cybersecurity strategies and inadequate support for these initiatives.

# TRANSLATING TECHNICAL RISKS INTO BUSINESS TERMS

Many inefficiencies in addressing potential risks stem from how the information is conveyed. These problems arise from the security teams' understanding and translation of the business context so that other teams can see the value and act on it. Without bridging this communications gap, security teams become additional noise and a burden rather than a vital part of the solution. Yet, they still take the blame when exposures are not addressed, resulting in a breach or impact on the business.

## Difficulty in Validating Threat Exposures

Proving that a threat exposure has merit and needs remediation requires validation. Security teams have long been able to prove that an exposure exists, but they struggle with demonstrating relevance from a business perspective. This difficulty is compounded by the sheer volume of security data and alerts, which is already daunting and overwhelming. As a result, there is an inefficiency in the analysis phase due to the massive scale of data, leading to slower response times in addressing these issues.

This situation is exacerbated when security teams are inundated with new findings, making prioritizing and responding effectively challenging. Businesses dealing with a high incidence of low-value "emergencies" strain their resources and divert attention from more significant areas of exposure. This misdirection is primarily due to a lack of understanding of the actual business impact of each threat exposure. As a result, significant amounts of time and resources are wasted on vulnerabilities rated as critical in terms of CVSS but have minimal impact on the business. This approach relies solely on scoring vulnerabilities and leads to 'alert fatigue' among security and remediation teams. They become desensitized to alerts and can't precisely identify which risks require immediate attention.

> "We more than doubled our infosec team productivity with Brinqa and risk operations. It streamlined vulnerability management, automating workflows and consolidating insights, so we can stay ahead of risks and easily meet audit requirements."
>
> **Mohamad Toka, CISO, SAP**

## Inadequate Recognition and Reporting on Risk Reduction Impact

To business teams, scores and technical details come off as jargon, detached from the actual business risks they face. Without translating technical risks into business-relevant metrics and Key Performance Indicators (KPIs), the actual cost and impact of security threats on the business remain obscured, leading to a lack of understanding and urgency in addressing these risks.

Barriers to communication between technical security teams and non-technical stakeholders are the problem. Reports and documentation that are heavily technical fail to resonate with business-focused audiences. This disconnect leads to the security team's warnings being ignored, akin to the boy who cried wolf – raising alarms that are not understood or seen as relevant by the wider organization, and as a result, remediation is not made a priority.

Security teams often encounter a communication challenge: they alert business teams to cyber threats, but these warnings can seem irrelevant without proper context. It's like saying, "A storm is approaching," without explaining the potential impact or severity of the storm. Without understanding the relevance, business teams may disregard the alerts, leading to the significant issue of these warnings being ignored. The communication of threats must be clear, relatable, and directly tied to the business impact, ensuring that the message reaches the intended audience and prompts timely and appropriate action.

Section 2

# The Approach

“We needed to apply risk-based vulnerability management against business-critical vulnerabilities. Brinqa enabled us to dig out of a hole. 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.”

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

# TAKE A BETTER PATH

There is a clear path forward for vulnerability management that deviates from old, fragmented methods. This new approach involves shifting to a comprehensive, continuous, collaborative strategy to deliver tangible business value. This approach is encapsulated in the Risk Operations Center (ROC), which is a framework enabling organizations to manage their vulnerabilities and threat exposures more effectively by integrating various security aspects into a unified system. It's not just about handling exposures pre-attack but also holistically understanding and managing the organization's risk profile. Notably, a ROC helps businesses meet new regulatory mandates, like those from the SEC, by providing a clearer understanding of their risk landscape.

## Evolving Your Approach

Security capabilities that merely detect and score vulnerabilities based on tools fail to reflect the true priorities of a business. This is where the Risk Operations Center becomes pivotal. A ROC begins with creating a unified inventory of all vulnerabilities and their related assets, integrating business context to understand the relationships and ownership of these assets. This approach ensures that the inventory is organized and tailored to reflect the specific needs and context of the business.

The essence of a ROC's efficiency lies in its risk prioritization process. A prioritized list of exposures across all security disciplines is generated by automated risk scoring that factors in vulnerabilities, business context, and threat intelligence. This process represents a significant evolution from traditional methods by consistently applying risk-based scores and standardizing prioritization across the entire attack surface. It effectively bridges the gap created by different tools that may prioritize vulnerabilities in disparate ways, akin to translating between metric and imperial systems without a conversion. By integrating these diverse prioritization methods at scale, a ROC provides a comprehensive and coherent framework for addressing the most critical risks first, aligning security efforts with the strategic needs of the business.

