

CASE NOTE
**AGRICULTURE CLIENT
PROACTIVELY
PREVENTS CYBER-
ATTACKS**



www.risual.com



PUTTING SECURITY AT THE HEART OF EVERY ENGAGEMENT

A new client to risual in the Agriculture and Horticulture industry has recently engaged to kick start its Managed Service on-going support agreement. In early 2022, the client desired to have a focus on improving security organisation-wide ensuring all employees, data and devices are protected.

Initially, the client had an SIEM tool scanning the environment for security-threats, but found it quite challenging to turn the data into easy-to-understand actions.

Many people and organisations underestimate the threat and likelihood of becoming the next victim against cybercrime. The effects of cybercrime can be extremely damaging, and just as devastating as physical crimes, leaving a powerful impact on individuals and organisations globally.

Cybercriminals are targeting end users in increasingly sophisticated ways including advanced phishing attacks which are harder than ever to recognise (ransomware twists the power of encryption to work against you). These individuals are taking critical files hostage and social engineering attacks can take advantage of people who are just trying to be productive.



ADVANCED THREAT INTELLIGENCE

To ensure the requirements are met as part of the Managed Services agreement, the rMS team worked closely with the client to understand its desired outcomes from the potential security work. Following this conversation, a key outcome was to ensure that all data captured as part of the proactive monitoring can be used by internal staff to turn it into suitable actions.

risual implemented a Managed Security Operations Centre (Managed SOC), which advanced threat intelligence, vulnerability scanning and security analytics, to ensure incident prevention and detection. The Managed SOC is based on Microsoft Sentinel that can collect events cross all users, devices, applications, and infrastructure, both on-premises and in multiple clouds, coupled with risual's Microsoft accredited security expertise.



MICROSOFT DEFENDER FOR CLOUD



To further support this, risual used Defender for Cloud to help investigate the security posture of the client's environment. Defender for Cloud is able to identify vulnerabilities across machines, devices, and SQL server to help ensure the entire environment is monitored for potential threats.

According to Microsoft research, almost 60% of small and medium businesses said they didn't feel equipped to maintain cybersecurity hygiene, citing insufficient resources and lack of specialised security skills. Microsoft Defender for Business has been launched to bring the power of enterprise-grade endpoint security to small and medium businesses with up to 300 employees.

Microsoft Defender for Cloud adds a new application governance capability providing security and policy management to help identify, alert, and protect against risky behaviour across data, users, and applications.

PROACTIVE MONITORING TO PROTECT AGAINST CYBER-ATTACKS

Following this work, the risual client has already seen immediate benefits including unlocking accurate proactive monitoring. The client has a considerable amount of external facing applications accessible to the public, and since the Managed SOC engagement have been able to provide reassurance in all users that it is entirely safe, and if something were to occur, there are people working around the clock to prevent and protect. Further to this, the client will also see;

- Continuous proactive monitoring
- Assurance to internal and external users
- Visibility into entire network and environment
- Increased visibility of user activity within the environment
- Assurance external facing applications are secure
- Potential attacks and vulnerabilities are identified early
- Access to clear security recommendations
- Continuous suggestions for improvements

