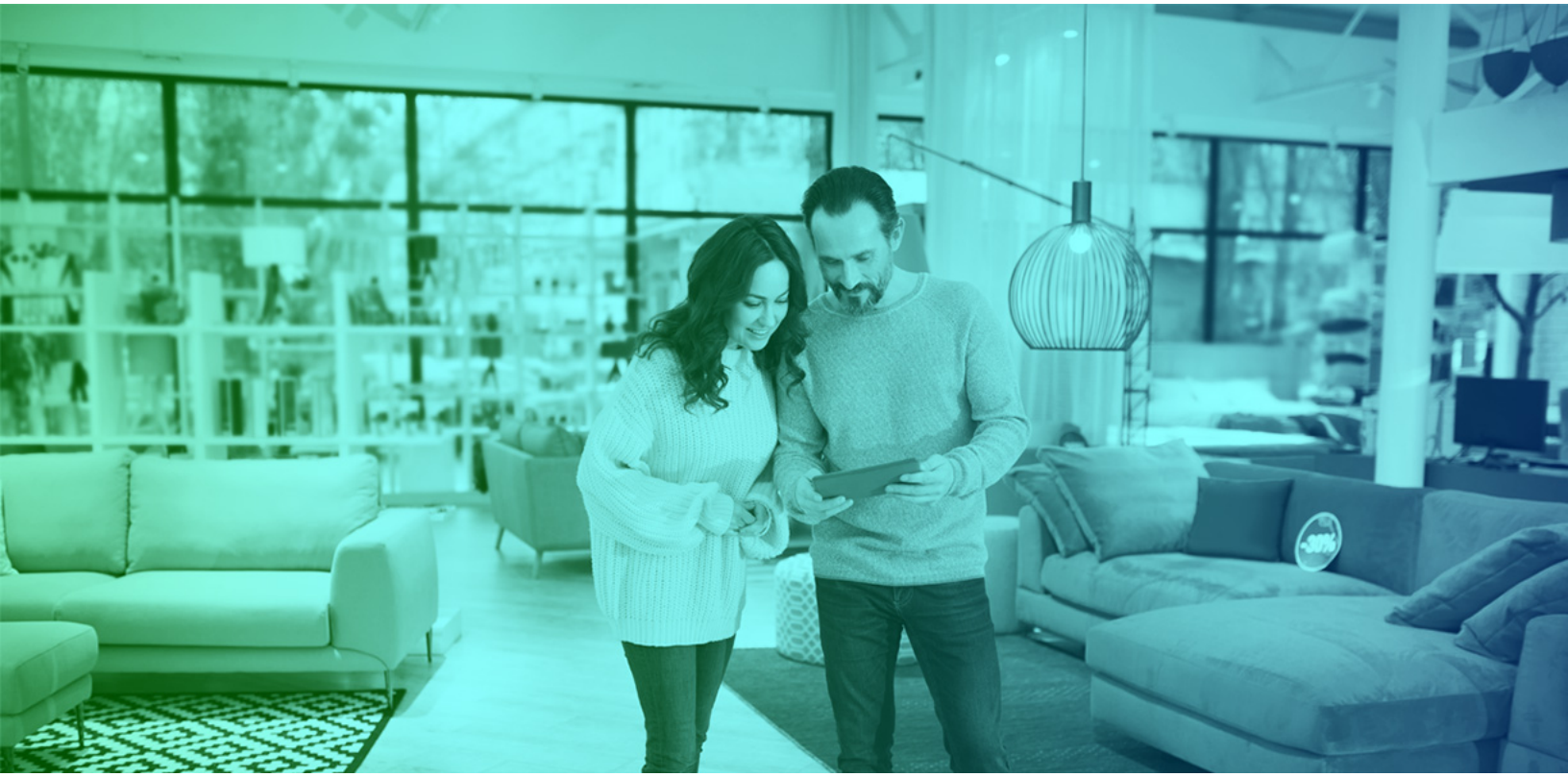

CASE STUDY ARMOR XDR+SOC

Family Focused Home Furnishings

E-commerce furniture retailer securely transitions to public cloud

COMPANY PROFILE

- **Industry:** Retail
- **Armor Solution:** XDR+SOC, Microsoft Sentinel
- **Technologies:** Azure

