Balbix Recognized as the

2021

Technology Innovation Leader

North American

Cybersecurity Posture Management Industry

Excellence in Best Practices

FROST *&* SULLIVAN

Strategic Imperatives

Frost & Sullivan identifies three key strategic imperatives that impact the security industry: geopolitical chaos, disruptive technologies, and innovative business models. Every company that is competing in the security space is obligated to address these imperatives proactively; failing to do so will almost certainly lead to stagnation or decline. Successful companies overcome the challenges posed by these imperatives and leverage them to drive innovation and growth. Frost & Sullivan's recognition of Balbix is a reflection of how well it is performing against the backdrop of these imperatives.

THE IMPACT OF THE STRATEGIC IMPERATIVE 8™ ON SECURITY INDUSTRY
The following 3 strategic imperatives will ensure growth in the security industry.

SI8

GEOPOLITICAL CHAOS	DISRUPTIVE TECHNOLOGIES	INNOVATIVE BUSINESS MODELS
Why • The COVID-19 pandemic caused manufacturing operations that rely on multi-national supply chains to experience significant disruptions. • Project extensions are delaying contract fund allocation, which will affect contractors and subcontractors' bottom lines. • Commercial and passenger-centric industries will experience sharp declines in revenue due to the impact of COVID-19, whereas opportunities in the public sector will grow exponentially. • National security skirmishes between nations continue to cause piecemeal disruptions to security technology deals.	• Investment in digitization will increase to improve the intelligence cycle and address the current threat landscape, which includes ransomware, digital intrusion, and data theft. • Wearables, drones, and augmented reality will find application in crime scene mapping, automatic translation, border surveillance, search and rescue, and threat detection. • Demand will increase for artificial intelligence (AI)-enabled remote or cloud interactions to foster better communication and system support.	• Security forces are gradually transitioning from ownership to subscription-based business models. New business models (e.g., screening as a service, biometrics as a service, ISR as a service, and infrastructure as a service) are reducing the cost of ownership. • Increasing need for niche security solutions, rapid tech advancements, and budget pressures will drive the industry to explore innovative revenue models. • Customers want modular surveillance alternatives that allow for the contracting and scaling of long-term system design.
When • Firms will need to pursue strategic partnerships between vendors with complementary solutions and local suppliers to improve global customer reach, without increasing their overhead costs. • After the pandemic, larger security companies will realign and acquire portfolios and businesses in growth areas (such as digital security) to expand their solution portfolios across end-user verticals. • Cloud access, zero-trust and multi-factor authentication, and security-as-a-service solutions will become imperative to business continuity in the next 1 to 5 years. • Security firms must understand the national security policies applicable to specific international customers because policy affects security technology.	• Firms must prioritize the development of data analytics and sensor networks' capabilities to provide increased value to customers. • Security companies will need to invest in contactless technologies, biometrics solutions used with AI technology, remote access and authentication, and multi-use analytics in the next 4 to 5 years. • Firms will need to differentiate technology offerings for vertical-specific solutions (i.e., analytics tailored to an airport or public safety function) among multiple end-user industries. • Actionable intelligence and multi-source data aggregation will gain prominence in the next 5 to 10 years, as will the desire to shift some security operations away from a physical location to a cloud-based, remote system.	• Competitive strategy, technology, and IP opportunities will push vendors to re-examine their solutions and road maps to account for market slowdowns. This will lead them to reposition existing offerings to meet new market demands in the next 2 to 3 years. • Achieving vertical market expansion and distribution channel optimization through strategic partnerships and acquisitions will become top priorities in the next 3 to 6 years. • Businesses will seek flexible business models to stay lean by minimizing capital expenditure while ensuring scalability and redundancy in critical operations processes. These models include leasing/renting and moving toward a security as a service (SECaaS) approach in the next 5 years.

Source: Frost & Sullivan

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Balbix excels in many of the criteria in the cybersecurity posture management space.