## Context is Key

Context plays a crucial role in transforming security detection data into actionable insights for a ROC. This process must be reliable, with a continuous flow that pulls quality data to suit your organization's needs. With this data, dynamic prioritization mechanisms are employed to assess the threat landscape more precisely. By correlating vulnerabilities with business-specific factors, the ROC enables the development of risk management strategies that are both precise and relevant to the business.

Prioritizing threats and vulnerabilities is heavily based on their impact on the business, ensuring that those posing the most significant risks to business operations are addressed first. This prioritization process is enhanced by centralizing all contextual information in one location, essential for avoiding repeating the same work across different teams and systems.

> This centralization simplifies and streamlines the risk management process, making it more efficient.

Quality and reliable integrations to a broad set of data sources are essential in this context; they must consistently provide the necessary data in the format required for effective analysis. This approach ensures that the ROC's risk assessment and prioritization are grounded in a comprehensive understanding of the business's unique environment and needs, enabling more strategic and impactful decision-making.

## Central Management

Implementing a Risk Operations Center (ROC) centralizes the management of vulnerabilities and security policies, effectively integrating data from diverse sources to streamline pre-attack cyber risk operations. By offering a comprehensive overview of the entire business, ROC targets the most pressing threats for preemptive remediation and shifts the focus from purely technical details to more business-centric risk narratives. This shift enhances understanding and accountability across different organizational departments, reducing wasted time and duplication of effort, which enables teams to dedicate more time to proactive security work.

## Identification is the First Step of the Lifecycle

Continuous monitoring is critical in the lifecycle of exposure identification within a Risk Operations Center. This process involves constantly scanning and identifying new threats and vulnerabilities as they emerge rather than solely depending on periodic assessments. Organizations must initially manage continuous and periodic scans at scale to effectively transition to a lifecycle process. This can be accomplished using a central hub consolidating the latest exposure information for a comprehensive view of the cybersecurity landscape.

Leveraging the ROC approach enables organizations to proactively identify and address consequential risks, implementing preventative measures for timely vulnerability mitigation. This proactive stance provides a centralized approach to cyber risk management, effectively overcoming the formation of data silos and promoting more effective risk mitigation strategies.

## Business Integration

Integrating cybersecurity into business operations is a crucial aspect of a Risk Operations Center (ROC), which translates technical risks into business terms, fostering a collective understanding and response to cyber threats. By embedding cybersecurity within the broader risk management strategy, ROC ensures that cyber risks are considered alongside other business priorities.

Unlike traditional practices where a given vulnerability is listed along with its respective CVSS score, a ROC contextualizes them. The vulnerabilities are no longer in just technical terms; they are grouped in business terms such as “revenue-driving, web-facing applications,” “applications with sensitive data,” or “all internet-facing assets.” When business units see prioritized findings in “revenue-driving, web-facing applications,” the impact is clear and aligns with the organization’s objectives. This integration is crucial for aligning cybersecurity efforts with the organization’s risk profile and strategic goals.

The other aspect of business integration is the addition of automation to streamline the response process, reducing the time it takes to mitigate threats. Effective automation works across teams, from the point of detection through the owner’s remediation. The goal is to reduce the time from detection to response, improving overall remediation speed.

# HOW TO GET STARTED

Establishing a Risk Operations Center goes beyond compliance with SEC mandates; it's a response to multiple catalysts, including the realization that ineffective communication and manual processes are no longer sustainable.

As CISOs feel the pressure of accountability, there's a growing recognition of the need to shift from the status quo to a more effective vulnerability management strategy. This shift starts with honestly assessing your organization's cybersecurity position and acknowledging that it's time for a change. Once the decision for change is made, it's about methodically progressing from where you are to a more advanced, proactive state of managing exposures and vulnerabilities.

## Building Support

A Chief Information Security Officer (CISO) is an essential advocate in building a ROC, as the process is most effective when driven from the top down. The CISO plays a pivotal role in unifying efforts across the organization, acting as the voice of security with a business vision.

The process can start by strategically using the vulnerability management team, which already falls under the CISO's purview. Given its close alignment with the role's responsibilities, this team is ideally positioned to spearhead the ROC initiative. This team can act as a catalyst for the ROC's implementation, leveraging its vulnerability management expertise to drive the organization toward a more proactive security posture that encourages the business to listen and act on security guidance.

As the ROC grows, it can expand to encompass the three key pillars of infrastructure, cloud, and application security. By harmonizing these areas, the foundation for a successful ROC is laid.

Leading and visionary vulnerability management teams have already adopted this approach to transform traditional practices. An example is Asurion, a noted technology insurance provider that successfully implemented a Risk Operations Center to escape the conventional hamster wheel of vulnerability management. Their experience illustrates the transformative impact of a ROC in streamlining and enhancing cybersecurity efforts within an organization.