FAMILY FOCUSED HOME FURNISHINGS

E-commerce retailers face a range of challenges in today's competitive and ever-evolving digital landscape. Managing inventory, logistics, and fulfillment efficiently is crucial. Delays or errors in these processes can lead to customer dissatisfaction and lost sales.

Online commerce websites can be attractive targets for cyberattacks. IT leaders of these companies need to defend against threats such as DDoS attacks, ransomware, and phishing attempts, which can compromise customer data and disrupt operations. According to the IBM Security X-Force Threat Intelligence Index, the retail and wholesale industry was the fifth-most targeted industry in 2022.

When a leading Scottish furniture retailer embarked on plans to improve its e-commerce offering it needed a security partner to safeguard its transition to the public cloud.

Armor's technology-agnostic approach and deep integration with Microsoft supported the company in successfully migrating to the public cloud, bolstered by cloud-native security monitoring with Microsoft Sentinel.

BUILT TO LAST PRODUCTS

Over a period of 50 years, a Scottish furniture business has established itself as a brand leader in home furnishings. The family-owned firm boasts a significant turnover and employs hundreds of staff across ten concept stores.

The key to the brand's success has been knowing when to change and evolve. When the company celebrated its 50th anniversary with the appointment of a 'digitally minded' new CEO, it entered a new era, undertaking a major rebrand to reflect a new curated offering of furniture, accessories, flooring and interior finishes. And, whilst bricks and mortar stores remain crucial to the brand, it wanted a bigger slice of the available online sales.

With new premium stores rebranding across the country, the business wanted to ensure its online presence was as forward thinking as its new stores and engaged a digital agency to design and build a new ecommerce site, migrating from a hosted private cloud to Microsoft Azure.

NAVIGATING CLOUD MIGRATION CHALLENGES

Whilst the move to Azure would allow the furniture business to capitalise on Microsoft's many inbuilt cloud services, such as Azure Blob, SQL as a service and Azure Active Directory, it left the company feeling exposed. With a small IT team with no experience of Microsoft cloud, or the expertise or time to manage threats, the company was apprehensive about the risk of business interruption.

At the same time the business was onboarding Microsoft 365 and was particularly concerned about lateral movement attacks.

These worries were further exacerbated by a high profile, week-long cyber-attack on a competitor brand, which saw trading cease for a week and customer orders interrupted for almost six months. More recently, the industry was also rocked when an IT services company, which was a supplier to the furniture business, was subject to a cyber-attack that left 300 retailers unable to fulfill orders.

> "We fall into that small to medium enterprise bracket that is particularly vulnerable, a perfect target.
>
> IT Director

"The threat landscape in the retail sector is fast moving and constantly shifting," remarked the IT Director. "For example, you now have ransomware as a service, which has created out-of-the box software packages to launch a software attack. We fall into that small to medium enterprise bracket that is particularly vulnerable, a perfect target. Also, because of the nature of what we sell – bespoke furniture – it's a 13-week lead time for our products. If we are hit with a ransomware attack that timescale becomes significantly longer, and the likelihood is that the customer will simply cancel and go elsewhere. We have a responsibility to ourselves and our customers to make sure that doesn't happen."

FINDING THE RIGHT PARTNER

The company needed a partner capable of offering an Extended Detection and Response (XDR) function backed by a 24/7 Security Operations Center (SOC).

The IT Director explained “We needed somebody who not only understood the threat landscape, but who had the expertise we lacked in Microsoft Azure and could help us unlock the benefits of Microsoft Sentinel. The team at Armor immediately impressed us with the depth and breadth of their knowledge.”

