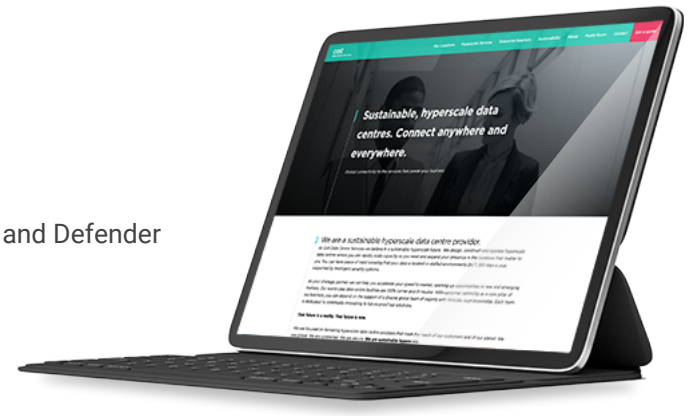
CASE STUDY ARMOR XDR+SOC

Hyperscale Data Centre Services

Enterprise data centre provider strengthens cybersecurity capabilities

COMPANY PROFILE

- **Company:** Colt Data Centre Services
- **Industry:** IT
- **Armor Solution:** XDR+SOC, Microsoft Sentinel and Defender
- **Technologies:** Azure
- **Website:** https://www.coltdatacentres.net/



HYPERSCALE DATA CENTRE SERVICES

Securing enterprise data centres from cyber attacks has become an increasingly formidable challenge in the modern digital landscape. With the rapid evolution of technology, the prevalence of sophisticated cyber threats continues to rise at an alarming rate. According to the Cybersecurity and Infrastructure Security Agency (CISA), in 2021 alone, there were over 4,000 reported data breaches, resulting in the exposure of more than 37 billion records. Furthermore, a study by the Ponemon Institute revealed that the average cost of a data breach for an organization in the United States reached a staggering $8.6 million in the same year.

These statistics underscore the pressing need for resilient security measures and strategies to safeguard enterprise data centers against the ever-persistent and increasingly sophisticated cyber adversaries.

As a global leader providing hyperscale and large enterprise data centre solutions, a robust, scalable and efficient cybersecurity solution is of critical importance to Colt Data Centre Services (Colt DCS).

When looking for a partner to bolster its threat detection and response capabilities, Colt DCS turned to Armor to provide a uniform cybersecurity platform across all its multi-national sites; implementing Armor's XDR+SOC solution as well as its VAPT programme to continually identify potential flaws.

SAFEGUARDING CUSTOMER DATA

Operating 16 state-of-the-art data centres in seven cities across Europe and Asia Pacific, Colt DCS has been designing, building and operating hyperscale and large enterprise data centres for more than 25 years.

Like all hyperscale data centre solution providers, Colt DCS' business model is dependent on customer confidence and being able to convince potential customers that their confidential data, and the data of their own customers, is in the safest of hands.

The vast amounts of sensitive and valuable information stored, processed and transmitted by Colt DCS for some of the world's largest organisations make it a potentially attractive target for cyberattacks. Therefore, effecting a robust and highly assured cybersecurity platform is essential to its operations and ongoing success.

NAVIGATING DISPARATE SOLUTIONS

As part of its commitment to delivering a sustainable hyperscale future for its clients, Colt DCS undertook a thorough evaluation of its cybersecurity posture.

The business found itself reliant on a multitude of disparate solutions, making threat monitoring and response less efficient. This fragmentation also meant that Colt DCS' IT teams did not have a single view of the threat landscape and associated vulnerabilities, instead having to sift through data from various vendors, which reduced response efficiency.

Guy Gibson, IT Infrastructure Manager at Colt DCS says: "What we realised is that we were often 'reactive' to threats. We had access to a huge amount of data, but no single view. It felt disjointed and that our current approach lacked structure and control."

Greater vulnerability assessment and penetration testing (VAPT) was also an area Colt DCS identified for improvement, requiring continuous monitoring and testing of the environment in order to expose potential faults and security weaknesses.

> "We had access to a huge amount of data, but no single view. It felt disjointed and that our current approach lacked structure and control.
>
> Guy Gibson
> IT Infrastructure Manager
> Colt DCS

Guy Gibson explains: "At the heart of what we were trying to achieve was more efficient threat detection and response; seeking a single source of truth solution that would provide us with greater global threat intelligence, control, testing and guidance whilst also facilitating large scale growth when required.

"We needed to work with someone who really understood the threat detection landscape and who could provide a solution that offered zero downtime to facilitate business continuity. The solution would also have to be compliant to data storage regulations across every country we are located in and, crucially, allow us to retain ownership and control of all data. In essence we needed security delivered in an unobtrusive way."

