CYBER RISK QUANTIFICATION

—

Automatically quantify your cyber risk with Balbix: Communicate cyber exposure in money terms, justify security investments, and drive corrective action

Balbix®

Balbix

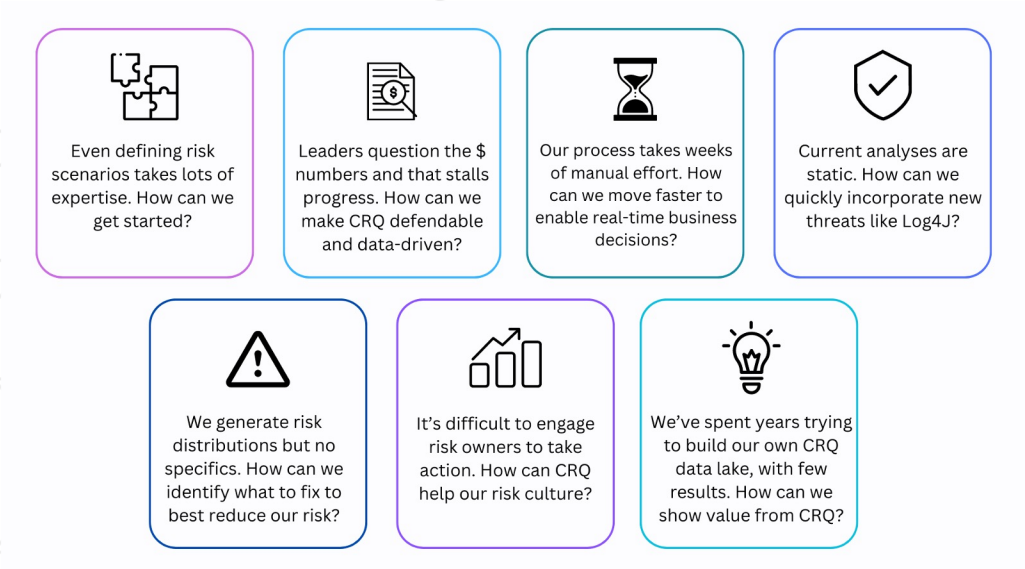
SOLUTION BRIEF

AUTOMATE YOUR CYBERSECURITY RISK THROUGH QUANTIFICATION

Cybersecurity and business leaders are recognizing the need to analyze, manage and communicate cyber risk in the same way as any other risk to the business, in quantified money terms. The goals are clear, and increasingly urgent:

Effectively communicate to risk owners, C-level execs and the Board	Enable key decisions around cyber plans and investments
Manage cybersecurity aligned with corporate risk practices	Make better business trade-offs, e.g., cyber insurance strategy
Keep up with increasing regulatory reporting requirements	Ensure regulatory and policy compliance
More accurately prioritize cyber risks based on impact to the business	Maximize ROI from cybersecurity programs and investments

Cybersecurity and risk teams have traditionally faced many challenges when pursuing Cyber Risk Quantification (CRQ). We hear about the following challenges regularly from enterprises of all sizes:

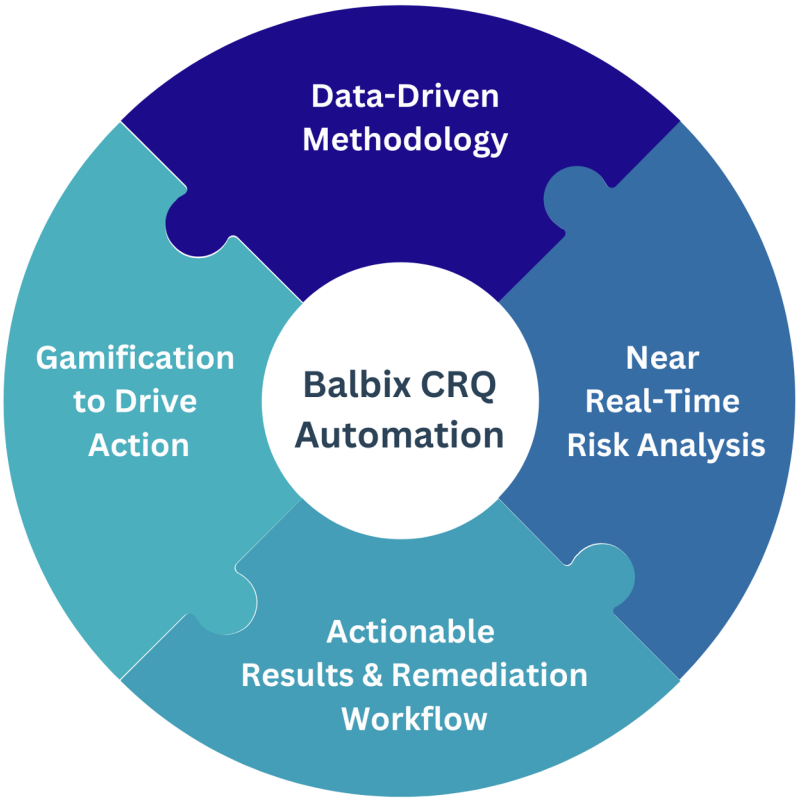


Fortunately, there is a better way forward. We have designed Balbix Cyber Risk Quantification (CRQ) to help you specifically overcome these challenges and drive the impactful business outcomes you need.

The Balbix CRQ Automation Playbook

Say goodbye to painfully manual, subjective, non-actionable cyber risk analysis. Balbix helps customers quantify their cyber risk with a continuously automated, data-driven approach enabling clear communication, defensible analysis, and specific actions to dramatically lower cyber risk. The Balbix Security Cloud platform enables a maximally automated, continuous, and high-velocity quantification of cyber risk across your entire organization to rapidly address your most critical risk scenarios.