AWARD CRITERIA

Technology Leverage	Business Impact
Commitment to Innovation	Financial Performance
Commitment to Creativity	Customer Acquisition
Technology Incubation	Operational Efficiency
Commercialization Success	Growth Potential
Application Diversity	Human Capital

Automated Cybersecurity Posture Management makes Proactive Cybersecurity Possible

In today's world of digital connectivity, enterprises must protect their digital assets and information. The proliferation of cyberattacks and their complexity means a company's security and information technology (IT) teams' workloads are rapidly increasing. Added to this, traditional approaches to cybersecurity threats are more reactive rather than preventative, with security and IT teams attempting to detect and mitigate attacks rather than prevent them from happening in the first place. Traditional techniques for tracking asset inventory, vulnerability management and periodic penetration testing are not effective, leaving many gaps in an enterprise's defenses that can be easily exploited by adversaries. Frost & Sullivan's independent research reveals that enterprises need new and automated cybersecurity posture capabilities management to proactively monitor their assets for security issues across a broad range of attack vectors and drive timely risk mitigation tasks.

"Balbix's BreachControl platform collects and analyzes data from enterprises' network-connected assets, including servers, desktops, laptops, mobile devices, infrastructure elements, cloud services, and Internet of things, to provide an automatic comprehensive, and up-to-date asset inventory. Enterprise assets are continuously analyzed for breach risk across hundreds of attack vectors, including unpatched software, misconfigurations, password issues, lack of encryption, and more. Specialized machine learning (ML) algorithms assess breach risk, estimating both breach likelihood and business impact for individual assets, asset groups, and whole organizations. "

- Elizabeth Whynott, Best Practices Research Analyst

Balbix's BreachControl platform offers a comprehensive solution to enterprise's needs for automated cybersecurity posture management. A two-time Frost & Sullivan award recipient, Balbix continues to develop and improve its BreachControl platform. The company's chief executive officer and founder, Gaurav Banga, started Balbix in 2015 in San Jose, California, making substantial headway in the cybersecurity industry.

The company's BreachControl platform collects and analyzes data from enterprises' network-connected assets, including servers, desktops, laptops, mobile devices, infrastructure elements, cloud services, and Internet of things, to provide an automatic comprehensive, and up-to-date asset inventory. Enterprise assets are continuously analyzed for breach risk across hundreds of attack vectors, including unpatched software, misconfigurations, password issues, lack of encryption, and more. Specialized machine learning (ML) algorithms assess breach risk, estimating both breach likelihood and business impact for individual assets, asset groups, and whole organizations. The system delivers a prioritized set of actions for the enterprises' security team to mitigate risk by fixing the underlying issues.

Unlike traditional techniques, most organizations do not have accurate asset inventory and often rely on multiple systems to track their assets. These legacy inventory systems typically require manual data input, and IT and security personnel need to collate information from more than one system for their daily tasks. Even with proper implementation, vulnerability management and manual penetration testing suffer from large gaps in attack surface coverage. Traditional vulnerability management tools are also awkward to operate and require substantial manual effort in workflows. Penetration testing has an even narrower scope and only provides a point-in-time snapshot of vulnerabilities. Additionally, these approaches typically produce a deluge of unprioritized vulnerabilities, many of which are false positives and practically unexploitable, leading to wasted efforts by cybersecurity defenders. Most importantly, vulnerability data produced by traditional vulnerability assessment tools and penetration test reports are hard to comprehend in terms of associated business risk. As a result, most risk owners do not understand vulnerabilities and fail to own critical mitigation tasks, leaving the enterprise at risk of a breach. Balbix's Software-as-a-Service approach makes it easy for organizations of all sizes to implement a highly automated and risk-based approach towards avoiding cybersecurity breaches.

