Packaging Manufacturer Saves Time with MDR and Microsoft Security Solutions

Large manufacturer turns to Critical Start for increased visibility, faster response times, and actionable alerts

CASE STUDY

AT A GLANCE

- Industry: Manufacturing
- Number of Employees: Upwards of 4,500

CORE AGENDAS

Challenge
A packaging manufacturer needed more visibility into data, faster response times, and their own Security Information and Event Management (**SIEM**) capabilities.

Solution
The security team found convenient and comprehensive coverage with Critical Start's Managed Detection and Response (**MDR**) and Microsoft security tools.

Results
The security team saved time with actionable alerts and gained confidence in their security program with improved rapid data.

Manufacturing Industry Most Targeted

According to IBM, the manufacturing industry moved up to the most targeted industry for ransomware attacks in the last several years. This is largely due to the inability of manufacturing organizations to shut down for any significant amount of time. Because manufacturers want to prevent any disruptions, they're more likely to pay the ransoms. This further intensifies the need for an effective MDR provider that provides complete visibility and fast response times.

One packaging manufacturing company understood its cyber risks and took action by partnering with an MDR provider. This packaging company is headquartered in the midwest region of the United States with plants across the country. Internally, there is a team of three security professionals under a Manager of Technical Services. The security team relied heavily on Microsoft tools and other services to ensure they stayed ahead of emerging threats. However, it was clear they needed to make a change to their MDR provider.

Needed More Data Visibility and Faster Response Times from an MDR Provider

With their previous MDR provider, the packaging manufacturer faced several challenges. Data visibility was limited and it sometimes took up to 12 hours to get their data. The alerts themselves also brought problems. The security team often received too many alerts, with a lack of information in those alerts. Despite trying to suppress excessive alerts, the slow response times made it difficult to achieve the balance they wanted.

Additionally, this packaging company needed its own SIEM and wanted to use Microsoft Sentinel. They knew the value of Microsoft security tools, so they needed a change to fully capitalize on Microsoft Sentinel and E5.

How Critical Start Exceeded Expectations

When the packaging company's security team set out to find a new MDR provider, they took their time. The Manager of Technical Services wanted to ensure the company found the right partner for the long term and was comfortable with the 5-6 month process of evaluating and choosing an MDR provider. Part of the journey was identifying what the organization needed to enhance its current security program and maintain a better work-life balance for the security team.

Since they already identified the need for their own SIEM and wanted to go deeper with Microsoft security tools, finding a provider with Microsoft expertise was crucial. The security team was relying on their MDR provider to roadmap Microsoft Sentinel and Microsoft E5, as they had previously not used those tools.

To start their provider search, they talked to manufacturing peers, created a list of seven vendors, and quickly whittled those down to two. When they began having conversations with Critical Start, they quickly realized the increased expertise, convenience, and integration capabilities that Critical Start offered. After talking to existing customers and learning about the success they found partnering with Critical Start, it was clear that Critical Start was the expert MDR provider they were seeking.

The team also believed Critical Start went above and beyond by helping their organization perform a detailed security analysis across Microsoft 365, with subsequent roadmap and quick wins. From there, Critical Start swiftly onboarded the customer to Microsoft Sentinel, optimized log source configuration, and tuned detections leveraging out-of-the-box content. Based on their partnership with Critical Start and the above-mentioned security assessment + road map, they went on to purchase Microsoft 365 E5 licensing. Both organizations have been working together to roll-out the E5 security tools and get them ready for additional MDR services.

Ultimately, the biggest differentiator was Critical Start's MOBILE**SOC**® app. The security team found the most value in this functionality because it made the analysts' jobs more convenient. Critical Start's MobileSOC app is designed to provide complete transparency into an organization's alerts and the ability to action alerts immediately. Additionally, organizations experience real-time collaboration with the Critical Start Risk and Security Operations Center (**RSOC**) analysts. The MobileSOC app goes beyond convenience and allows complete incident management and proactive threat mitigation on the go.

> **MobileSOC is great for my analysts' work-life balance. It makes their jobs more convenient. This was our biggest differentiator.**
>
> - Manager of Technical Services

Team Gains Confidence and More Work-Life Balance

With Critical Start, this packaging manufacturer feels more confident in their security solution. The data the security team receives is valuable and fast, so the analysts can reduce attacker dwell time and only focus on actionable alerts. The team gained more confidence and achieved a better work-life balance.

They shared that partnering with Critical Start has been a game changer and allows them to sleep better at night, knowing alerts are actionable, there is 24x7x365 coverage, and the data provided is timely and valuable. Before Critical Start, this security team was unsure if they had the right solution to prevent or minimize a cyberattack. Critical Start provided the necessary coverage and tools to build their confidence in their security program.

Critical Start has done more than just raising the team's confidence, though. They actively save 15-30 minutes per alert from not having to do additional research and utilizing Threat Analytics Plugins (**TAPs**). Critical Start eliminates any threats quickly, greatly reducing the hours spent investigating and responding to incidents.

> **Adding Critical Start has been a game changer to sleep better at night.**
>
> **- Manager of Technical Services**

Operationalizing Microsoft E5 for Manufacturing

This packaging company continues to put its Microsoft security tools to good use as it strengthens its security posture. To help the company overcome mitigate security risks and stop business disruption, the company's Manager of Technical Services plans to maximize the return on investment (**ROI**) of the Microsoft E5 licensing features, including:

- Streamlining security operations and reducing the number of siloed security tools
- Improving data analytics
- Adding advanced threat capabilities to eliminate coverage gaps and help protect against sophisticated cyber threats like phishing, malware, and ransomware attacks
- Using cross-domain threat detection capabilities to make it easier to identify and address potential security risks

Critical Start's Microsoft security experts and managed services focused on applying Microsoft security best practices and high-fidelity threat detection with continuous tuning as new risks are identified, helping this packaging manufacturer feel confident they are optimizing the power of their Microsoft security investment for protection beyond the endpoint and using their Microsoft E5 license to its full potential.

To learn more about how Critical Start can help your organization simplify breach prevention and stop business disruptions, contact an expert today.

CRITICALSTART®

Don’t Fear Risk. Manage It.

For more information, contact us at:

https://www.criticalstart.com/contact/