securonix

ALLANGRAY

Industry:
Banking & Financial Services

Customer Since:
2025

Number of Employees:
Approximately 1,450

Location:
South Africa

CASE STUDY

Allan Gray Strengthens Detection Coverage and Automates Response with Securonix

Allan Gray used its SIEM migration to simplify legacy detections, expand behavioral analytics and threat modeling, and automate response for high-priority incidents.

Benefits

- A more focused detection landscape built around relevant security use cases
- 81% of detection alerts identified as true detections, helping analysts focus attention on higher-confidence security activity
- Broad out-of-the-box detection content that reduced the need to recreate legacy policies
- Expanded behavioral detection through UEBA and complex Threat Models
- Detection-policy provides broad coverage of mapped MITRE ATT&CK tactics and techniques
- Automated handling and alerting for high-priority incidents
- Access to advanced security analytics capabilities that had previously been cost-prohibitive
- Responsive support from a globally distributed Securonix team
- Rapid migration from the existing SIEM platform in less than 45 days

Results

- Migrated the basic configuration from the existing SIEM platform to Securonix in less than 45 days
- Enabled approximately 845 Securonix policies, including 344 UEBA-based policies spanning eight different user and entity behavior analytics types
- Deployed 34 Threat Models to support detection of more complex attack patterns
- Strengthened MITRE ATT&CK TTP detection-policy coverage, with continued expansion underway
- Extended SOAR playbook execution to approximately 90% of incidents, automating alerting workflows while preserving analyst oversight
- Used Securonix out-of-the-box detection content to cover applicable legacy use cases and accelerate migration
- Established Securonix as the primary platform for security-focused telemetry and operations

The Challenge: Reassessing the SIEM Strategy

Allan Gray is a private financial services company in South Africa with approximately 1,450 employees. Its lean security team supports a substantial organization, making efficiency, visibility, and disciplined use of security resources critical.

Before moving to Securonix, Allan Gray had invested heavily in its Splunk environment. Over several years, the team had built extensive customized telemetry, alerts, and detection content and regularly tested its defenses through purple-team exercises. Visibility was already mature. The constraints were increasingly tied to economics, licensing, and access to additional analytics capabilities.

Allan Gray was moving from on-premise to cloud and explored the marketplace eventually settling on Securonix which delivered better value for money as well as offered more features. Rather than approach the situation as another renewal, the security team reassessed its SIEM strategy and went back to market.

With Securonix, Allan Gray gained greater control over which telemetry needed to enter the security analytics environment. Using Data Pipeline Manager, the team could segregate data according to its security value and reduced more than 100 GB of unwanted, non-security log data before it added unnecessary processing and storage overhead.

The team also wanted greater access to capabilities such as user and entity behavior analytics and risk scoring, which had previously been difficult to justify because of additional cost.

The Solution: A Structured Evaluation Led to Securonix

Allan Gray documented its requirements and evaluated Securonix alongside Exabeam, Microsoft Sentinel, Google security technology, its incumbent SIEM provider, and other options. Product capabilities, commercial considerations, Gartner research, customer references, and hands-on testing all played a role in the process.

After narrowing the evaluation to Securonix and Exabeam, Allan Gray selected Securonix. The proof of concept gave the security team an opportunity to test the platform directly against its requirements, while conversations with other customers provided additional perspective beyond product demonstrations and vendor claims.

The implementation became an opportunity to revisit the detection landscape rather than recreate the existing Splunk environment. Allan Gray provided approximately 250 legacy policies for review. Around 100 were identified as irrelevant or no longer required, leaving approximately 150 policies that needed to be addressed in the new environment.

Securonix out-of-the-box detection content provided coverage for many of those applicable use cases. Instead of carrying years of accumulated policy content forward unchanged, the teams could focus the migration on detections that remained relevant while using existing Securonix content where it met Allan Gray's requirements.

This approach also accelerated transition, with Allan Gray completed its migration of the basic configuration from the existing SIEM platform to Securonix in less than 45 days, while avoiding the need to recreate every legacy detection individually.

A More Focused and Capable Detection Program

Simplifying the Detection Landscape

Migrating from a heavily customized SIEM required careful decisions about what should move forward. Allan Gray had spent years developing telemetry, alerts, and detection content, so preserving every legacy policy would have added complexity without necessarily improving security.