Let's take a closer look at the four components* of the Balbix CRQ Automation playbook:

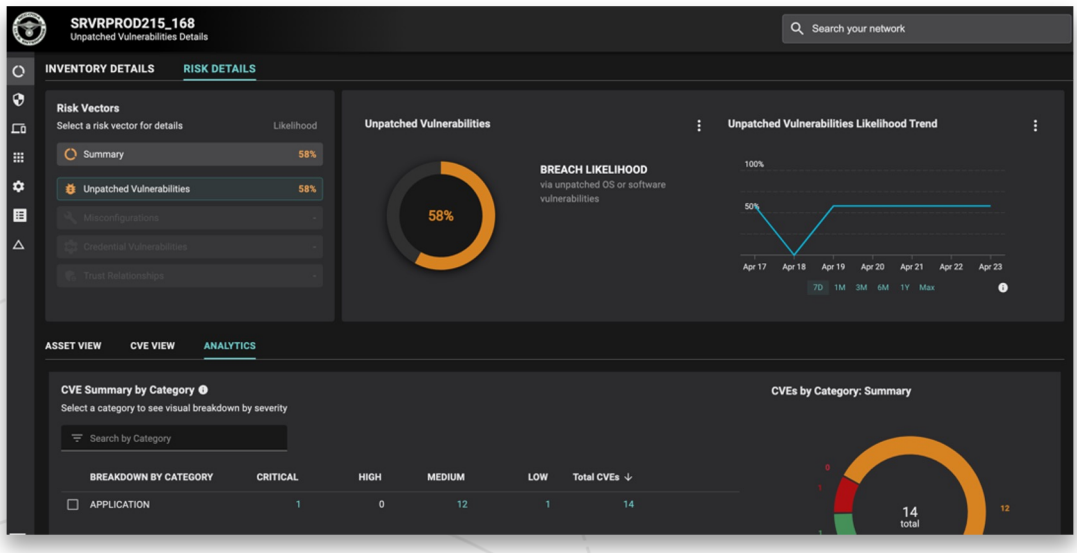


*These components are aligned with Gartner's essential elements for driving action from CRQ efforts: "Drive Business Action with Cyber Risk Quantification", Published, 21 March 2022

1 Data-Driven Methodology

Bottoms-Up Risk Model

The Balbix risk model is fundamentally different from traditional CRQ due to our data-driven and bottoms-up approach to cyber risk quantification. Balbix calculates cyber risk based on the expected financial loss resulting from a breach event by considering the likelihood and impact of the breach, down to the level of each individual asset.

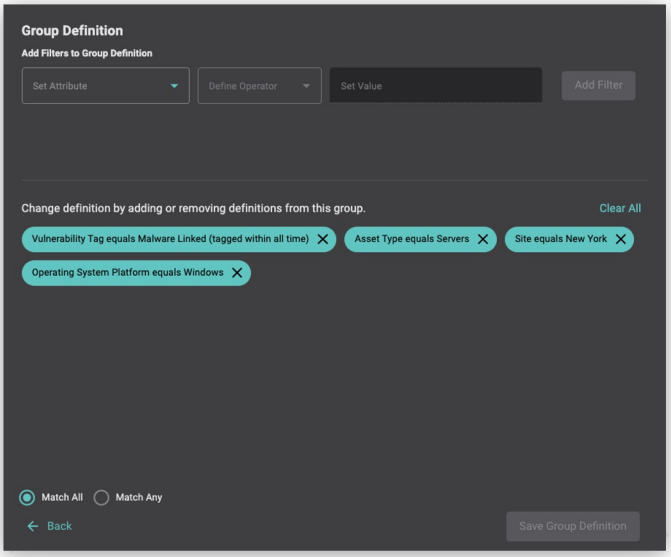


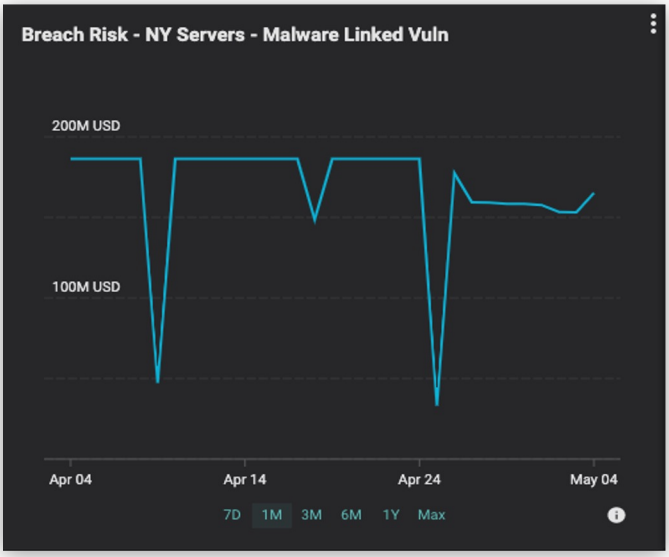
Unlike other CRQ solutions that require manual and subjective tops-down input to populate the risk model for each individual scenario, Balbix uses machine-learning techniques and automation to continually update a bottoms-up, enterprise-wide breach risk model using asset-level data already available in the environment. For customers, this means that not only can risk analysis be performed continuously in near real-time across a wide range of risk scenarios, but also that the resulting analysis is inspectable, defendable and actionable, with clear linkage to source data.

Instant Scenario Scoping via Search and Dynamic Groups

For cyber risk analysis to be useful in practice, it needs to be directed towards a specific scenario that enables decisions to be made, trade-offs to be judged, or corrective actions to be taken. For example, “Assess the malware-related risk associated with all Windows servers located in New York and identify their breach risk in monetary terms over time.” In traditional approaches to CRQ, once cyber risk specialists define such a scenario, they then face a painfully manual effort to collect and scrub the relevant inputs.

With Balbix, the system helps you automate the process of scenario scoping via search and dynamic groups. This example scenario can be easily constructed in minutes using Balbix's intuitive natural language and filtered search to define appropriate dynamic asset groups. Balbix users can define custom asset groups based on a wide range of asset, vulnerability, business, and user attributes that match the desired risk scenario in scope and update dynamically as the environment evolves. These groups enable users to not only report on risk metrics based on the most current data, but also to automatically trend and track this data over time.





Automated Risk Aggregation

When your cyber risk analysis covers a range of scenarios and perhaps multiple apps, segments of the environment, or even the entire organization, it is critical that the outputs roll up appropriately - without double counting or inaccurately inflating numbers. This traditionally requires painstaking validation to ensure that the scenario scoping, financial loss estimates and risk outputs "hang together" in a complementary way, without overlaps.

