








Global Executive Talent Leader Protects Core Business with CRITICALSTART MDR and Microsoft Defender for Endpoint.

CASE STUDY

AT A GLANCE

-  48 Offices in 23 Countries
-  3 Redundant Data Centers
-  Global Executive Talent Leader

CORE AGENDAS

-  Monitor Endpoints and Prevent Breaches
-  Secure Critical Assets Across Multiple Data Centers
-  Reduce Cybersecurity Workload
-  Employ 24x7 Threat Monitoring





In its 50+ year history, this global executive talent leader has enabled businesses across 10 sectors to connect with tomorrow's leaders.

But this organization has grown far beyond executive search. Through 40 unique practices, it now touches everything from board and CEO advisory to cultural transformation and succession planning.

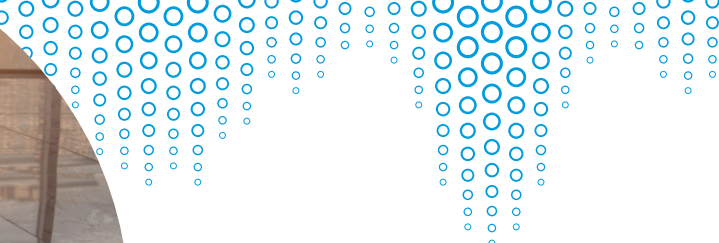
With such a broad portfolio, the only way the organization can gain its signature insight is through data—massive amounts of data. But with so much sensitive information, the organization realized it needed new thinking to protect one of its most critical assets from the multiverse of threats present in today's digital world.



Data Powerhouse

Due to the sensitive nature of this industry, the customer's name is redacted for security. But we can say that as a global leadership advisory and search firm, the organization thrives on the significant volume of data it collects to form the foundational core of many of its highly-sophisticated business units. The company has even developed its own internal search application to mine insight across both public and privately available information. The company database spans three redundant data centers and is shared through 48 offices in 23 countries.





“When we reevaluated our security, we knew that we did not want to just increase our headcount, but instead we wanted to focus on intelligence and expertise from the external security community to compliment what we were already doing,” stated the Global Information Security Manager for the firm. “It’s how we tend to operate as we have an outsourced security operations center (SOC) using Splunk in EMEA to analyze our data and we have consulting engagements with the vendors whose technology we use. But in the last two to three years, we’ve noticed that the focus has shifted back to endpoints. People are taking their devices

with them everywhere and it seems that the trend is for an attacker to compromise an endpoint and then move laterally throughout the system.”

“To address this, we’re now using Microsoft Defender for Endpoint (formerly ATP) to break out of the silos and monitor our endpoints wherever they may be,” he continued. “But it became noticeably clear from the start that we could not handle the volume of information produced by the endpoint detection and response (EDR) tool on our own. We knew we needed a Managed Detection and Response Provider (MDR).”



When we reevaluated our security, we knew that we did not want to just increase our headcount





CRITICALSTART's "Big Tent," yet Unique Approach to MDR

After evaluating their choices, the Security Director explained that the best option soon became clear. "CRITICALSTART was recommended to us by Microsoft as one of the top five partners for a Managed Security Services Provider (MSSP) including MDR," he shared.

"Our current software provider did not have the same 'sharpness' when working with Defender for Endpoint, and the refined level of CRITICALSTART's capabilities came into focus as we started working with them. They are platform agnostic, so we didn't have to worry about being locked in to one specific technology. But at the same time, they have an unparalleled expertise when it comes to Microsoft Defender for Endpoint. They are very sophisticated in how they handle the tool, the integration and the delivery platform, especially considering that Defender for Endpoint is still relatively new."

But this ISM was especially impressed with what he termed the "secret sauce" of CRITICALSTART in how it approaches alerts coming in from the EDR platform. While many MDR providers only flag critical or high alerts for investigation due to the sheer volume of alerts coming in, CRITICALSTART believes all alerts should be treated equally. Many advanced ransomware attacks may only trigger a low or medium alert, requiring that all alerts deserve proper attention. CRITICALSTART deals with high alert volumes by working with the customer to develop a trusted registry for alerts that indicate normal, routine activity. This unburdens the SOC team so they can focus on every other alert regardless of its stated priority level.

CRITICALSTART MDR for Microsoft Defender for Endpoint

Many organizations have teams that are very good at specific, siloed tasks. A team may be good at dealing with an alert relating to email, but lack knowledge when the alert is generated from another endpoint. CRITICALSTART analysts are actively engaged with Microsoft to stay fluent with the multi-spectral capabilities of Microsoft Defender for Endpoint. They can use Microsoft's cross-enterprise visibility to close gaps in coverage, leveraging threat detection and auto investigation capabilities with a radical reduction in alerts—no matter where and how a threat may appear across an enterprise.





Trending Alert Performance in the Right Direction

After a 6-8 week deployment, this CRITICALSTART customer was able to reduce false positive alerts by 90-95%. Forty-five days later false positives are almost eliminated. The ISM feels that he has far more visibility into what's happening with his network than ever before. "The platform itself is very intuitive," he said. "And I had access to a user-interface portal on day one. This puts all the information I need in one place, so I don't need to call or email the SOC every time I have a query. Watching the tickets and the kinds of responses from the SOC, it reassures me that we're catching the most probable malicious behavior we need to prevent."

"What this comes down to is that there was a definite risk vector through our endpoints," he continued. "We have now been able to identify the risk and address it through a workforce that alleviates the burden from my team. I have peace of mind knowing that these alerts are examined and escalated as needed, and that visibility is something I can take back to management as we determine how to allocate our resources in the future. I feel that working with CRITICALSTART puts us in a great position to keep our focus always on what's next."

Real-World Results: MDR in Action

The Security Director for this global leadership advisory and search firm shared a story of how the CRITICALSTART method protected his organization from a potentially serious breach.

"We had an endpoint that became infected from a USB drive," he explained. "It was setting off 40 or 50 alarms at one point. The CRITICALSTART SOC started notifying my team according to the predefined escalation chain. I called the person that had unintentionally infected the device and instructed them to get the device off the network. The SOC team performed an analysis and determined that we were able to stop the infection before it could propagate anywhere else, so that early detection stopped an issue that could have become much, much worse."

