WHITEPAPER

Enterprise Cyber Risk Management – Protecting IT Assets that Matter

Bay Dynamics®

Contents

Protecting IT Assets That Matter 3

Today's Cyber Security and Risk Management: Isolated, Fragmented and Broken 4

Protecting IT Assets at Risk: Connecting the Dots 5

Bay Dynamics Enables Enterprises To Take Action Based On Actual Risks 7

How Risk Fabric Drives Risk Based Asset-Centric Mitigation 8

Who Benefits? 11

Bay Dynamics®

Protecting IT assets is a complicated business. With so many moving parts and concerns, it's no wonder how quickly security teams can be overwhelmed by the threats and vulnerabilities barraging their enterprises every day.

Most teams find it difficult to decide how to address the right threats at the right time in order to defend the assets that mean the most to their organizations. The reason is multifaceted.

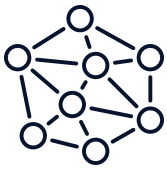
Not only are IT assets scattered across the enterprise in great volume, but these systems, applications and data all deliver different value to the business. In other words, no two assets are created equally.

At the same time, a huge number of vulnerabilities impact different assets with different levels of exposure. And the threats that exploit those vulnerabilities come in all shapes and sizes — from both inside and outside the organization — to impact assets with varying degrees of severity.

The problem is that most security teams and executives get so caught up in the tactical minutiae of any one of those factors, they forget that risk is based on the complete picture of how they all relate to one another.

If enterprises are really going to meet business risks head on, they need to understand how to comprehensively protect their IT assets at risk. And in order to do that, they need to address the following four crucial aspects of cyber risk not just one-by-one or in a scattershot approach, but *in relation to one another*:

IT Asset Value



IT Asset Business Context

Threat and Behavioral Anomaly Data

Vulnerability Data

Today's Cyber Security and Risk Management: Isolated, Fragmented and Broken

Risk is holistic. But most cyber security programs are not.

Security executives recognized long ago that cyber security requires a layered approach that involves a whole array of specialized products. Unfortunately, where many of them fall short is that these tools frequently operate in their own self-contained silos. On the threat and anomaly detection side of the house, organizations juggle isolated tools like Data Loss Prevention (DLP), endpoint protection, web proxy monitoring and log-in and user monitoring. On the vulnerability lifecycle management there are results from scanners, penetration tests and a slew of audit utilities. Each one of these tools sounds off alerts by the thousands each day, but these red flags are rarely connected with one another.

Companies have attempted to make some sense of the threat data by consolidating it into SIEM tools, but these have ultimately proved useful only for post-event forensics and regulatory logging. Similarly, vulnerability scan data gets pumped into GRC tools like Archer, but companies struggle to do anything with it beyond tracking open findings. Most companies lack an integrated view of threats and vulnerabilities.

And worse yet, organizations rarely loop in information about the value of the affected assets or the business context in which these systems or data are used. All these solutions treat assets equally without identifying the 'crown jewels' that may need more protection than others, such as the mission critical infrastructure or assets in scope of compliance.

As a result, security operations analysts never know which alerts are truly the highest priority based on risk. And security executives rarely get truthful, traceable metrics about how well their most important assets are being protected.