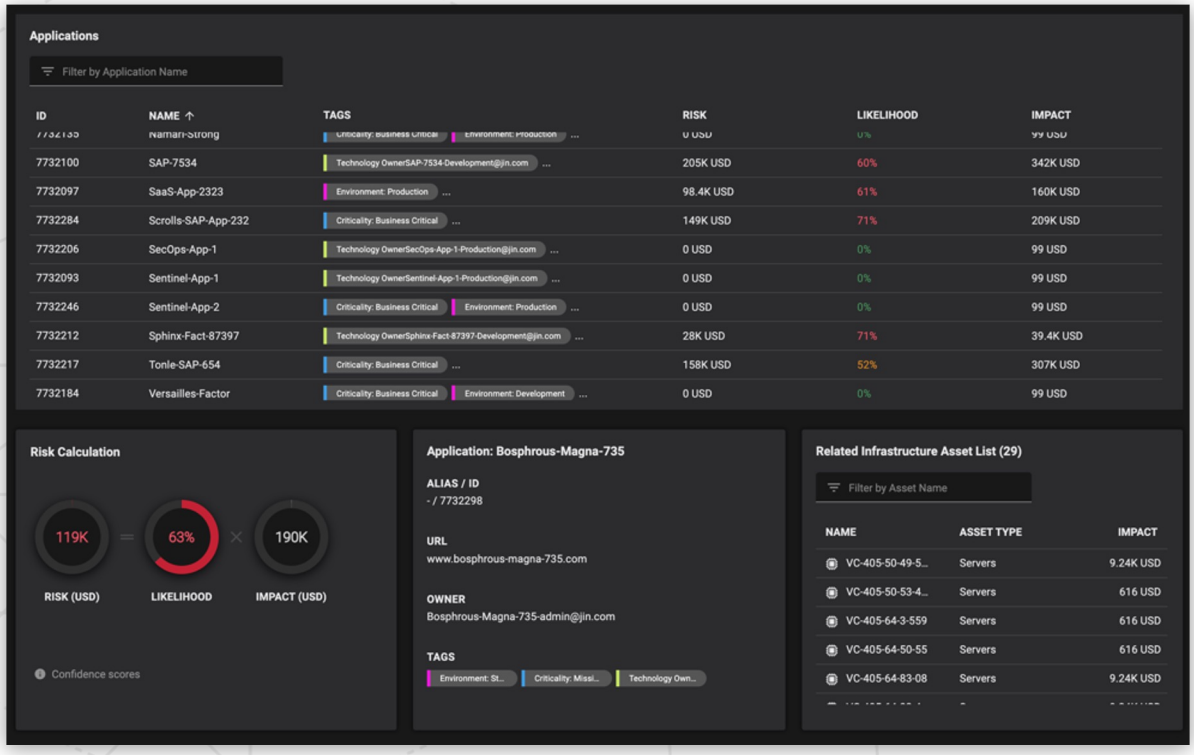
Balbix takes the stress out of this process with automated risk aggregation. The Balbix risk model natively computes breach impact, likelihood and risk at the individual asset level, which is automatically combined within groups of assets and the overall environment to avoid double-counting. By constructing appropriate dynamic groups and sub-groups, analysts can be confident that their analyses are comprehensive and cleanly defined. Balbix automatically performs the heavy lifting of first figuring out which assets belong to which group, and then doing the relevant group-by-group calculations.

Application-level CRQ for Maximum Business Context

Applications are the lifeblood of most modern enterprises, powering revenue generation, business operations, administration, and essentially the entire enterprise – as well a natural vantage point for quantifying risk. Your leaders understand the key apps that run the business and need visibility into cyber risk at this level to appropriately balance investments. Typical trade offs involve time to market, compliance, and security concerns.

However, it can be difficult to quantify risk associated with applications. For example: What is our overall app inventory? What are the vulnerabilities associated with each specific app? What infrastructure does it run on and what risk does that infrastructure bring to the app? What risk do employees bring to the app via day-to-day usage and administration and management of the underlying infrastructure?

Here, most CRQ efforts struggle without the ability to connect these dots and incorporate into the risk assessment in a scalable way. Balbix provides businesses with a unified view of the inventory, vulnerabilities, and risk associated with each application – enabling security leaders to easily investigate, prioritize, and remediate risks based on a comprehensive and accurate view of business risk.



Balbix brings native support for business applications to the bottoms-up CRQ model – providing crucial visibility and accuracy to the risk analysis. By building a unified application inventory, and unifying vulnerabilities and risk across apps and underlying infrastructure, the Balbix application-level CRQ maximizes business context and relevance.

Balbix

2 Near Real-Time Risk Analysis

Comprehensive 5-Pronged Risk Equation

Traditional CRQ methods typically use a simplistic, tops-down, aggregate risk calculation leveraging subjective inputs - resulting in lack of confidence, trust, and usefulness of the analysis across stakeholders.

Balbix computes breach risk on a continuous, near real-time basis across all assets within the environment through the following comprehensive, 5-pronged risk equation:

Impact = g (Business Criticality)

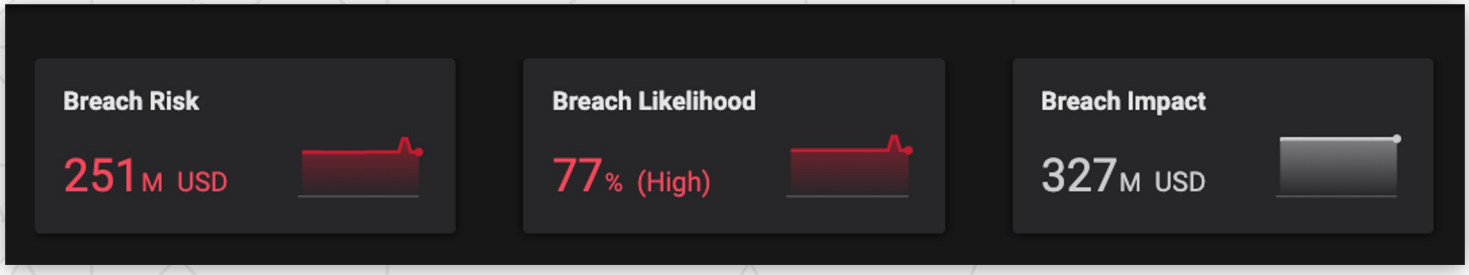
Risk = Likelihood X Impact

Likelihood = f (Vulnerabilities, Threats, Exposure, Security Controls)

Within Balbix, the breach risk calculation considers five critical factors. The first four factors are used to calculate breach likelihood: vulnerability severity, threat level, asset exposure to detected vulnerabilities, and the risk-mitigating effect of security controls. The fifth factor, business criticality, is used to calculate breach impact.

Individual assets are continuously monitored for their exposure to the most frequently exploited risk vectors – software vulnerabilities, misconfigurations, credential vulnerabilities and trust relationships. Breach likelihood is computed for each asset across each risk vector, and then combined to determine a total risk value per asset, with a confidence score.

