Industry:
Banking & Financial Services (BFSI)

Location:
Middle East & Africa (MEA)

CASE STUDY

Redington DigiGlass Accelerates MDR Growth with Securonix

Challenge

Redington DigiGlass sought to rapidly establish a scalable Managed Detection and Response (MDR) and SIEM-led security services practice in a highly competitive, price-sensitive market. As a newer MSSP brand, DigiGlass needed a platform that could be deployed quickly, scale seamlessly, integrate with diverse log sources, and provide advanced threat detection—while also helping the business differentiate against large global MSSPs and system integrators.

Solution

Redington DigiGlass selected Securonix as the foundation for its MDR and SIEM services. With advanced UEBA, extensive out-of-the-box integrations, and strong engineering and leadership engagement, Securonix enabled DigiGlass to launch, scale, and mature its MDR offerings while delivering consistent security outcomes and business growth.

Benefits

- Rapid deployment and onboarding
- Advanced threat detection with UEBA
- Strong vendor partnership and enablement
- Executive-level visibility and reporting

Results

- 100% customer retention
- Growth from 750 EPS to ~15,000 EPS
- Competitive wins against global MSSPs
- Zero major audit non-compliances

The Challenge

Redington DigiGlass embarked on its journey to build a modern MDR and SIEM services practice at a time when the security services market was becoming increasingly crowded and competitive. Customers expected enterprise-grade detection and response capabilities, rapid onboarding, and clear return on investment, often at aggressive price points.

As a newer brand in the MSSP ecosystem, DigiGlass faced the dual challenge of building technical depth while also establishing credibility and trust with enterprise customers. The organization needed to demonstrate maturity quickly, particularly when engaging regulated industries and large corporate environments with strict audit and compliance requirements.

The team's prior experience with legacy SIEM platforms revealed persistent obstacles. Deployments were often complex, requiring significant effort to onboard log sources and normalize data. This slowed customer onboarding and increased operational overhead, limiting the ability to scale efficiently.

In addition, several incumbent platforms lacked consistent innovation. Limited R&D investment made it difficult to keep pace with evolving threat landscapes, forcing MSSPs to compensate with manual processes and custom tooling.

Vendor engagement was another critical pain point. While many vendors were highly responsive during the sales cycle, access to engineering and product leadership often diminished post-sale. This made it difficult to resolve issues quickly or influence product direction based on real-world MSSP requirements.

DigiGlass also needed a platform that could support a multi-tenant MDR delivery model. Managing multiple customers with different environments, log sources, and reporting requirements required flexibility, automation, and strong analytics capabilities.

From a business perspective, the team needed to differentiate against large global MSSPs and system integrators. Competing solely on price was not sustainable; DigiGlass needed to offer superior visibility, responsiveness, and service quality.

Enterprise customers demanded more than raw alerts. They required executive-level dashboards, SLA tracking, trend analysis, and clear communication of security posture, all without adding complexity to daily operations.

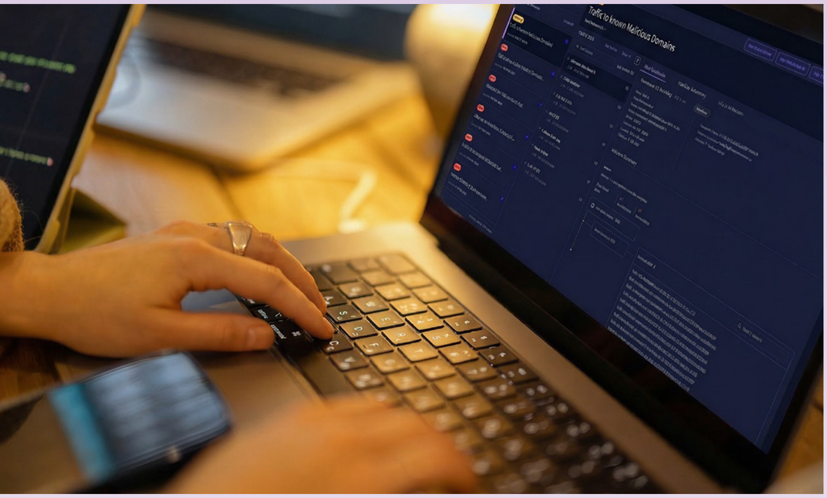
Audit readiness was another non-negotiable requirement. Customers expected consistent reporting and defensible detection capabilities that could withstand internal and external audits.

Scalability was also a concern. DigiGlass anticipated rapid growth and needed assurance that any chosen platform could scale from initial deployments to enterprise-grade ingestion without performance degradation.

The organization also required a vendor willing to act as a true partner, one that understood the realities of building and scaling an MSSP business, not just selling software licenses.

Ultimately, DigiGlass needed a platform that could serve as both a technical foundation and a business enabler, supporting growth, retention, and long-term differentiation in the market.

> **"Securonix has been instrumental in helping us build and scale our MDR business. Beyond the technology, the ease of deployment, strong engineering support, and leadership-level engagement enabled us to establish our footprint in the market and achieve 100% customer retention."**
>
> – Saikat Sen
> General Manager, DigiGlass, Redington



Key Challenges

- Complex and time-consuming SIEM deployments
- Limited R&D innovation in legacy tools
- Difficulty onboarding diverse customer log sources
- Lack of direct access to vendor engineering teams
- Need to differentiate against large global MSSPs
- Supporting enterprise and audit-driven customers

> **"Redington DigiGlass exemplifies how MSSPs can use Securonix's SIEM and UEBA capabilities, combined with strong partnership and enablement, to successfully scale and win in competitive markets."**
>
> – Bassam Sartawi
> Senior Director - MEA

