ARCTIC WOLF

CASE STUDY

CloudHesive

Company at a Glance

CloudHesive
cloudhesive.com

CloudHesive, an AWS Premier Consulting Partner based in Fort Lauderdale since 2014, specializes in cloud migrations, managed services, and AI-powered Amazon Connect solutions. Its flagship platform, ConnectPath CX, is an advanced CCaaS solution that delivers seamless omnichannel customer experiences. CloudHesive continues to lead in AI, machine learning, and data analytics while expanding globally. As a trusted AWS partner, it empowers businesses with innovative cloud technologies to help them succeed in today's digital landscape.

Challenges

- Alert fatigue resulting from insufficient context and time-intensive investigations
- Gaps in specialized security knowledge as the company grew to serve a wider variety of customers and use cases
- Information security policies that had not evolved with the cyber threat landscape over time

Results

- Accelerated time between investigation and remediation from weeks to hours
- 50% reduction in the number of alerts requiring triage
- 10X cost savings investing in Arctic Wolf versus building an in-house SOC

CloudHesive Cuts Alerts and Strengthens Security Posture with Arctic Wolf®

> **"We have seen a 50% reduction in the number of alerts that we've had to triage."**
>
> *— Patrick Hannah, CTO, CloudHesive*

It would be fair to say that CloudHesive, a cloud solutions and consulting provider that helps businesses optimize performance, enhance security, and drive innovation, has a "lead by example" business model: The company first pilots its ideas internally before offering them to clients.

"We prove success internally first, then use those lessons to demonstrate ROI to customers," said Patrick Hannah, CTO of CloudHesive.

This dedication to deep expertise and proven methods has propelled the company to success over the years. Exclusively providing solutions based on Amazon Web Services (AWS), CloudHesive has developed extensive experience in the cloud provider's ecosystem, earning 10 AWS Competencies and more than 200 AWS certifications. In addition to being named one of the fastest growing companies in South Florida, CloudHesive's timeline includes landmark moments such as winning the Deloitte Technology Fast 500 award and expanding to Latin America.

Among CloudHesive's lines of business is managed security services, which provides clients with advanced security tools either through reselling or direct services. CloudHesive's dedicated team delivers around-the-clock protection and real-time incident response, assisting customers with mission-critical security capabilities goals, such as compliance customized to various industries, data protection, and network security. But as CloudHesive grew, so did its customers, which meant extending these services came with new challenges.

"The security landscape has gotten more difficult for our clients, with evolving end user personas, methods, and vulnerabilities," Hannah said. "Many tech organizations, including us, start as tech-heavy, but as we grow, we build out our back office with teams that may not be security experts. Business and geographical expansion increased our risk footprint, and as a managed service provider (MSP) with a growing presence, we've become more vulnerable to targeted attacks, making it critical for us to invest in a security solution that unifies and strengthens our defenses."

Initially, CloudHesive used a different managed detection and response (MDR) solution, but it wasn't effective at filtering alerts. For its client security services, CloudHesive addressed a high-volume of triage needs; its 230 users could generate one million events over a seven-day period, sending teams into "analysis paralysis."

"We've seen cases where customers' web properties faced brute-force attacks, but only a handful — around nine — were actual alerts that required action," Hannah said. "The rest were raw events automatically triaged by the system. Without that filtering, it's easy to feel overwhelmed and assume the threat is worse than it is. Eventually, someone's going to get tired of manually sifting through the noise and miss something."

After months of looking into alternative MDR and XDR providers on the market, CloudHesive decided to become both a reseller and partner of Arctic Wolf.

"We determined that Arctic Wolf offered the ideal combination of features to protect our customers — it brought everything we needed together and integrated with the other services we were using," Hannah said.

More Visibility and Reduced Alerts Make Life Easier for CloudHesive's Security Teams

CloudHesive's approach to proving the value of solutions internally before recommending them to customers drove the company to optimize its implementation of Arctic Wolf Managed Detection and Response (MDR). It would do this by working closely with Arctic Wolf's Concierge Security® Team (CST). CloudHesive chose Arctic Wolf Managed Detection and Response not just for revenue potential as a reseller, but also to leverage the vendor's expertise in internal security monitoring and escalation. Instead of developing its own monitoring techniques, CloudHesive could rely on Arctic Wolf's established methodologies to efficiently detect threats and intervene only when necessary.

Arctic Wolf MDR monitors clients' networks, endpoints, identity, and cloud sources 24x7 so that it's poised to detect and respond to cyber threats. The CST serves as a dedicated point of contact when CloudHesive needs personalized security guidance and practical recommendations. The service uses advanced threat detection technologies, including machine learning and threat intelligence to actively search for and analyze potential threats. It also provides log retention and search capabilities, cloud monitoring, compliance support, and unlimited data collection.

A major benefit of Arctic Wolf Managed Detection and Response is its ability to integrate seamlessly with major infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) platforms. Arctic Wolf ingests telemetry data from multiple sources for broad coverage across environments without needing to rip and replace. This wider data collection enhances visibility into potential security threats, helping organizations monitor and protect all their critical surfaces.

This broader integration facilitates CloudHesive's ability to provide comprehensive visibility and monitoring across multiple clouds, ensuring a unified security posture for clients operating in multi-cloud environments. So, despite CloudHesive being a pure-play AWS solutions provider, the company can better serve customers using multi-cloud environments. This has been particularly valuable for Microsoft Office 365 and Microsoft Entra ID customers who experience significant SaaS platform sprawl, multi-factor authentication (MFA) complexities, and increasingly sophisticated phishing attempts within the cloud.