74%

of large enterprises

regularly ignore some security alerts because they're so overwhelmed

31%

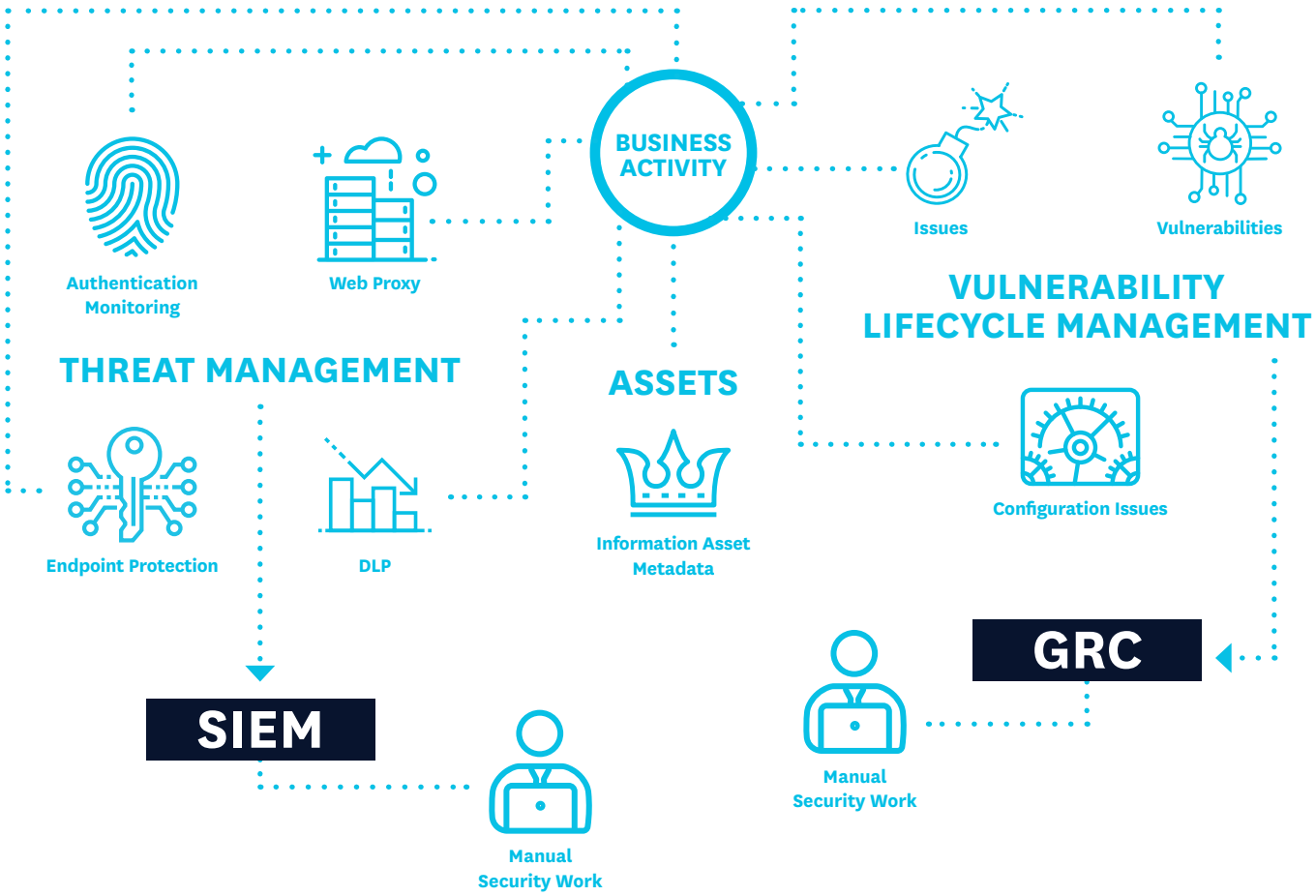
of large enterprises

ignore at least half of these alerts[1]

[1] securityweek.com/incident-response-becoming-more-difficult-survey

Protecting IT Assets at Risk: Connecting the Dots

To run an effective cyber security and risk management program, enterprises need to find a way to unify the information isolated in current security tool silos so that they can get true visibility into the assets most at risk.



Unification requires enterprises to build in *interconnection* between the four aspects of IT asset protection—IT asset value, IT asset business context, threat and behavior anomaly data and vulnerability data—so that the security program can make decisions and respond quickly based on a holistic risk profile.

IT Asset Value

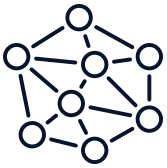
Perhaps the most important component when it comes to prioritizing risk mitigation activities, asset value is also often one of the most forgotten. One of the biggest and most common failures of security and IT departments today is that all of their actions are based only on threat or vulnerability severity. Rarely do they ever frame the urgency of response based on the value of the impacted asset.

