

Case Study: Aspen Skiing Company

Security Analytics Challenges

Aspen Skiing Company (ASC) creates premium, sustainable and transformative experiences in recreation, culture and nature. Located in Aspen, Colorado, ASC owns and operates the world-renowned Aspen Snowmass resort, consisting of four ski areas: Snowmass, Aspen Mountain, Aspen Highlands and Buttermilk. In addition, ASC owns and operates the award-winning Ski & Snowboard Schools, the Four Mountain Sports chain of rental and retail shops, a unique blend of on-mountain food and beverage outlets, and the Little Nell Hotel Group.

The combination of guest wifi networks, storefront points of sale, onsite hotel accommodations, and widespread shared endpoints create potential exposure to a range of threat vectors that the small and efficient ASC cybersecurity team must protect against. They also contend with security awareness across an employee base that expands and evolves significantly each year during the ski season.

With expanding endpoint infrastructure and a growing investment in cybersecurity tools to protect its guests and employees, the ASC security team found itself exhausting its capacity to process and analyze all the security telemetry being generated. Data sources such as DNS, DHCP and EDR – while critical to threats such as phishing and other email based attacks – were evading analysis. To close this visibility gap, the team started investigating potential solutions.

Key Challenges

- Shared endpoints
- Seasonal staffing
- Limited resources
- EDR data visibility
- Threat investigation efficiency

Chronicle Security Analytics Platform

After evaluating various existing and emerging technologies in the security analytics space, the ASC team selected the Chronicle Security Analytics Platform (part of Google Cloud) for its distinct advantages in addressing their specific needs:

COVERAGE	Single platform and interface for analysis of all network and endpoint high volume telemetry
TIME TO VALUE	Pure SaaS model without infrastructure procurement, deployment and management overhead
COST/TCO	Fixed, predictable pricing model decoupled from data volume and usage levels
AUTOMATION	Continuous and automated correlation of threat intelligence with all telemetry



The biggest draws for us with Chronicle were the power of merging all the data, the speed of access, and the automated correlation.



Security Impact and Outcomes

THREAT VISIBILITY	<p>Several data sources critical to threat investigations were previously not consolidated and analyzed effectively. The pricing model and scale of the Chronicle platform have enabled visibility across all security telemetry for improved detection and investigation.</p>
SCOPE DISCOVERY	<p>With commonly encountered attacks such as phishing, the team can now investigate and instantly expand from a single phished user, search on the culprit domain and uncover other compromised users; and then lock those accounts or impose other remediation measures.</p>
EFFICIENCY GAINS	<p>In the past, uncovering the scope of an incident involved accessing multiple tools and interfaces (e.g., EDR, EPP, and firewalls) separately and manually stitching events across those data sources. The point and click user interface in Chronicle coupled with the automated merging and correlation of data have enabled ASC's small security team to do more by investigating incidents 2-3 times faster than before.</p>
SOC/SECURITY BUDGET OPTIMIZATION	<p>While security investments such as EDR were providing their primary value of inline protection, the telemetric value of these investments was not fully realized. The unique pricing model of Chronicle along with its analytics have enabled ASC's security team to maximize the return on their broader security investments.</p>