GIGAOM

Competitive Intelligence Battlecard

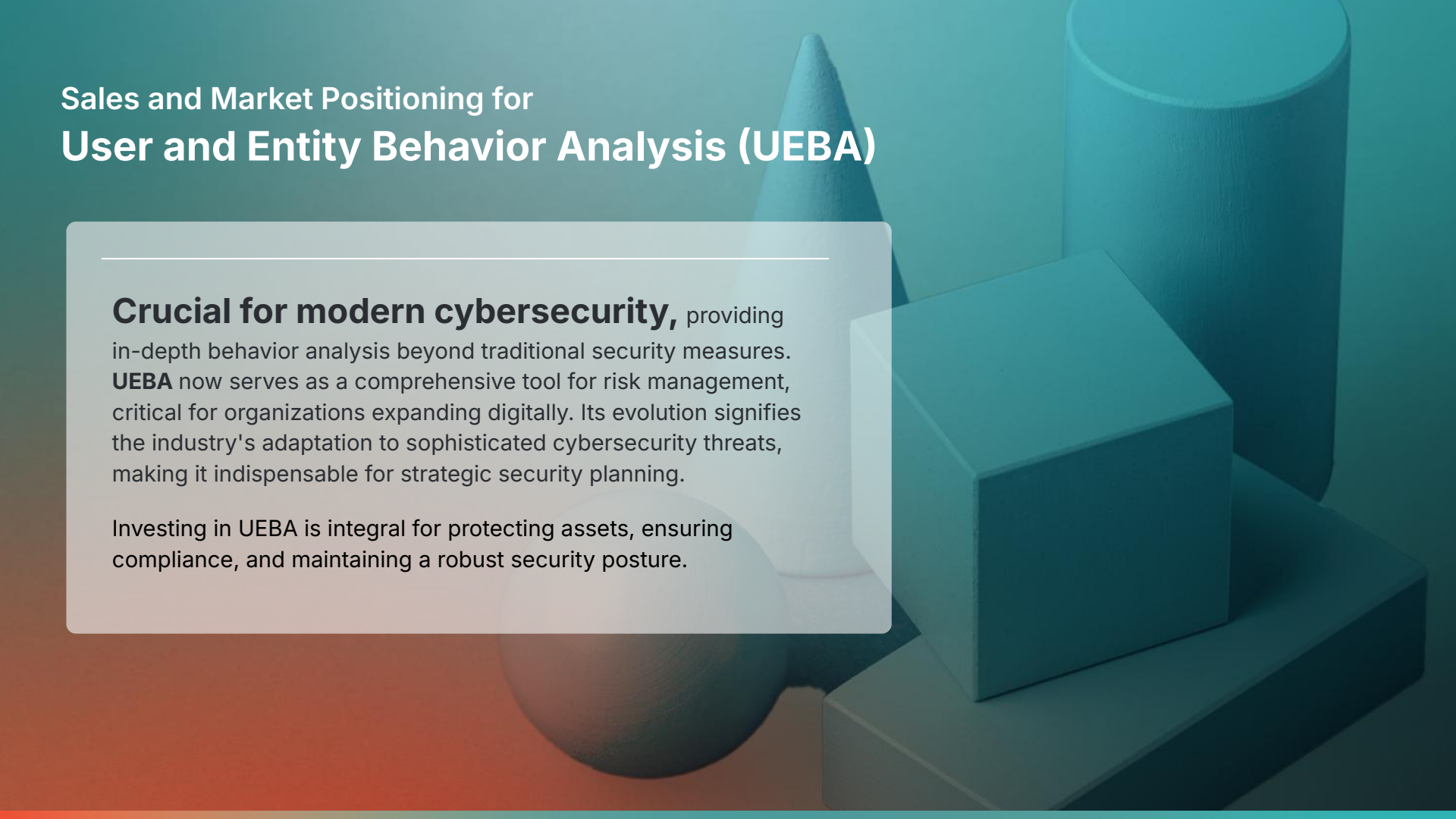
You + GigaOm | Turning Complexity into Clarity

Sales and Market Positioning for

User and Entity Behavior Analysis (UEBA)

Crucial for modern cybersecurity, providing in-depth behavior analysis beyond traditional security measures. **UEBA** now serves as a comprehensive tool for risk management, critical for organizations expanding digitally. Its evolution signifies the industry's adaptation to sophisticated cybersecurity threats, making it indispensable for strategic security planning.