As a result, for example, a low-value asset with a severe critical vulnerability may be treated more swiftly than a mission-critical asset affected by a vulnerability with a lower criticality rating. This wouldn't reflect the actual risk posed in the situation, as those crown jewels demand faster remediation in most scenarios.

Threat and Behavior Anomaly Data

Threat and anomaly information comes from numerous sources across the enterprise infrastructure and from external threat intelligence feeds. When done right, all sources should be fed into risk analysis, including those that offer information about events potentially involving abuse of privilege, dangerous web activity, malware and data exfiltration.

IT Asset Business Context



Not only is the value of the asset important, but so too is the context in which it is being operated. This includes compliance considerations for specific assets, as well as contextual information about the on-the-ground working conditions that may drive user behavior. For example, an alert that pops up as a result of a user accessing sensitive assets from a strange geography or at a strange time of day may be easily explained by the fact that that user's group is on a business trip out of the country.

Much of that contextual information can be easily provided by the line-of-business application owners who have the most knowledge of how the asset is used and should be governed. Unfortunately, that's a big blind spot of most security tools and practices today. They typically do not build an easy line-of-business (LoB) engagement mechanism into the threat and vulnerability analysis workflow in order to better qualify issues in need of mitigation.

Vulnerability Data

Finally, vulnerability data provided from all means of application testing, penetration testing and audit findings should be considered in context of the other three components to develop a complete picture of risk for affected assets. This includes ranked vulnerability lists, configuration problems and other potential exposures within software and systems.

Bay Dynamics Enables Enterprises To Take Action Based On Actual Risks

The Bay Dynamics Risk Fabric® platform enables organizations to reduce risk by bringing together and correlating information from all four components that make up an asset's risk profile.

The Risk Fabric platform creates the connection between those components through these key capabilities:

Data Ingestion and Normalization

- Ingests threat data from SIEM, DLP, Web Proxy, Endpoint and other security tools
- Ingests vulnerability data from GRC, vulnerability management solutions and pen testing tools
- Ingests asset management information from the company's various asset management tools

Line of Business (LoB) Engagement

Engages LoB application owners to provide the asset value and business context

Algorithmic Analysis

Analyzes, correlates and enriches the consumed data using Risk Fabric's purpose-built behavioral analytics engine and value-at-risk algorithms

Prioritized and Orchestrated Remediation

- Automates workflow orchestration to equip decision-making analysts with highly-qualified incidents
- Qualifies incidents based on context from LoB to categorize them as business justified, qualified security incidents or needing further investigation