Balbix Provides Comprehensive Cybersecurity Posture Management as Challenges Increase

The cybersecurity challenge is only getting more demanding as digital connectivity increases and drives business growth. However, more connected devices mean more access paths to the enterprise, which attackers can compromise. More entry points for an attack also mean less visibility and safety control for IT teams, making it difficult to manage and prioritize threats. During the COVID-19 global pandemic more employees are working from home and do not have the same IT and security controls in place that are present in their organization's offices and data centers. This dramatic increase in attack surface makes it imperative that organizations rethink their cybersecurity posture management strategy.

Balbix's BreachControl platform seamlessly navigates the demands of monitoring more connected devices and a distributed enterprise network while also providing better insights to security and IT teams to prevent cybersecurity breaches. Balbix's system monitors the enterprise using three types of sensors and numerous connectors. Network sensors identify risks from open network services, traffic sensors provide real-time monitoring of internet activity and phishing attempts, and host sensors collect information directly from endpoints. Connectors gather data from existing enterprise IT and security tools. In essence, these sensors and connectors continuously gather information about asset inventory as well as many factors relevant to the ease or difficulty by which an adversary may compromise an asset. This data becomes the input for Balbix's ML algorithms, and all sensory data is de-duped and collated to the relevant assets. Specialized ML models then analyze this information to predict risk and

provide actionable steps to mitigate these vulnerabilities and security issues. Additionally, customizable dashboards enable various security and IT roles to use Balbix in their daily workflows.

For prioritizing vulnerabilities and other security issues, BreachControl incorporates five factors: vulnerability severity, threat level, business criticality, asset exposure, and the risk-negating effect of relevant security controls. These factors ensure that security and IT personnel know which issues need immediate attention, which can wait a day or so, and which are just noise and do not require additional scrutiny. As security and IT teams implement risk management solutions, the platform provides a further assessment of control efficiency while continuously monitoring weak points in the network's security infrastructure.

BreachControl further stands apart from traditional cybersecurity methods with its continuous mode of operation. That is, conventional penetration tests are typically performed a few times a year, cannot keep pace with new breach attempts, and usually focus on a segment of the enterprise's overall infrastructure. Frost & Sullivan's research finds this type of penetration testing obsolete as it does not provide a broad risk assessment and can leave enterprises floundering when a breach occurs. BreachControl resolves these issues by conducting security assessments that are automated, continuous, and comprehensive, thereby providing security teams with up-to-date risk metrics and supporting information. Due to its continuous nature, Balbix's BreachControl not only offers an innovative and robust cybersecurity platform but also provides enterprises peace of mind.

Work-flow Reduction with a Customizable User-friendly Platform

Balbix's BreachControl provides breach risk reporting built out-of-the-box with customizable views based on the organizational structure, processes, and other requirements. A chief information security officer or chief information officer's view of enterprise breach risk might look like the dashboard below (see Figure 1).[1] Inventory and categorization of all assets, as well as criticality analysis, are performed automatically and continuously, ensuring that foundational information is always at the team's fingertips. Balbix's platform not only surfaces risk issues but also reduces the number of steps and the time security and IT teams spend working to mitigate such threats. Numerous time-consuming tasks are now done automatically and within seconds instead of taking hours or days. Additionally, easy-to-understand visuals help security and IT teams prioritize which asset groups are at greater risk and provide actionable insights to alleviate threats. The platform also offers access to threat intelligence, risk heat maps, risk by attack vector, and detailed security and inventory information for each enterprise asset. Furthermore, the platform has easy-to-use drill-downs and supports natural language search for quick access to various cybersecurity, risk, and IT queries.

---

[1] https://www.balbix.com/product-overview/

As a drill-down example, Figure 1 shows a view an organization might choose, which shows vulnerabilities by risk owner. This drill-down capability demonstrates Balbix's commitment to innovation. The Balbix dashboard maps risk from the network layer to the business layer, enabling security and IT teams to monitor vulnerabilities and security issues in a business context such as "risk to customer data." Risk is also mapped automatically to specific owners, who can view personal dashboards and all information to do their part in mitigating enterprise breach risk. Feedback from a typical customer indicates that the Balbix platform helps reduce the mean-time-to-resolve for security issues to 7.5 days, down from over 300 days, while saving thousands of labor-hours.