Reviewing approximately 250 Splunk policies reduced the migration requirement to approximately 150 relevant policies. Securonix out-of-the-box content then provided coverage for applicable use cases, helping Allan Gray avoid rebuilding every legacy detection from the ground up.

The result was a more deliberate detection foundation built around current security requirements rather than the full history of the previous environment.

Expanding Behavioral and Threat Detection

The detection program has since expanded beyond the policies identified during migration. Approximately 845 detection policies are currently enabled, including 344 UEBA policies spanning eight different behavioral analytics types. Allan Gray now has behavioral coverage across multiple forms of user and entity activity rather than relying on static rules.

Allan Gray has also enabled 34 Threat Models. These models allow the team to connect related activity and evaluate more complex patterns that may be difficult to assess through individual detections alone.

Securonix detection policies, UEBA, cloud-focused coverage, and multistage analytics increased Allan Gray's measured cloud and cyber threat-detection coverage by **50%** compared with its previous SIEM platform.

These broader detection policies are also producing higher-confidence security outcomes, with **81%** of detection alerts classified as true detections.

Broadening MITRE ATT&CK Coverage

Current Securonix detection policies provide Allan Gray widespread coverage across the measured MITRE ATT&CK TTPs.

This is supported by hundreds of policies active, behavioral analytics incorporated through 344 UEBA detection policies spanning eight analytics types, and Threat Models managing more complex detection scenarios.

Securonix and Allan Gray continue to fine-tune existing detections and enable additional relevant policies, with further MITRE ATT&CK coverage forming part of that ongoing work.

Automating Response for High-Priority Incidents

Detection improvements have been paired with broad response automation. Securonix and Allan Gray designed and deployed SOAR playbooks that now support execution across 90% of incidents, moving defined response and alerting activities into consistent automated workflows.

These workflows help move priority incidents from detection into a defined response process without requiring analysts to perform every step manually. For Allan Gray's lean security team, automation helps preserve analyst capacity for investigations and decisions that require human judgment.

A Platform Built to Keep Evolving

Securonix now serves as Allan Gray's primary platform for security-focused telemetry and operations as the team continues to mature the environment. The migration has given the company access to behavioral analytics and risk-based capabilities it had previously wanted to explore more deeply.

The environment is also enabled with Securonix AI agents operating through the Agentic Mesh, providing a foundation for coordinated AI-powered workflows across the threat lifecycle while keeping analysts in control.

Relationships have also played an important role. CISO Werner Lunow described Securonix as responsive when assistance is needed and highlighted the team's ability to bring in the right expertise quickly.

With the initial migration largely reframed around relevant detection coverage rather than simple policy replication, the focus can continue moving toward fine-tuning detections, extending MITRE ATT&CK coverage, strengthening behavioral analytics, and applying automation where it can reduce workload for the security team.

"Moving to Securonix gave us the opportunity to rethink our detection program rather than simply recreate what we had in Splunk. The out-of-the-box detection content gave us valuable coverage from the start, while UEBA, Threat Models, and SOAR have helped us broaden our detection capabilities and automate the handling of high-priority incidents. We also have a responsive Securonix team behind us. When we need support, they are quick to engage and bring the right people in."

• **Werner Lunow** | CISO, Allan Gray

About the Customer

Founded in 1973, Allan Gray is an investment management firm headquartered in Cape Town, South Africa. The firm serves individual and institutional investors and follows a long-term, research-driven investment approach focused on identifying investment opportunities it believes are undervalued. Allan Gray is based in Africa, with offices in South Africa, Namibia and Botswana, and an affiliate office in Australia. Through its partnership with Orbis, Allan Gray also draws on global investment research and expertise. Allan Gray Proprietary Limited is an authorised financial services provider in South Africa.

About Securonix

Securonix is transforming security operations with the industry's first Unified Defense SIEM with Agentic AI, built to decide and act across the threat lifecycle with a human-in-the-loop philosophy. Its cloud-native platform unifies detection, investigation, and response, while enabling Sam, the AI SOC Analyst, and a productivity-based AI operating model for the SOC, so organizations can measure and govern AI by the analyst work it delivers. Helping enterprises become Breach Ready and Board Ready, Securonix delivers accountable, outcome-driven security operations at scale. Recognized as a Leader in the Gartner® Magic Quadrant™ for SIEM and a Customers' Choice by Gartner Peer Insights™, Securonix delivers trusted security operations for global enterprises. For more information, visit securonix.com., or follow us on LinkedIn and X.

securonix