Investing in UEBA is integral for protecting assets, ensuring compliance, and maintaining a robust security posture.



Importance of UEBA

UEBA is a game-changer in cybersecurity, using stats and machine learning to spot unusual patterns in user, machine, and network behavior. Vital for elevating security beyond the basics, it pinpoints potential threats like insider risks or compromised accounts.
Paired with tools like DLP, it's a powerhouse for proactive risk management. UEBA simplifies the digital threat landscape, protecting assets and ensuring operational integrity.

UEBA's value lies in its ability to detect anomalies signaling potential threats, thereby enabling proactive risk management and incident response.

Value of UEBA to Executive Leaders

- **Proactive Threat Detection:** Identifies unusual behavior patterns, enabling early detection of potential security incidents. 'Canary in a coal mine'
- **Comprehensive Risk Management:** Consolidates diverse data points into actionable intelligence, providing a holistic approach to threat mitigation.
- **Regulatory Compliance:** Enables compliance with data protection laws by monitoring and analyzing user activities. 'Trust but verify'.
- **Enhanced Incident Response:** Reduces response times by pinpointing the exact nature and scope of a threat, facilitating quicker remediation.
- **Adaptability to Evolving Threats:** Continuously learns and adapts to new user behavior patterns, staying ahead of sophisticated cyber threats.

Communicating UEBA's Value to Customers

Emphasize the blend of UEBA with insider risk management	▶ Highlighting PROVIDER's unique position to offer in-depth insights into encrypted data and granular endpoint activities.
Stress the importance of behavioral analysis in the early detection of threats	▶ That bypass traditional security measures, showcasing PROVIDER's advanced anomaly detection capabilities.
Highlight the efficiency and scalability of PROVIDER's cloud-first approach	▶ Ensuring comprehensive coverage with minimal data processing overhead.
Point out the cost-effectiveness of enhancing existing security investments	▶ With PROVIDER's UEBA capabilities, improving overall security ROI.
Tailor discussions to the specific challenges and needs of each organization	▶ Using real-world examples and case studies where PROVIDER's UEBA solution has made a significant impact.

Top 5 Current Trends in UEBA

Integration with Broader Security Platforms

UEBA is increasingly being integrated into more extensive security platforms, offering a more unified approach to threat detection and response.

Emphasis on Cloud-Based Solutions

There's a growing preference for cloud-first UEBA solutions, facilitating scalable, flexible, and cost-effective deployments.

Advanced Machine Learning Algorithms

Enhanced ML capabilities for more accurate and dynamic anomaly detection, minimizing false positives and improving threat response times.

Focus on Insider Threat Detection

A significant trend towards the use of UEBA for insider threat detection, leveraging behavioral analytics to identify risky insider activities.

Expansion of Predictive Analytics

The incorporation of predictive analytics into UEBA solutions, enabling organizations to anticipate and preempt potential security incidents before they occur.

Sales and Product Positioning for **PROVIDER**

Pros

- **Advanced Endpoint Telemetry:** Unmatched depth of insight.
- **Cloud-First Scalability:** Efficient processing with minimal impact to local resources.
- **Innovative Use Cases:** Continuously evolves to address emerging security.

Cons

- **Focus on Endpoints:** May not suit if seeking broader network or application-level insights.
- **Complexity:** May overwhelm smaller entities with limited cybersecurity expertise.
- **Integration:** Incorporating into highly diverse or incompatible technology stack may challenge some.

PROVIDER stands out in the UEBA market with its unique integration of UEBA capabilities into its insider risk management platform, InTERCEPT. PROVIDER specializes in providing granular, endpoint-based insights with a cloud-first approach, enabling comprehensive surveillance over user and entity behaviors with minimal overhead. This approach positions PROVIDER as a leader in detecting insider threats and compromised accounts by leveraging rich endpoint telemetry and advanced analytics.