Figure 1: BreachControl Dashboard View

Source: Balbix

Balbix further demonstrates a commitment to its clients by being receptive to their needs. While many tasks that Balbix performs are fully automated (e.g., scans, progress reports, graph creation, and other reporting outputs that typically take days to gather and create), it can sometimes cause unseen issues for some enterprise networks. The company understands these considerations and provides easy to use controls to supervise automation for tasks that may interfere with systems.

> *"BreachControl resolves these issues by conducting security assessments that are automated, continuous, and comprehensive, thereby providing security teams with up-to-date risk metrics and supporting information. Due to its continuous nature, Balbix's BreachControl not only offers an innovative and robust cybersecurity platform but also provides enterprises peace of mind."*
>
> *- Elizabeth Whynott, Best Practices Research Analyst*

Out-of-the-box, BreachControl serves three purposes: inventory and discovery, vulnerability management, and risk calculation and mapping; enterprises can choose all or a specific feature to fit their requirements. This specificity has given Balbix an edge over competitors who only offer one solution. With Balbix, clients have a choice for a three-pronged comprehensive cybersecurity risk solution or can choose one or two that best suit their needs. The company also provides customization options to meet enterprises' unique needs, supporting a broad class of cybersecurity jobs and projects. Once BreachControl is active in an enterprise's network, operators can further customize the platform by integrating their proprietary data sources and custom workflows.

Expanding and Continuous Success

Since 2018, Balbix continues to expand its customer base and improve its financial performance. The company gained large contracts upwards of $2.5 million with companies ranging from 500 to 500,000 employees. In comparison to 2018, Balbix's largest customer had 50,000 employees, demonstrating its platform's ability to service both small and large business needs. Balbix's BreachControl offers enterprises a versatile cybersecurity posture management platform that provides a large tool-belt for security and IT teams to take advantage of and reduce their workloads and operational costs. Saving companies time, money, and managing their risk furthers Balbix's market reach and ensures future growth. In 2019, the company saw revenue growth of 450% and maintain a strong investor base. The company's investors include Mayfield, JC2 Ventures, Singtel Innov8, and Mubadala Ventures. Balbix's rapid growth, expanding client-base, and committed investors help ensure its future in the cybersecurity posture management industry.

Conclusion

Balbix's BreachControl platform continues to offer the ability to automate cybersecurity posture management for enterprises' cybersecurity needs. The company's platform addresses cybersecurity needs before a breach occurs by monitoring network-connected devices, continuous risk assessments and analyses, and prioritizing actionable insights to mitigate breaches from occurring. Balbix demonstrates outstanding customer service by providing customization options to meet enterprises' unique cybersecurity posture management and automation needs and incorporate their feedback in developing advanced versions of the platform. The agnostic platform means its market reach is not limited to one industry and ensures its future growth potential. Backed by leading technology venture capitalist firms, Balbix demonstrates its ability to maintain and grow its standing in the cybersecurity posture management industry.

For its strong overall performance, Balbix is recognized with Frost & Sullivan's 2021 North America Technology Innovation Leadership Award in the cybersecurity posture management industry.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create on-going growth opportunities and strategies for our clients is fuelled by the Innovation Generator™. Learn more.

Key Impacts:

- **Growth Pipeline:** Continuous flow of Growth opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** Implementation Excellence
- **Transformational Growth:** Industry Leadership

The Innovation Generator™

Our six analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- **Mega Trend (MT)**
- **Business Model (BM)**
- **Technology (TE)**
- **Industries (IN)**
- **Customer (CU)**
- **Geographies (GE)**