Executive-Level Measurement

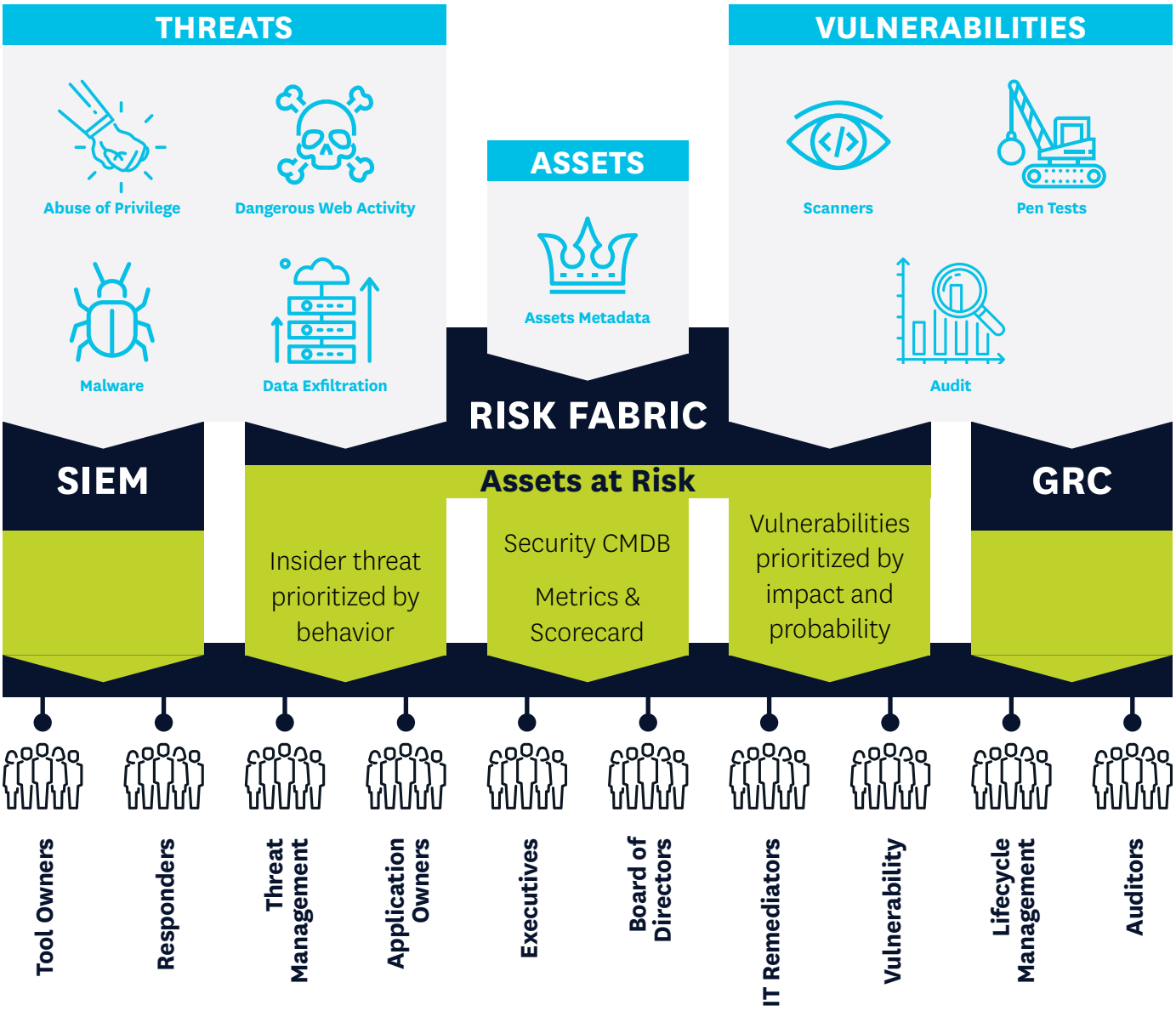
Enables cyber risk visibility and communication through automated security metrics and business dashboards serving the needs of all key stakeholders (Boards of Directors, C-Suite, LoB, Security and IT Operations)

It is the synergy of rolling all of these key steps into a single platform that gives Risk Fabric the edge.

Using a combination of behavior and value-at-risk based analytics, the platform successfully engages LoB application owners who provide asset value and business context, which previously was never taken into consideration for addressing security and risk. This collaboration makes cyber risk everyone's business at the organization – from employees to LoB application owners to the board – and actively engages all parties in measurably reducing it. By involving the right individuals, understanding the assets at risk, and focusing on the metrics that matter, the platform decentralizes risk from the security and risk team and simplifies the process of protecting what matters most with limited resources.

How Risk Fabric Drives Risk Based Asset-Centric Mitigation

Through its comprehensive and streamlined approach, Bay Dynamics Risk Fabric provides security teams the tools they need to minimize false positives and to cut through the alert noise that has been hamstringing their efforts.



As a result, they're able to create a high quality list of the threats and vulnerabilities that could lead to a compromise of companies' crown jewels. What's more, that information can be condensed and analyzed into relevant reports and metrics that help executives and boards of directors make informed decisions about the company's cyber risk management program.