## Moving on from Manual

Organizations move too fast, and the stakes are too high for the “find problems and point fingers” method. These reactive, manual vulnerability processes are slow and rely too heavily on headcount to be effective. In the current economy, the fact is that headcount is not rapidly rising, so manual processes will leave your organization falling behind.

Using a ROC, organizations adopt a strategic, risk-based security program. This more intelligent and more efficient process helps leverage existing staff, getting the most security improvements for the least effort. The ROC helps organizations see beyond the unrealistic goal of eliminating all vulnerabilities and instead mitigate what delivers the most significant value and improvement to the organization’s risk posture.

## Making Program-Level Improvements

Implementing the first steps towards a proactive security program involves adopting the cyber risk lifecycle and prioritizing risks, which begins with building a unified vulnerability and asset inventory. It’s crucial to start with what’s manageable, understanding that “unified” should be constrained by scope and resources, especially at the start. Over time, the scope can be expanded to include automated remediation, ticketing, and validation processes.

Beginning with a few data sources integrated into one view is a significant step forward, contributing to better security than before. Pursuing perfection with the ultimate goal of comprehensive integration should not impede progress. The process should gradually focus on adding more data sources over time until the goal is achieved.

Alternatively, organizations might start with one security program, such as Traditional Vulnerability Management (i.e., Infrastructure Security) or Application Security. It can be as simple as focusing on a particular program or a key data source, such as creating better processes around just Qualys findings or just Checkmarx findings. The improvements can encompass prioritization to remediation through reporting, with each step driving the organization toward a more meaningful and proactive security posture.

## Running a ROC

Running a Risk Operations Center represents a significant evolution in the Vulnerability Management discipline, combining operational rigor with a risk-based management approach. This transition signifies a shift towards a proactive security strategy that covers the entire attack surface and incorporates business-level risk communication.

# TECHNOLOGY SUPPORTS A RISK OPERATIONS CENTER

Building a Risk Operations Center is a pivotal decision for organizations aiming to enhance their cybersecurity posture and a key part of the process is using technology to support your required scale and complexity.

You can build your own custom developed solution, but the complexities of doing so should not be underestimated. It entails integrating dozens of vulnerability data sources, managing hundreds of millions of findings, pulling in various streams of business and threat intelligence data, and ensuring seamless collaboration with remediation teams.

Given the sheer scale of the challenge, it's become clear that spreadsheets and manual approaches don't work. So the question arises: should an organization build this capability in-house or collaborate with a seasoned expert? Nestle faced this crossroads and opted not to build such an extensive system alone. Instead, they sought a trusted SaaS platform, choosing Brinqa for its proven track record across Fortune 1000 companies. Partnering with Brinqa provides the necessary technology and support needed to build a Risk Operations Center.

> "We've built a Risk Operations Center that brings vulnerability debt back to zero as new technologies or applications roll out. With Brinqa, we've created a model for risk and vulnerabilities — well beyond what scanners tell us."
>
> **Jim Desmond, CISO, Asurion**

## Build Your ROC on Brinqa's Unified Exposure Management Platform

Brinqa connects your IT assets and exposures with business risk at enterprise scale—helping you reveal and reduce cyber risks that truly impact your business.  Brinqa's SaaS platform adapts easily to your business's unique needs and processes, bringing together data from your existing detection tools, normalizing it, and enriching it with the business and threat context you need to prioritize and enforce remediation.

Only Brinqa transforms painful, outdated vulnerability management approaches, enabling you to cut through endless backlogs, fill visibility gaps, and eliminate operational chaos to triple your vulnerability team's productivity and reclaim up to 50% of IT and development time from unnecessary patches. All while speeding MTTR to patch vulnerabilities before they can be exploited.

**Here's how:** The Brinqa Unified Exposure Management Platform integrates seamlessly with hundreds of popular detection tools, bringing all your scan data into one place—aggregated, normalized, and correlated. From there, our SaaS platform calibrates potential issues by adjusting risk scores to reflect the unique blend of business and technical risk for each asset and exposure. Brinqa has been used for years in the world's largest and most complex environments including Walmart, SAP, Deutsche Bank, Adidas, Nestle and many others.

Connect the dots between technology risk and business risk with Brinqa.
Learn more at www.brinqa.com.

brinqa

Brinqa is trusted by the world's leading brands, including Adidas, Nestle and Rolls Royce, and has been recognized as a leading vendor by Gartner, Forrester, IDC, GigaOm and G2. Based in Austin, Texas, Brinqa is backed by Insight Partners.  Learn more at **www.brinqa.com.**