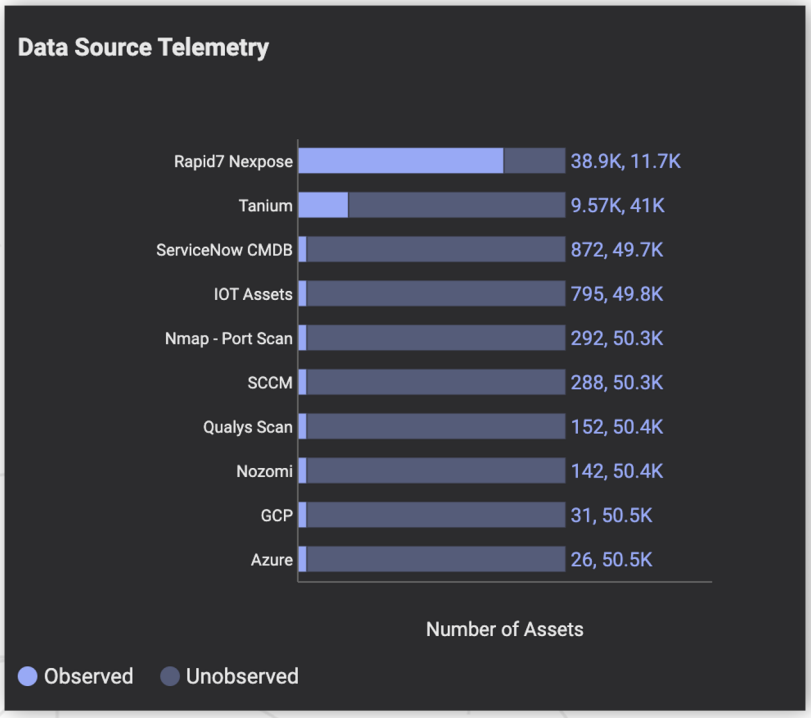
The result? A highly granular and accurate assessment that incorporates the critical underlying drivers of risk within your environment, while also inspectable and understandable to enable maximum confidence in the results and recommended actions.



Telemetry-Driven Data Model

Generating solid data for a CRQ effort can seem daunting. Most existing approaches require high-level subjective inputs that rarely exist across the enterprise. Thoughtful practitioners recognize the need for data-driven analysis, but struggle to marshal the siloed and complex data resources available.

Unlike other risk models, such as most implementations of FAIR, which rely on aggregate Monte Carlo simulations based on “guesstimated” probability distributions of subjective manual inputs, Balbix leverages a granular, bottoms-up, data-driven model for fact-based analysis. Balbix ingests telemetry data from existing sources in your own environment to continuously update a unified cyber risk model.



The foundation is a unified, accurate, de-duped, auto-categorized asset inventory and software bill of materials (SBOM) that Balbix builds by automatically consolidating and normalizing data from your CMDB, GRC, Endpoint, Networking, Cloud, IoT/OT, Vulnerability Assessment, or similar tools or sensors. Balbix then builds a unified view of all vulnerabilities, either ingested from scanning tools or inferred natively - leveraging dozens of vulnerability parsers scanning commercial, government, open source and vendor sources. External global threat intelligence is pre-integrated and automatically correlated against vulnerabilities within minutes or hours of detection. Controls are recognized as deployed on individual assets or ingested from configuration compliance sources.

The result is a fully telemetry-driven data model that makes maximum use of existing enterprise sources and automation, while doing away with the manual effort traditionally needed to build, maintain, and update CRQ analysis. Maximum ease of use and scalability, minimum hassle.