Additionally, CloudHesive can better meet clients' compliance needs around historical data. Arctic Wolf provides long-term log retention, allowing CloudHesive to retrieve critical audit logs that were no longer available from the original provider.

Because Arctic Wolf MDR is so effective at filtering and prioritizing alerts with rich context, CloudHesive has been able to reduce detection and response times — what once took weeks now takes days or even hours. Part of this is Arctic Wolf's security dashboard, which prioritizes and categorizes alerts, helping teams quickly identify, triage, and focus on the most critical threats while reducing noise. By swiftly identifying policy violations and abnormal user behavior with minimized effort for incident response, CloudHesive can conduct investigations faster. This efficiency also reduced recovery time and, in some cases, prevented incidents from escalating altogether, leading to a measurable improvement in security operations.

"We have seen a 50% reduction in the number of alerts that we've had to triage," Hannah said. "We like the funnel visualization because it clearly shows where we need to focus our time."

Because CloudHesive can deliver its MSP services with less effort, it has improved operational efficiency and profitability. "On a per customer basis, we probably save one or two full-time employees, just in terms of alert monitoring," Hannah said. "We can cover the gaps that the other MDR providers didn't fill, such as triage response."

Practicing Reactive and Proactive Security Simultaneously

When CloudHesive was ready to onboard Arctic Wolf Managed Detection and Response for its own operations, the team turned to Arctic Wolf's experts for guidance on how to implement it. CloudHesive had just acquired another company that came with its own suite of security tools, and the company needed to understand how it all fit together. Arctic Wolf helped CloudHesive determine the company's needs, find redundancies, and decide how to best evolve its security posture without undergoing a total system overhaul. This has helped CloudHesive with day-to-day security efforts and boosted the company's overall security strategy.

For example, after 10 years of using Microsoft Office 365, CloudHesive's information security policies had not evolved alongside service changes, and the company knew some fine-tuning was in order. Arctic Wolf helped identify opportunities to optimize these policies, providing deep domain expertise down to the application level. Unlike other vendors that charge high consulting fees and offer little guidance, Arctic Wolf brought strong, informed recommendations that made a meaningful impact on CloudHesive's security posture. CloudHesive was able to see value quickly while focusing protection efforts on its most important areas and users. This approach worked particularly well with CloudHesive's internal Virtual Desktop Infrastructure redesign project — by the time the team finished the migration, Arctic Wolf's security protections were already delivering results.

Arctic Wolf also helped CloudHesive strengthen its security policies by detecting region-specific challenges, such as VPN usage to bypass geographic restrictions, and clarifying what is and isn't permitted. With Arctic Wolf's insights, CloudHesive developed both technical controls and policy updates to address evolving security risks across multiple countries. Additionally, Arctic Wolf helped implement a structured exception process for its growing, geographically distributed workforce via a travel request system. If an employee needs to travel to another country for work, they submit a request form that helps CloudHesive correlate security alerts with confirmed user activity, reducing the risk of overlooked threats. By streamlining security processes, Arctic Wolf enabled CloudHesive to better balance risk management with operational efficiency.

"It's helping drive policy improvements, but more so it's helping drive well-developed process improvements that prevent us from overlooking potential risks, while, at the same time, reducing the overhead and managing those processes," Hannah said.

With proactive and reactive security, CloudHesive swiftly triages incidents, implements controls, validates threats, and updates policies. CloudHesive will continue to evolve its security posture by taking advantage of Arctic Wolf's quarterly reviews. These assess how CloudHesive's business and technology landscape are evolving so the company can make informed security adjustments and stay ahead of potential threats.

Internal and External Results Drive a Better Business

CloudHesive's partnership with Arctic Wolf has delivered remarkable improvements in visibility and alert management, reducing weekly alerts from hundreds to an average of nine, with only about five requiring feedback — allowing security teams to focus exclusively on genuine threats.

"The amount of noise that has been cut down because of Arctic Wolf's has been massive," Hannah said.

By leveraging Arctic Wolf's expertise, CloudHesive has closed security gaps within its own organization, strengthening its credibility. In selling the service externally, Arctic Wolf's cohesive solutions and pricing flexibility have helped CloudHesive provide clearer security guidance, including budget expectations, so customers can better plan their investments.

Additionally, engaging Arctic Wolf has yielded a tenfold cost advantage for CloudHesive compared to building an in-house Security Operations Center, all while minimizing downtime, enhancing compliance, and strengthening security policies across diverse environments.

As the company grows, Arctic Wolf's tailored security insights help them stay ahead of evolving threats, ensuring long-term resilience and continued success in an increasingly complex threat landscape.

Security Never Sleeps

CloudHesive is currently working with Arctic Wolf to enhance its single sign-on implementation across the organization, aiming for full coverage of all software and SaaS subscriptions. This effort builds on data-driven insights from the previous year, helping them address security, legal, financial, and intellectual property risks by ensuring comprehensive visibility and control over user access.

"We have definitely matured our security posture over what we had a year ago," Hannah said. "We've improved visibility, process, action policy, and the data we have to make decisions around how we need to influence user behavior, where we need to make investments, and what our true risks are as an organization."

ARCTIC WOLF