Key Features Utilized

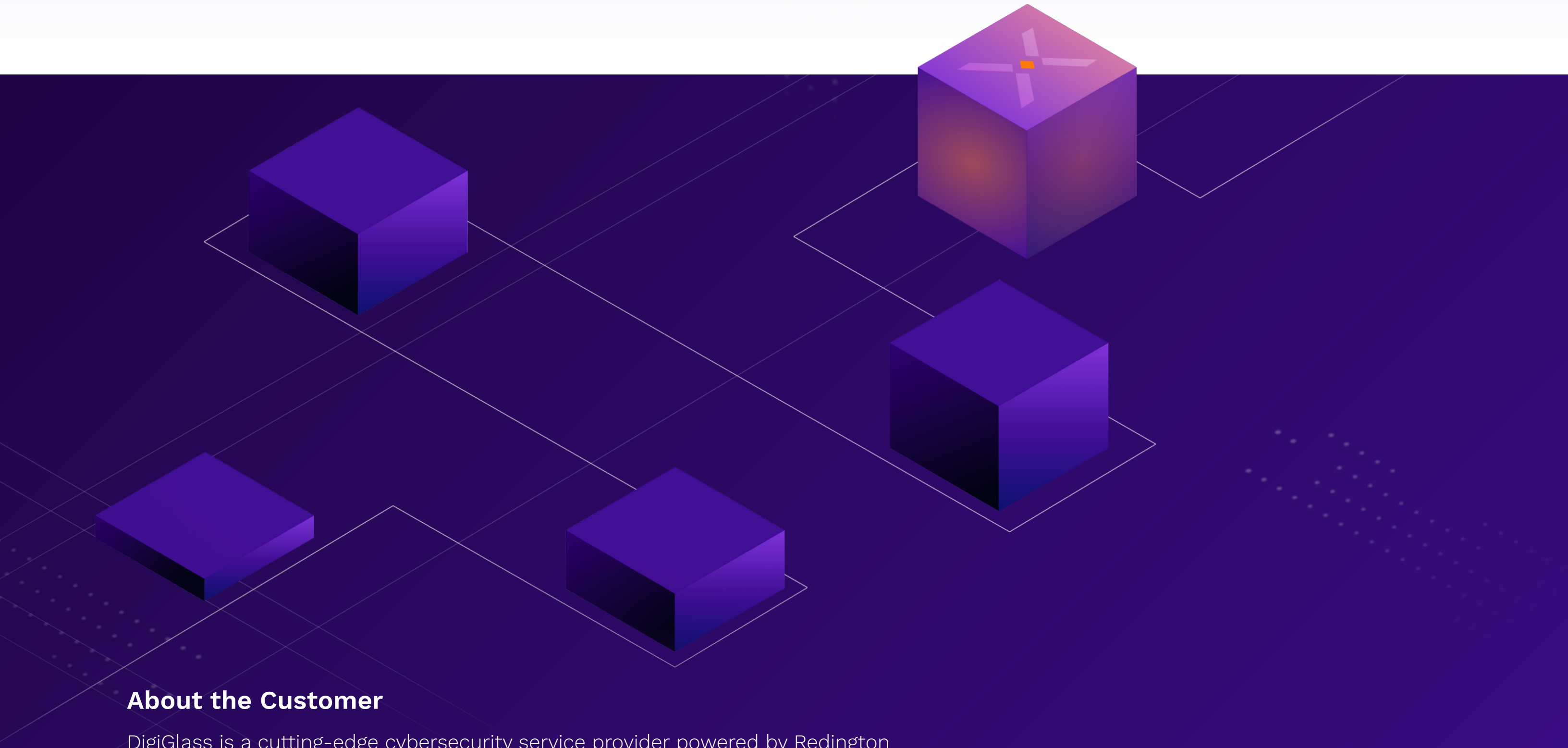
- Securonix **SIEM**
- **User and Entity Behavior Analytics (UEBA)**
- Extensive **out-of-the-box integrations**
- Threat intelligence integration
- High-scale ingestion supporting rapid growth
- Close engineering and enablement collaboration

Benefits

- 100% customer retention on the Securonix platform
- Rapid onboarding and faster time to value
- Enhanced threat detection and response visibility
- Executive-ready reporting via a single pane of glass
- Competitive wins against global system integrators and MSSPs
- Zero major audit non-compliances for enterprise customers
- Growth from 750 EPS to ~15,000 EPS, scaling toward TB-scale ingestion

Conclusion:

By choosing Securonix as the foundation of its MDR and SIEM offerings, Redington DigiGlass successfully built a scalable, differentiated security services practice. Securonix's advanced analytics, ease of deployment, and strong leadership and engineering engagement enabled DigiGlass to outperform established competitors, retain customers, and accelerate business growth across regions and enterprise segments.



About the Customer

DigiGlass is a cutting-edge cybersecurity service provider powered by Redington Gulf, a leading technology distributor in the Middle East and Africa. With DigiGlass, organizations can enjoy a comprehensive suite of cybersecurity solutions that cover critical areas such as threat management, network security, and identity and access management. Our team of seasoned cybersecurity experts works tirelessly to ensure that our clients have the necessary tools and resources to protect their digital assets from cyber threats. We leverage the latest technologies and methodologies to deliver customized cybersecurity solutions that are tailored to the specific needs of our clients.

About Securonix

Securonix is pushing forward its mission to secure the world by staying ahead of cyber threats, reinforcing all layers of its platform with AI capabilities. Securonix Unified Defense SIEM provides organizations with the first and only AI-reinforced solution built with a cybersecurity mesh architecture on a highly scalable data cloud. The innovative cloud-native solution is enhanced by Securonix EON to deliver a frictionless CyberOps experience and enables organizations to scale up their security operations and keep up with evolving threats. For more information, visit **securonix.com.**, or follow us on **LinkedIn** and **X**.

securonix