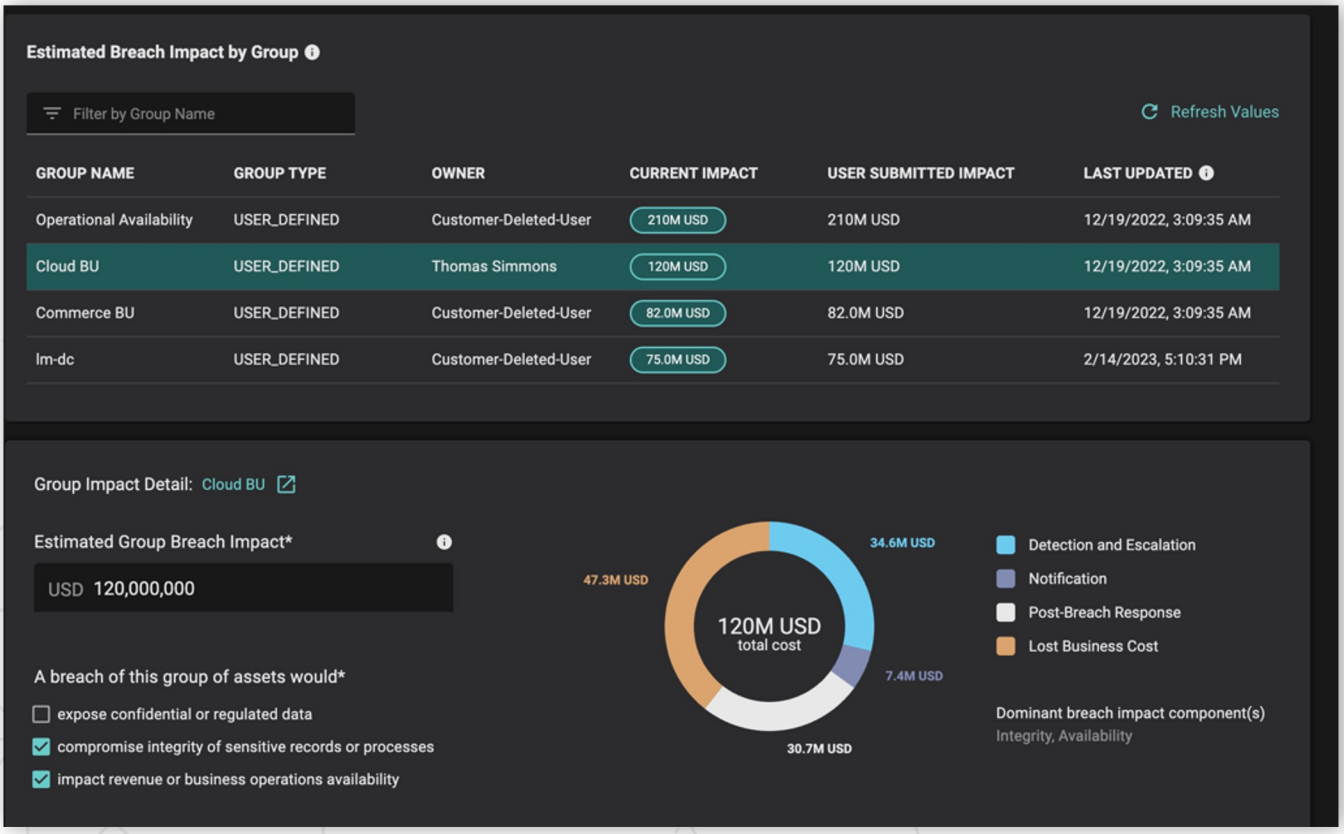
Balbix

Easy-to-Use $ Breach Impact Guidance

Loss estimates are historically one of the most challenging components of a CRQ model. Often with limited relevant monetary loss data at their fingertips, analysts are left to use gut feel, or bring in expensive consultants to attempt the same.

Balbix automation makes loss estimates a snap.

Within the Balbix platform, baseline breach impact for every asset is automatically determined based on asset-level fingerprinting considering attributes such as type, usage, users, and location within the environment.



Balbix then provides a monetary loss guidance model pre-tuned based on analysis of thousands of global breaches, requiring just a few commonly available user inputs, that generates breach impact estimates that you can apply (or customize) in minutes at the overall enterprise, business group/app, or even individual asset level. Breach impact is allocated into four categories for you: detection and escalation costs, notification costs, post breach response costs, and lost business costs.

Balbix automatically cascades, allocates and aggregates the breach impact across the full model for maximum consistency.

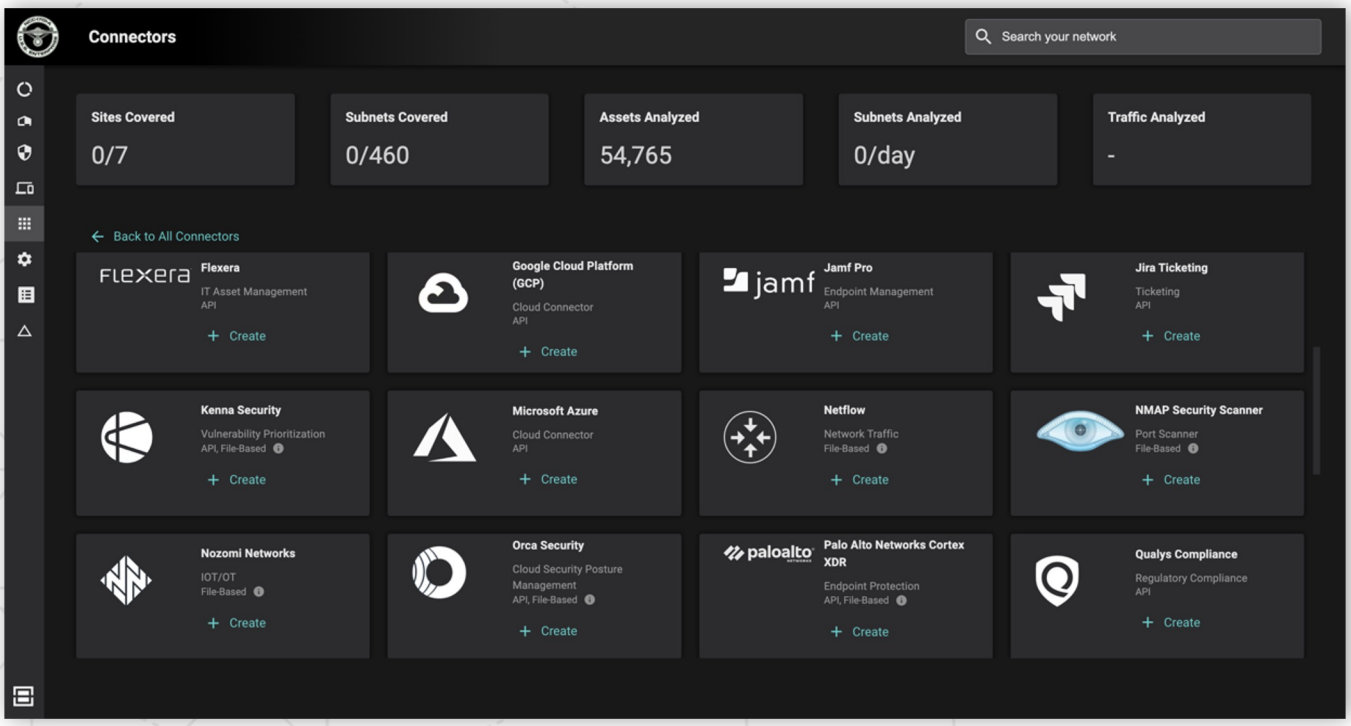
Balbix

Scalable Data Connector Framework for No-Touch Ingestion

With traditional cyber risk analysis, sourcing, gathering, cleansing, and staging necessary data is a major project in itself. And once that analysis is done, forget about reuse for the next time.

Balbix completely changes the data paradigm for CRQ. Leveraging a highly scalable connector framework, data pipeline and cloud-based data lake, Balbix is agnostic to data source and ingests, cleanses and processes Fortune 100-scale data volumes without breaking a sweat. Simply identify your required 3rd party or custom tools, configure one-time API or snapshot-based connectors in minutes (whether on-prem or in the cloud), set up your desired recurring automation schedule, and go. And for customers with data gaps across part or all of the environment, Balbix provides a variety of software-based sensors to fill in the gaps and provide robust data assurance. Cyber risk quantification becomes a continuous, scalable process without operational care and feeding from your side.