This kind of progress is achieved through several key avenues:

Prioritizing Threats And Anomalies Based On Asset Context
Risk Fabric prioritizes threats and anomalies based on asset context. It does this by involving the asset owner to provide context for the security incidents. This is a streamlined process that quickly puts the right information in front of the right people to help them speedily qualify or disqualify anomalies for further investigation. The orchestration capability routes already pre-qualified incidents that need more context for follow-up to impacted application owners to classify incidents as:

- Business Justified, which white lists the unusual or anomalous incidents based on business need;
- Security Incident Qualified, which tags events that need action through either automated incident remediation or orchestrated human-powered workflow; or
- Needing Further Investigation, which add incidents to a watch list for further analysis and investigation.

Prioritizing Vulnerabilities Based On Asset Value
Similarly, Risk Fabric prioritizes asset vulnerabilities by correlating vulnerability data from scanners, GRC systems and asset management data against input from LoB application owners. LoB stakeholders are given the chance to rank assets by perceived value and Bay Dynamics' proprietary value-at-risk algorithm pinpoints the data, systems and applications that, if compromised, would most impact the business. The platform automates the communication of up-to-date vulnerability information between application owners, security teams and executives. It also provides false positive management and exception management workflows that are tied to vulnerability management process.

Continuous Compliance

Risk Fabric supports a continuous compliance operating model by reporting risk information on a daily basis for applications in the scope of compliance. This reporting offers continuous visibility into vulnerabilities, third-party risk, endpoint agent coverage and open issues, all indexed against in-scope applications, ensuring that organizations are always ready for their next audit. Risk Fabric also pulls together configuration management database (CMDB) data from across the enterprise and creates a centralized and integrated repository of configuration data that's continually updated. The platform leverages this CMDB data to provide security tool coverage that can be automatically reported and communicated against different PCI-scoped applications and LoB application owners.

Cyber Risk Visibility

Additionally, Risk Fabric gives boards of directors and senior executives a top-down view of the company's cyber risk posture by gathering all the aforementioned data into valuable metrics reporting. The platform offers a real-time view of the organization's overall risk posture, as well as a cyber risk scorecard that offers repeatable, automated and traceable results for the CISO to report to the board.

The metrics can be further parsed into risk reduction trends about top insider threats, top risky vendors, top vulnerable assets and top candidates for security awareness training.

This gives CISOs the transparency needed to hold their organization accountable for results and the ability to communicate the state of risk to key business stakeholders.

Who Benefits?

With Risk Fabric, organizations can proactively protect high-value assets, enhance end-user experience, empower users with self-service ability, increase risk visibility, and improve operational efficiency.

The platform benefits stakeholders across the organization.

SOC Analysts – Reduces alert fatigue and improves response effectiveness by driving prioritized investigations based on collaboration with application owners.

CISO – Improves measurement of risk and enables targeted improvements of security practices based on tangible evidence.

Compliance Officers – Eliminates the quarterly or annual spreadsheet and email scramble to gather information and remediate open items.

LoB Application Owners – Improves business efficiencies by ensuring security intervention is carried out on the most important incidents and vulnerabilities that matter to their applications and users.

Boards of Directors and C-Suite – Enables cost efficiencies by maximizing value from existing security and IT tools; offers best visibility into the risks that could most impact the business.

To learn more about Risk Fabric's technical capabilities, visit *https://baydynamics.com/risk-fabric/*

About Bay Dynamics®

Bay Dynamics® is a cyber risk analytics company that helps enterprises measure, communicate and reduce cyber risk. The company's flagship analytics software, Risk Fabric®, automates the process of collecting and reporting cyber risk information. The platform also tells security teams, application owners and incident responders which vulnerabilities to fix and which threats to investigate. Bay Dynamics enables some of the world's largest organizations to understand the state of their cyber security posture, including what their insiders, vendors and bad actors are doing, which is key to effective cyber risk management. For more information, please visit *www.baydynamics.com*.