Armor is a Microsoft Security Solutions Partner with advanced specialisation in Cloud Security and Threat Detection and a member of the Microsoft Intelligent Security Association (MISA).

Armor’s first step was to deploy and manage Microsoft Sentinel, Azure’s SIEM solution, as part of its Extended Detection and Response service.

As part of the deployment, Armor configured each of the following native log sources:

- **Azure AD**: insights into audit and sign-in logs
- **Azure Activity**: overview of subscription level events
- **Azure SQL Database:** audit and diagnostic logs
- **Azure Storage Account:** audited and diagnostic logs
- **Azure WAF:** web application firewall logs

Armor's team of solution and security engineers configured the data connectors to collect all the logs and telemetry from these sources, then overlayed Armor's propriety rule set. Since then, the role of Armor's Security Operations Center has been to fine tune those rules, adapting and changing them as the threat landscape evolves, giving the furniture business a continuous and complete picture of its security and risk posture.

Armor's SOC monitors the furniture company's environment for potential threat vectors and support the in-house team to navigate and deploy appropriate security controls and processes, ultimately supporting them in building a more effective and resilient IT infrastructure.

"Armor implemented all the automation rules according to best practice and really helped educate the IT team on the basic elements of Sentinel," said the IT Director, "what the automation rules do and, crucially, how to remediate any alerts which do come through. They held our hands through the entire onboarding process, their approach could not have been more comprehensive."

> "They held our hands through the entire onboarding process, their approach could not have been more comprehensive.
>
> IT Director

TRUSTING THE TECH

The furniture business now has a 'single pane' of enhanced threat visibility which, combined with Armor's 24/7 SOC is supported by the latest security intelligence to detect current and emerging threats. Armor's team works alongside the company to provide high-quality insight and mitigation guidance so that the small IT team can respond to incidents appropriately as they arise. And, as a result, the company has experienced a significant reduction in the meantime to detect and respond to threats, reducing the possibility of an attack.

Event and incident information is shared through Microsoft Sentinel's Workbook feature, with each event being analysed for indications of compromise. From phishing attempts and erroneous log-ins from strange locations, to fully fledged ransomware attacks, all can now be detected, isolated and remediated before they have an impact on business operations.

"Working with Armor has been an education," said the IT Director. "The team and I have learned so much about the threat landscape and our own knowledge and awareness is growing daily. They've taken the time to teach us and empower us to deal with incidents quickly and with confidence. For a business of our size, having access to that level of expertise is invaluable. The time was right for us to move to Microsoft Azure to support our e-commerce growth plans, but partnering with Armor has meant we've been able to do it safely and securely."

Successful Partnership Wins

- Faster incident response
- Reduction in people hours to detect and manage threats
- Enhanced threat visibility and coverage across network
- Elimination of threats before they cause damage
- Greater situational awareness amongst IT team
- Enhanced knowledge of threat landscape

ARMOR XDR+SOC

Armor's XDR+SOC solution combines cloud-native detection and response capabilities with our 24/7 team of cybersecurity experts utilizing our comprehensive, threat hunting and alerting library to deliver critical security outcomes.

Available on-demand and delivered in native ways that supercharge your security program to improve your risk and compliance posture. Our Security Operations Center adds a layer of cybersecurity expertise to respond to threats quickly and thoroughly to inform and guide remediation efforts.

ABOUT ARMOR DEFENSE

Armor is a global leader in cloud-native managed detection and response. As a trusted partner to more than 1,500 firms in over 40 countries, Armor offers cybersecurity and compliance consulting, professional services, and managed services. Armor's industry-leading experts leverage non-proprietary frameworks and a 24/7/365 SOC to help organizations tackle the complexities of cybersecurity and compliance at a cloud-scale.

WWW.ARMOR.COM

(US) +1 877 262 3473 (UK) +44 800 500 3167