Reach

Threat Analytics
Tools Rationalization
Product Licensing
ACME inc.
33,584
Total Number of Attacks
2,749
Number of Attacks Delivered
2,735
Number of Attacks Preventable
8X
The risk of your average individual
9.6%
Of your organization´s risk
99.993%
Reduction in attack anatomy risk
100%
Initial risk before security program implemented
Attack Anatomy
Malware
0.007
Residual risk after se program implen
Attacks Sent
Attacks Delivered
Risk Score
3500
3000
2500
2000
1500
1000
500
0
130
People in this group
1.2% of your organization

Case Study

ARISTOCRAT GAMING

Aristocrat is a global leader in gaming and entertainment, serving millions of players every day with innovative experiences. With a team of over 8,500 people spanning the globe, Aristocrat is driven by its mission to bring joy to life through the power of play. This commitment to innovation and customer delight is matched by a focus on sustainability and security, supported by Aristocrat's adoption of modern security architectures to ensure a safe and engaging experience for players worldwide.

The Security Control Challenge

As a cloud-first organization with 95% of operations in the cloud, Aristocrat recognized the need for an innovative approach in managing a dynamic and growing security environment. After completing a comprehensive, 9-month project to baseline and optimize controls across their cybersecurity infrastructure, they realized more than ever that the evolving nature of threats and the complexity of modern security stacks posed new challenges, making the adoption of a modern approach essential to optimizing their security posture since it would provide:

1

Scaling excellence:

Ensuring consistent configurations and reducing complexity across a diverse range of security tools.

2

Maintaining momentum:

Avoiding the inefficiency of repetitive, one-time efforts by developing a program for continuous validation.

3

Enhancing visibility:

Gaining deeper insights into how controls performed against both vendor best practices and the threats they were facing.

4

Strategic alignment:

Strengthening security as a business enabler under the "Protect and Fortify" initiative which is part of Aristocrat's broader five-year growth strategy.

Aristocrat's commitment to excellence in cybersecurity positioned them to adopt innovations to improve their security posture and further optimize their operations.

Solving the Challenge is within Reach

Aristocrat partnered with Reach to address these challenges and bring continuous posture management into their operations. Reach integrated with Aristocrat's tech stack—including identify, network, endpoint, conditional access and email— to enable a unified and automated approach to optimizing security controls.

> “
>
> Last year, we undertook a massive effort to 'Scale, Integrate, Optimize, and Automate' across our entire tech stack. It was a major success, leading to new deployments, expanded capabilities, and improvements across all our tools. But our biggest fear was having to repeat the entire process every year to ensure everything stayed optimized. Reach eliminated that fear by embedding continuous validation into our operations, giving us the confidence that our tools are always performing at their best without redoing all that work.
>
> Joe Masud
> VP of Cybersecurity Architecture & Engineering, Aristocrat
>
> ”

Why Aristocrat Chose Reach:

1 Enhancing visibility:

Reach fit well within their existing technology ecosystem which includes multi-cloud and a limited amount of on-prem.

2 Tailored security:

A POC highlighted Reach's ability to address specific challenges and enhance the team's efficiency.

3 Collaborative approach:

Reach worked closely with Aristocrat's team to define priorities and ensure meaningful outcomes.

Deployment Highlights:

1

Integrated across a multi-cloud environment and key security platforms.

2

Supported strategic alignment with the NIST CSF framework for security maturity.

3

Enabled security engineering and operations teams to streamline processes and collaborate more effectively.

sales@reach.security | reach.security

Business Impact

Since implementing Reach, Aristocrat has transformed its security operations and achieved several improvements:

1
Continuous Posture Management:

Reach automates monitoring and optimization of security controls, reducing the need for repeated manual efforts.

2
Operational Efficiency:

Reach streamlined workflows, helping the team act quickly on actionable insights.

3
Improved Visibility:

Reach enhanced understanding of attack surfaces through tools like NIST CIF compliance dashboards and MITRE alignment.

4
Cross-Team Collaboration:

Reach facilitated stronger ties between IT and security teams, ensuring alignment on tool management and objectives.

> “
> Reach has been a game-changer for our team. It simplifies the process of identifying what needs to be done and provides detailed, actionable guidance to get it done efficiently. It’s like having a trusted guide for optimizing our security posture, saving us time and reducing uncertainty.
>
> Joe Masud
> VP of Cybersecurity Architecture & Engineering, Aristocrat
> ”

Feedback from Aristocrat’s cybersecurity team underscores the value of Reach in simplifying complex processes and providing prescriptive guidance tailored to their environment.

The Road Ahead

Aristocrat plans to deepen its collaboration with Reach further embedding the platform into their environment, with a focus on:

1. Expanding integration with IT-managed tools to ensure comprehensive risk mitigation.
2. Exploring advanced threat modeling capabilities.
3. Continuing alignment with Zero Trust principles under their Identity and Access Management strategy.

Reach was founded to help organizations proactively find and fix hidden security blind spots. Traditional approaches surface issues, but stop short of fixing them. This leaves teams exposed, overwhelmed, and under-resourced. We built Reach to close that gap, delivering a platform powered by cybersecurity domain-specific AI models that reveal misconfigurations and underutilized capabilities across your existing security toolset; proactively remediate them; continuously validate that security controls are working as intended; and ensure your defenses stay aligned with your evolving environment and threat landscape.