eSENTIRE

CUSTOMER CASE STUDY

Align Communications

Disrupting the traditional MSP model: Embracing security as a fundamental component of modern-day managed IT services.

- Managed IT, cybersecurity advisory services and infrastructure solutions
- Based in New York City and founded in 1986
- Eight offices spanning two continents

The Organization

Align Communications (Align) is a premier global provider of technology infrastructure solutions. For over 32 years, leading firms worldwide have relied on Align to guide them through IT challenges, delivering complete, secure solutions for business change and growth. Align is headquartered in New York City and has a number of customers in both the investment management industry and in the broader financial services sector.

Financial service organizations face an unprecedented level of cybersecurity risk. The volume of online attacks is growing, in part because the barrier to entry for cybercriminals is falling. There are more tools available on the dark web, easily available for anyone who wants to launch a cyberattack campaign. With many of these tools now offering sophisticated user interfaces and configuration options, attackers don't even need extensive cybersecurity knowledge.

These attacks disrupt financial services organizations' business, creating network incidents that can render services unavailable. A successful breach can damage a financial services company's reputation and cause financial losses.

The Challenge: A Cybersecurity Talent Gap

The ever-changing cybersecurity landscape and the continued growth of the connected business world means that the demand for highly skilled cybersecurity professionals will not wane in the foreseeable future. Further investment in the process and technology necessary to leverage a Security Operations Center (SOC) can be very costly–and many small and medium-sized businesses (SMBs) are not prepared to make the investment.

Managed service providers (MSPs) can offer the tools organizations need while also supplying the skilled individuals. Many MSPs provide affordable security services for their customers through partnerships like that with Align and eSentire.

Align, an MSP partner of eSentire's, deals in technology infrastructure solutions, managed IT services and data center deployments. It faced overwhelming demand for specialized cybersecurity services from concerned financial services customers that went beyond its ability to serve them with its own network operations center. Unlike many other MSP's, Align viewed the paradigm shift brought about by the cybersecurity phenomenon as an opportunity to evolve and invested heavily in creating a cybersecurity advisory services business unit. Align's cybersecurity team is comprised of subject matter experts in three distinct disciplines: regulatory compliance, security and technology, allowing them to address the multi-factorial nature of cybersecurity with a multidisciplinary approach.Align works with many alternative investment customers, including smaller hedge funds and family offices, says the company's CISO Alex Bazay. "They have highly sensitive data, making them potential targets for hackers."

Although these companies face the same cybersecurity threats as large investment banks, they don't have the same capabilities. A large bank can afford an internal SOC, with a minimum of five people offering 24x7 cybersecurity monitoring. There's no way a smaller investment operation can do that.

"They don't have adequate staffing capacity to achieve that level of security," he warns, adding that smaller investment companies focus on hiring revenue-generating roles rather than cybersecurity experts.

Align found itself in the position of de facto security manager for these companies. It needed to integrate a full suite of cybersecurity solutions, whether technological, operational or governance-related, into its service set, providing the same enterprise-class network monitoring capabilities that larger financial firms enjoy. It needed to do this efficiently, with a streamlined service that would be easy to manage and wouldn't take a huge internal investment.

The Solution

At the forefront of Align's cybersecurity technological offerings is a Managed Detection and Response (MDR) solution. Knowing this would be the crown jewel of its various cybersecurity solutions, Align carefully and methodically set out to find the best MDR solution for its customers and discerningly identified eSentire's MDR for Network service as the premier MDR solution that provides customers with unprecendentded visibility into what's happening within their infrastructure. Align was particularly impressed with the monitoring agents that are deployed within its customers' infrastructure to deliver data to eSentire. This data is applied to eSentire's proprietary machine learning techniques, which analyze the data and spot incidents that need escalating. Align can set the alerting levels for each customer according to each customer's unique needs. They then receive automatic notifications about network incidents with no human interaction.

As the principal component for eSentire's MDR for Network is a zero latency IPS/IDS designed to provide full network visibility, eliminating attack blind-spots that traditional technologies miss. Operating on a philosophy that all network signals from security appliances are potentially malicious until analyzed, eSentire SOC analysts leverage always-on full packet capture (PCAP) with a proprietary attack pattern and behavioral analytics engine to ensure every threat is detected.

More than relying on simplistic signatures or IOCs with meaningless alerts, their network information and human-driven forensic analysis enables rapid detection and investigation of attacks. This enables alerting and response to not only known threats, but unknown threats and suspicious behavior. Once a threat is confirmed, SOC analysts can disrupt malicious traffic on a customer's behalf and conduct post-attack forensics to aid in co-managed remediation to minimize the risk of business disruption.

> *eSentire combines different tools under the same umbrella. That's unique and valuable for multiple reasons...It drives costs down, you don't have to learn multiple solutions, and there's just one number to call.*
>
> *Alex Bazay*
> *CISO*
> *Align Communications*

The Result

Bringing eSentire on board has enabled Align's cybersecurity team to provide an unparalleled level of distinct cybersecurity services, including MDR, to its clients in a streamlined, automated way that keeps costs low and satisfaction high. The automated alerts, combined with eSentire's integrated services, mean that Bazay and his team only need to make one call when asking a cybersecurity question or escalating a client issue.

eSentire's SOC has adapted to fit Align's unique needs. A customer success manager conducts quarterly meetings with the Align team to highlight any emerging problems and brainstorm enhancements for their working partnership.

"eSentire has learned what's normal for our environment and developed playbooks for us, describing what to do in every situation," Bazay says. "That has helped us to shrink the response time after they detect something on the network."

eSentire's reporting capabilities have also helped to satisfy the regulatory pressures facing Align's customers. Align can now help its customers and augment its cybersecurity advisory services by producing periodic reports, with empirical evidence that serves well to satisfy auditors, closing a big gap in the regulatory compliance process. "That has answered a lot of questions, saving time and money," he says.

Bazay sees more opportunities with eSentire and Align through automation and expansion to endpoint monitoring and management next. He also sees possibilities to integrate eSentire's vulnerability management, Security Information and Event Management (SIEM) and active response offerings more closely into the Align service set.

The two companies are only just getting started.

> *You have a live analyst helping you 24x7x365. That really helps us give peace of mind to our clients and the regulators.*
>
> *Alex Bazay*
> *CISO*
> *Align Communications*

Crossing Paths Again

Bazay already knew eSentire well. He had chosen it as a service provider at his previous employer, a capital management company where he worked as CISO and CTO before joining Align.

When the SEC issued its guidance in 2015, he had taken responsibility for security at the capital management company and looked for a service to help it achieve its goals, which included gaining more visibility into its network.

He chose eSentire from a list of several vendors, due in part to the highly integrated nature of its tools and services. It offered a 24x7 network monitoring service, which gave him visibility into his network, along with an incident detection service and a rapid response capability.

Thanks to eSentire's SOC, he always felt taken care of. "You can always talk to somebody," he explains. When dealing with network security incidents for a high-value target on a daily basis, it's important to be protected.

His experience with eSentire was so good that he was all set to recommend the company when he arrived at Align and found eSentire was already a partner.

> *"In one solution you are achieving three big main objectives of your cybersecurity program. You're getting the visibility, you're getting the detection and identification of potentially bad traffic and you're getting response if anything is detected as malicious."*

Alex Bazay
CISO
Align Communications

Reach out to learn more.

Get Started

If you're experiencing a security incident or breach contact us 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.