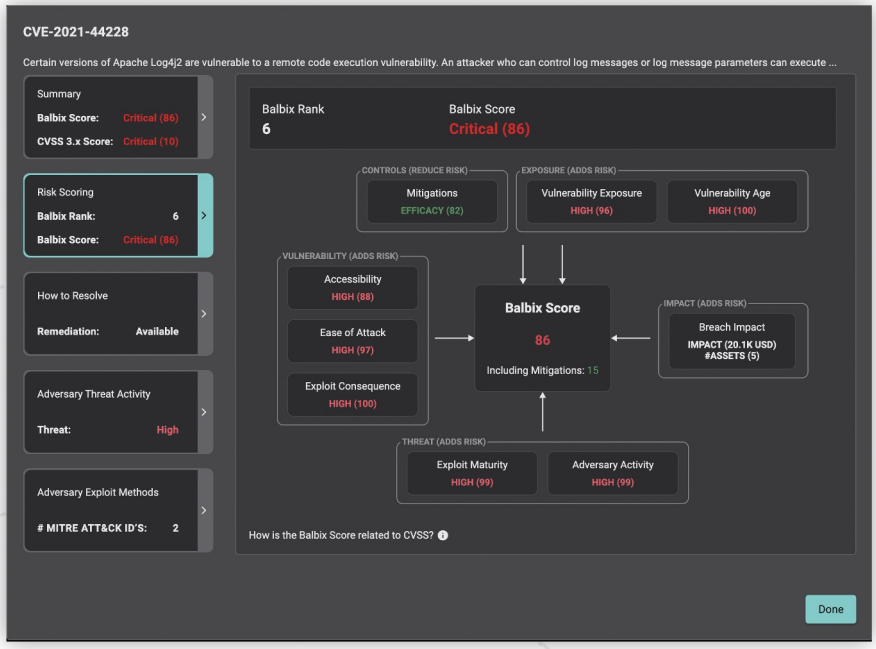
And what's more, Balbix retains all relevant data during the length of your subscription, whether asset, control, vulnerability, risk, or business context-related – optimizing data usage as well as ability to track and trend both granular details and business-aligned metrics over time.



AI/ML-Driven Automation Tames your Data Complexity

One of the historical hurdles to deploying CRQ has been the shear complexity of the analysis, particularly the need for expert teams to scrub and interpret input data, cleanse and normalize, and ensure alignment to changing business parameters.

Cyber and risk teams have recognized the potential for AI (artificial intelligence) and ML (machine learning) to make sense of partial, messy, semi-structured, and evolving data without requiring overloaded human teams in the loop. However, building and maintaining the needed in-house AI/ML and data science expertise and platforms can be daunting, to impossible.



Balbix has invested significant resources over many years into developing a modern and highly performant machine-learning data pipeline, tuned for a bottoms-up cyber risk model, that tames the data complexity problem for you – even at massive scale. And the pace of our ML development only continues to increase. Practical implications for you? Balbix ensures that your CRQ outcomes are comprehensive, clean, up-to-date, and accurate. Just a few examples:

- Identifying, cleansing, de-duping, and auto-categorizing assets with high accuracy even with missing, partial, and complex identifying attributes (Enumeration Logic)
- Discovering, normalizing, and tagging new vulnerabilities accurately across tens of thousands of software products, packages, and components within hours of availability (Vulnerability Parsing and Inference)
- Auto-detecting deployed endpoint controls and computing associated breach likelihood reduction vs. all detected vulnerability instances per asset (Controls Discovery, MITRE ATT&CK Mapping and Controls Efficacy Estimation)

Balbix

3 Actionable Results & Remediation Workflows

Drive Actionable Risk Reduction with Risk-Based Vulnerability Management

The output of an effective CRQ analysis starts with the “what” – specifically, what is the monetary level of risk associated with your organization, business units, or key applications. This is a critical step; however astute business leaders will then ask for a plan around how this risk can be reduced. To develop this plan, we need to answer the “where, why, how, who and when” – where is the underlying vulnerability driving each risk, why it exists, how it should be addressed and prioritized to focus on the riskiest items first, who is responsible, and when it needs to be remediated per enterprise policy and SLAs.

This is Risk-Based Vulnerability Management (RBVM). Ultimately, a core foundation of your proactive and cybersecurity efforts is a robust RBVM program designed to keep you ahead of potential threats and efficiently reducing identified risks in an optimal way.

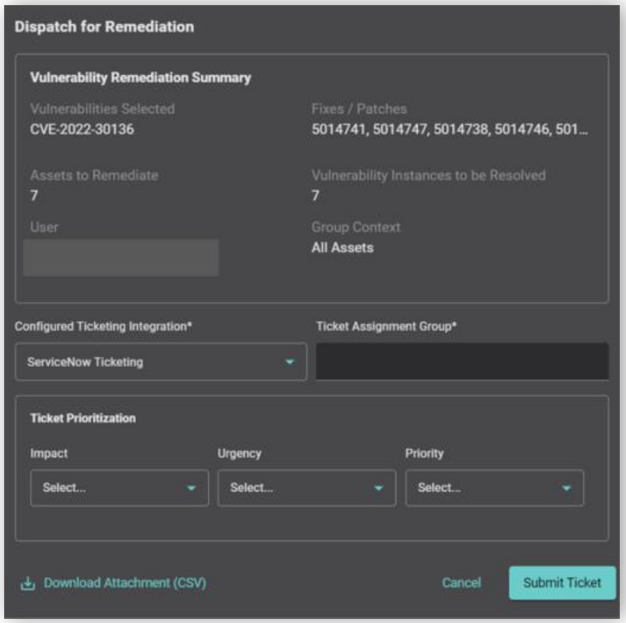
Unlike other CRQ tools and approaches, Balbix doesn’t just stop at quantification. Rather, Balbix natively automates your best-in-class RBVM program to discover, prioritize, remediate, and report on your vulnerabilities to reduce your risk at high velocity, all from the same integrated platform. The Balbix RBVM automation playbook spans the following steps: continuous and unified asset inventory, continuous and unified vulnerability visibility, risk-based vulnerability prioritization, actionable remediation workflows, and comprehensive vulnerability management metrics.

Don’t just report on your risk. Reduce it at high velocity with confidence and accuracy.

Enabling Remediation Workflow & Integrations

Are you looking for an efficient way to streamline your remediation process?

Through Balbix's integrations with ticketing platforms such as ServiceNow ITSM or Jira Service Management, creating remediation tickets is a breeze. By pushing detailed fix information to remediation tickets, your teams can quickly address prioritized vulnerabilities with minimal manual effort. Plus, these integrations enable your security and IT teams to work more efficiently by utilizing your established systems for remediation workflows.



Risk Acceptance Workflow

A successful risk management program must provide a way for risk owners to accept and manage related risks in line with the organization's policies. This is exactly what Balbix helps you enable.

Balbix makes it easy for risk owners to select the vulnerabilities they want to address, assign responsibility, document the reason for risk acceptance, and set an expiry target date. All risk acceptance events are automatically tracked and summarized in a comprehensive dashboard that includes vulnerability instances, trends, severity analytics, and associated details. Balbix's vulnerability risk acceptance management framework also helps key stakeholders such as GRC leaders and auditors understand the level of risk the organization is taking on.