The cybersecurity team at Colt DCS was also looking for the reassurance of 24/7, 365 days a year platform security, as well as a trusted supplier and subject matter expert who could provide guidance, training and knowledge to their teams, helping them to grow.

"We wanted to learn and improve, so trust, communication and seamless integration between the new provider and our Incident Management Team (IMT) was also a must," Guy continues, "focusing on detecting and resolving Priority 2 (P2) incidents or higher with a well-defined process for incident resolution."

> "We needed to work with someone who really understood the threat detection landscape and who could provide a solution.

Guy Gibson
IT Infrastructure Manager
Colt DCS

FINDING THE RIGHT PARTNER

With all challenges and concerns identified, Colt DCS initiated a search for a cyber security partner who could provide an effective solution across its multinational sites.

Armor immediately impressed with its delivery capabilities, technical expertise and the comprehensive solution it proposed to simplify the detection and remediation of cybersecurity-based threats.

Guy explains: “We were highly impressed with the solution proposed by Armor. Other vendors/platforms were considered, but Armor came out top in terms of the technical solution, delivery and the flexible capabilities it offered.”

Armor project managed the implementation of Microsoft Sentinel, Azure’s cloud-native security information and event management (SIEM) system, as part of its Extended Threat Detection and Response (XDR) function to correlate logs and telemetry data from all sources, providing a complete view for threat identification.

A 24/7 Security Operation Centre (SOC) added an additional layer of cybersecurity expertise to Colt DCS’ defence, enabling swift threat response and guiding remediation efforts effectively.

As part of the XDR+SOC deployment, Armor configured each of the following custom and native log sources:

- **Azure AD**: insights into audit and sign-in logs
- **Azure Activity**: overview of subscription level events
- **Azure WAF:** web application firewall logs
- **Azure Firewall:** network security and application rule logs
- **Azure SQL Database:** audit and diagnostic logs
- **Azure Storage Account:** audited and diagnostic logs
- **Microsoft 365 Defender:** monitors and logs logons, file, process and registry events
- **Microsoft Defender for Endpoint:** security alerts on network endpoints e.g. laptops, tablets, routers etc.

Additionally included in the solution were Armor's advanced:

- **Analytics Rule Library**: including correlation alerting and threat-hunting rules
- **Security Dashboards and Widgets**
- **Configuration of Open Source and Commercial Threat Intelligence Feeds**

FURTHER IMPROVEMENTS

An ongoing VAPT programme was also deployed to identify any potential security flaws and enhance Colt DCS' DPS' overall security position.

As a second stage to this project, Colt DCS is now ingesting a new telemetry as part of its XDR solution – Microsoft's Defender for IoT. This will enhance its security further by protecting and monitoring internet-connected devices and endpoints within the data centre infrastructure to prevent cyber threats and vulnerabilities.

Guy explains: "The implementation of the solutions was well-managed and required minimal input from our internal teams. Not only was it straightforward, but the benefits were felt almost instantly. The solution from Armor has allowed us to have a better oversight of our global operations and assess the cyber landscape more efficiently.

"I haven't received a single complaint from my team. Everyone sees Armor as a force for good. Armor's solution has allowed us to shift our mindset internally, we are more proactive and focused. We can spend more time on access control rather than trying to process and understand vast quantities of data, which had become the norm.

"The solution from Armor has allowed us to have a better oversight of our global operations and assess the cyber landscape more efficiently.

Guy Gibson
IT Infrastructure Manager
Colt DCS

"There have been numerous threats and vulnerabilities picked up since the implementation of Armor's system. Issues that I think could have posed a real risk had our teams not been able to detect and remediate them. One example was the detection of a compromised email account which had the potential to be used for malicious means if not resolved swiftly. With this new solution we were able to be informed accordingly and take immediate remediation steps."

Shortly after the implementation of the Armor solution, Colt DCS expanded capacity across ten of its sites. Guy adds: “Having implemented the XDR solution ahead of this expansion undeniably meant that this process was much swifter. It was far less concerning to all involved than it would’ve been using our previous approach.

“Overall, the entire solution has helped us to achieve every single objective we set out to achieve on this journey; making the assessment of the cyber landscape a lot simpler for our team, threat detection and response quicker and more efficient, whilst continually facilitating our expansion.”

Successful Partnership Wins

- Unified cybersecurity provision
- Reduction in people hours to detect and manage threats
- Minimized false positives and reduced alert fatigue
- Elimination of threats before they cause damage
- Simplified and faster incident response
- Improved global oversight across Colt DCS’ locations
- Implemented with zero downtime and full business continuity experienced
- Enhanced access control
- Compliant with data storage regulations across every location
- Retained ownership and control of all data
- Accessible guidance, training and knowledge support

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