Why customer should buy UEBA from PROVIDER

- **Granular Data Insights:** Detailed endpoint data provides **unparalleled** visibility into user and entity behaviors.
- **Cloud-First Efficiency:** Scalable and efficient solution processing data in the cloud, reducing on-premises infrastructure requirements.
- **Innovative Risk Detection:** Employs advanced statistical analysis and machine learning to detect anomalies, **significantly** reducing the risk of insider threats and compromised accounts.

Objection 1	Objection 2	Objection 3	Objection 4	Objection 5
Perceived Complexity	**Cost Concerns**	**Integrating with existing security tools**	**Endpoint Focus Doubts**	**Resource Intensity for Small Businesses**
Response: Ease of use, cloud scalability, and available support simplifies UEBA for orgs of all sizes	**Response:** ROI of reduced risk, efficiency gains, cost-savings of early threat detection and cloud scalability	**Response:** Examples of successful integrations, underscoring PROVIDER's flexibility and compatibility	**Response:** Highlight critical role of endpoint intelligence in security strategies, offer case studies that demonstrate its effectiveness	**Response:** Showcase managed services option, leverage capabilities without extensive internal resources

Why customers might hesitate to buy UEBA from PROVIDER

- **Endpoint-Centric Approach:** Organizations looking for a broader network-based or non-endpoint-centric UEBA solution might find PROVIDER's focus on endpoints limiting.
- **Resource Intensity for Smaller Organizations:** Small businesses may find the platform more sophisticated than their needs or resources allow for effective management.
- **Integration Considerations:** Companies heavily invested in non-compatible security ecosystems may face challenges integrating PROVIDER with their existing infrastructure.

Sales Positioning

When talking to customers, sales should position PROVIDER as:

A leader in endpoint-based insider threat detection, using UEBA to provide unmatched visibility and risk detection.

An innovative and efficient solution, especially suited for large enterprises or organizations in high-risk sectors.

A platform that offers both detailed security insights and scalability through its cloud-first approach, making it a **strategic investment** for advanced threat detection and response.

Advantage vs Competitors

Competitor 1

- **Endpoint Telemetry:** PROVIDER excels in capturing detailed endpoint data, providing insights into encrypted communications and nuanced user behavior.
- **Resource Efficiency:** By leveraging a cloud-first model, PROVIDER offers a more resource-efficient solution compared to COMPETITOR-1's on-premises or hybrid models.
- **Adaptive Threat Detection:** PROVIDER's continuous innovation leads to better adaptation to emerging threats, particularly around insider risks

Competitor 2

- **Granular Endpoint Insights:** PROVIDER provides deeper visibility into encrypted data and granular **user behavior on endpoints than COMPETITOR-2.**
- **Cloud-First Efficiency:** PROVIDER's cloud-first approach ensures scalable and efficient data processing with minimal on-premises footprint.
- **Innovative Use Cases:** Continuously evolves to address new security threats, leveraging unique data insights beyond traditional UEBA capabilities.

GIGAOM

Area	Facet	PROVIDER	COMPETITOR-1	COMPETITOR-2
Market Segment	SMB	✔	—	✔
	Large Enterprise	✔	✔	✔
	Government	✔	✔	✔
Deployment Model	SaaS	✔	✔	✔
	On-Premises	✔	✔	✔
	Agent-Based	✔	✔	✔
Key Features	Data Masking	++++	—	+++++
	Automatic User Attribution	+++	++++	++++
	Distributed Endpoint Telemetry Collection	+++++	+++	+++
	API Cloud Integrations	+++	+++++	++++
	Managed UEBA Detection and Response	++++	++++	++
	Real-Time Entity Link Analysis	++++	++++	+++
	User Peer Group Analysis	++++	+++	++++
Business Criteria	Scalability	+++++	+++++	+++
	Flexibility	++++	++++	+++++
	Time to Insight	++++	+++	+++
	Ease of Use	++++	+++	++++
	Cost	+++	++++	++++
Emerging Features	Predictive Analytics	+++++	+++++	+++++
	Zero Trust Integrations	+++	—	++