You Too Can Quantify Your Cyber Risk

In 2022, Balbix helped the average Fortune 500 customer **reduce their quantified cyber risk by 37%**, with the largest risk reduction achieved for a single customer being **$120M.** These improvements involved a combination of actions – increased visibility, deployment of new capabilities and gamification – all guided by insights provided by Balbix.

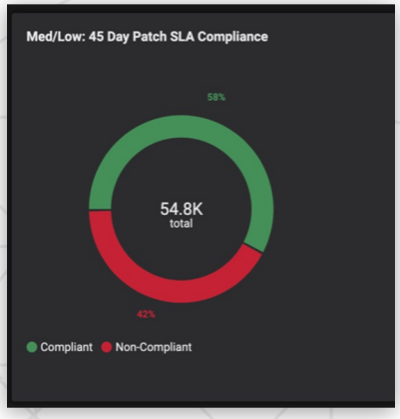
Targeted Compliance Reporting

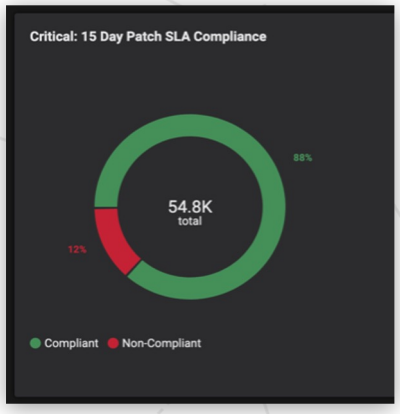
How can you ensure that your team is meeting critical compliance requirements relevant to industry-standard control frameworks such as NIST or CIS, key regulatory requirements, or internal policies and service level agreements (SLAs)?

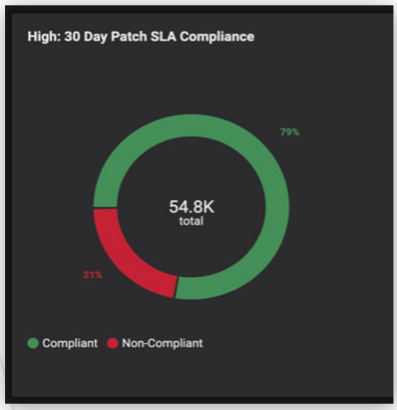
Unlike typical CRQ or controls assessment tools that rely on manual questionnaires and provide only high-level and subjective estimates of compliance status, Balbix's data-driven, asset-level risk model enables you to surface key compliance metrics based on bottoms-up data. Balbix not only automates your process with high accuracy, but also enables immediate inspection of the underlying sources of non-compliance to help your teams find and fix issues.

Below are just a few example compliance metrics that can be easily automated with the Balbix platform, enabling your teams to quickly identify, prioritize and address related compliance failures.

- Permitted asset types and manufacturers (e.g., address IoT/rogue assets)
- Permitted OS and 3rd party software (e.g., enterprise allow-list)
- End-of-life (EOL) OS and software
- Endpoint controls deployment coverage
- Vulnerability assessment coverage
- Patch SLA policy
- Mean-time-to-remediate (MTTR) policy





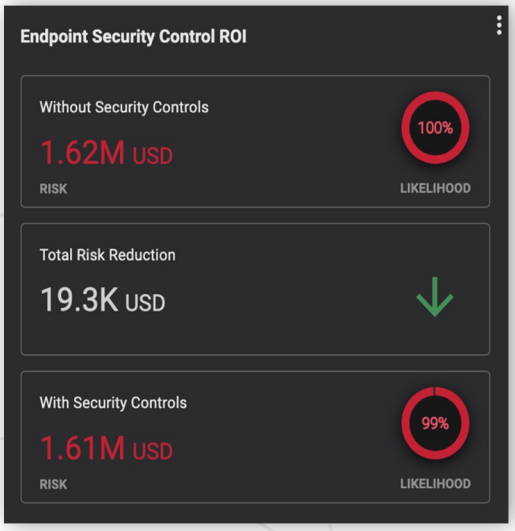


With Balbix, you can automatically generate and trend the above compliance-related metrics to take your compliance dashboards to the next level of actionability.

Report on ROI for Deployed Controls

Security controls are a core element of your proactive security program and strategy. However, it can be difficult to determine the actual risk reduction benefit enabled by these controls. Such understanding is critical to enable a proper monetary ROI (return on investment) analysis on your controls and scope out if cybersecurity budget is being well-spent or can be consolidated, reallocated, or optimized.

Historically, many risk and infosec teams have been limited to subjective guesstimates such as “Deployment of endpoint controls across my key assets is good”, feeding that into a simple CRQ model, and reporting on the results. Unfortunately, garbage-in means garbage-out and taking this type of estimate to your board is high risk and not very not defendable!



Balbix enables you to report on deployed endpoint controls ROI with confidence and accuracy by leveraging the bottoms-up, asset-level risk model. Under the hood, Balbix determines how effective each detected endpoint control is at mitigating the actual vulnerabilities discovered on each asset (using automatic mapping of both to MITRE ATT&CK tactics and techniques), and adjusting breach likelihood (and therefore, breach risk) of each asset accordingly.

The result? Balbix enables you to easily dashboard the risk-reducing effect of deployed controls across key assets, environments, applications, or business groups in monetary terms – and then drive the right decisions to be made regarding controls deployment or adjustments needed.

> “I wanted a system to produce an executive summary of our cybersecurity posture and say to the board ‘*hey, this is what we’re doing*’ and ‘*we’ve done better over time*.’ That’s what Balbix gives me. Balbix showed me the ROI for my entire cybersecurity program.”
>
> **- John Shaffer, CIO, Greenhill & Co.**

4 Gamification to Drive Action

Customizable Executive and Operational Dashboards

With Balbix, you can answer a nearly unlimited number of questions that come up as your teams go about their daily work. Balbix search allows you to query using the vocabulary of cybersecurity, IT, business context and cyber risk, e.g., “What is the breach risk related to mission-critical servers in Germany and managed by our Cloud BU?”

The dynamic groups built from these search queries enable stakeholders to precisely monitor and dashboard critical assets in scope, making it easier to stay ahead of potential threats. By assigning owners to specific asset groups, you can ensure that each owner has a clear understanding of their responsibilities and hold them accountable. Flexible dashboards and widgets can be quickly constructed out of these groups and used for near real-time reporting.

Think of Balbix's dashboards as a distributed workbench for your team or organization that enables real-time monitoring, analysis, and collaboration. Executive and operational dashboards and reports can be shared with the key stakeholders involved, effectively gamifying the process of overall cyber risk reduction.

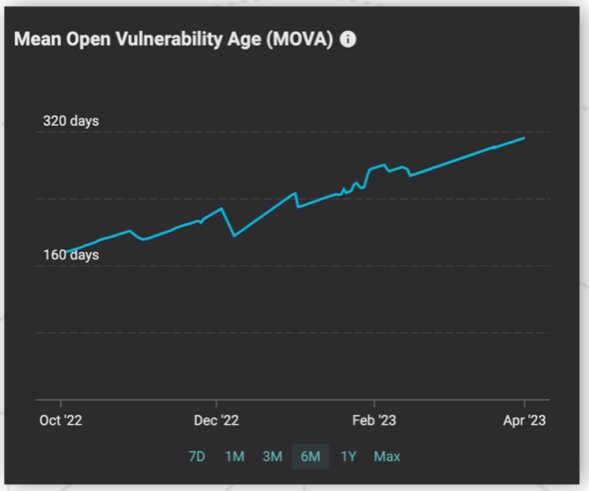
Using Balbix’s dashboards, you can provide each risk owner in your organization with the right information, the right tools, and the right incentives to do their part for effective risk management.

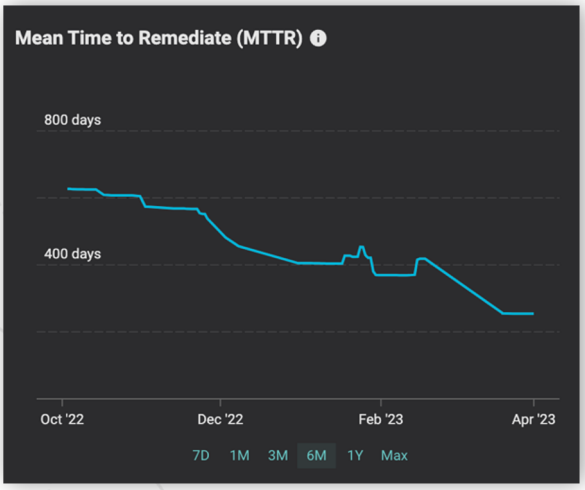
Built-in Trends and Benchmarking to Drive Effective Risk Communication

At Balbix, we have a saying, “Snapshots are emotional, trends are factual.” The meaning here is that without effective trending and relative benchmarking of data over time, single cyber risk data points have limited ability to drive fact-based decisions. Business leaders lack context, resulting in emotional or gut-driven interpretations.

Traditional CRQ analysis has struggled to provide effective trending and benchmarking. Efforts are periodic at best and typically generate a point-in-time snapshot risk distribution, perhaps annually or every 3-6 months. Stakeholders struggle to interpret these data points and use them effectively.

Here it is critical to focus on relative levels of risk across parts of the business or other enterprises (benchmarking) and rate of change (trends). Then cybersecurity, risk and business leaders can quickly determine which teams are struggling, and where they need help – along with identifying approaches that are bearing fruit and reducing risk to the business.



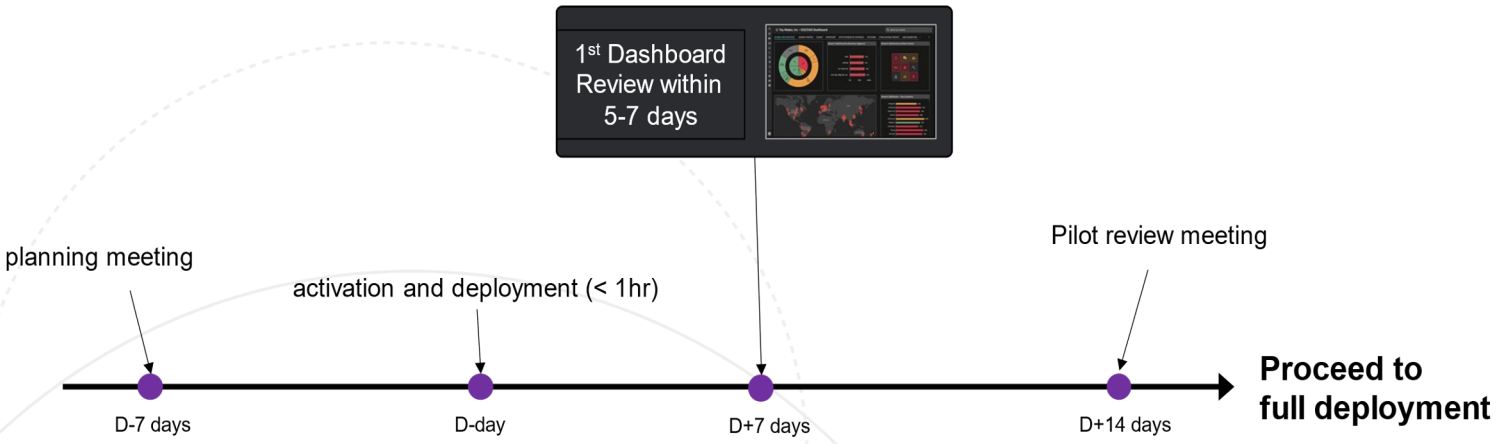


Balbix enables a step-change in effectiveness around cyber risk communication. Leveraging the powerful dynamic groups discussed previously, Balbix users can not generate only benchmark breach risk, breach likelihood and other key metrics across the business – they can also continuously track improvements with built-in trending over time. Dashboards “come to life” and can be shared or pushed to key stakeholders, enabling clear and meaningful communication, and energizing specific actions needed to better manage cyber risk.

It is easy to get started…

The Balbix Security Cloud is a modern, SaaS-based platform that enables rapid enterprise deployment. It uses AI and automation to reinvent how the world's leading organizations reduce cyber risk. With Balbix, security teams can accurately inventory their cloud and on-premise assets, conduct risk-based vulnerability management and quantify their cyber risk in monetary terms.

A typical Balbix pilot deployment covers enterprise-wide scope with a prioritized set of data sources and takes a matter of hours to plan and configure. If you wish, you can sample all the capabilities described in this document running in your environment next week. Our pilots roll forward naturally into full production with rapid time-to-value.



Please visit www.balbix.com to schedule a call with us.