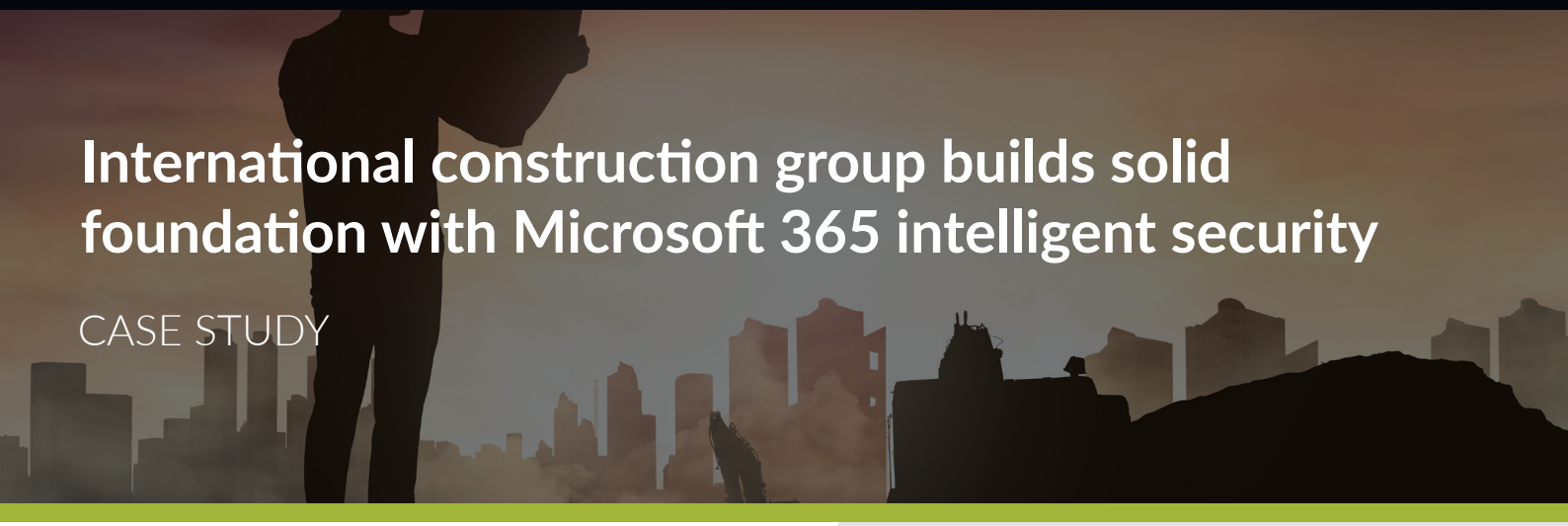
Threatscape

Microsoft Partner | 2020 Partner of the Year Winner Security and Compliance Award



International construction group builds solid foundation with Microsoft 365 intelligent security

CASE STUDY

Project Overview

With 1700 employees working on construction projects around the world, maintaining security and compliance for their mobile workforce was a huge priority for Sisk Group as they began their journey to digital transformation.

Working with Threatscape and Microsoft, Sisk began a security transformation across the business focusing on identity, application, email and device security. As part of this project, Threatscape and Sisk leveraged Identity Protection solutions in Azure Active Directory, Azure Advanced Threat Protection and Cloud App Security to secure corporate identities and mitigate the risk of compromised credentials being used by malicious actors.

Microsoft Information Protection solutions have also been deployed across Sisk controls to protect corporate data both on-premise and in the cloud.

Consultants from Threatscape's Microsoft Security Practice have worked with Sisk to provide a framework in achieving these goals and assistance in planning and deploying the recommended solutions. The outcome for Sisk is a reduction in time to detect and time to response for incidents, greater oversight and control over activities in their cloud resources and network, as well as gain confidence in their compliance and security.

SISK GROUP

Industry

Construction

Size

1000+

Country

Ireland & UK

Microsoft Solutions

- Microsoft 365 E5
- Azure Active Directory
- Azure Advanced Threat Protection
- Microsoft Information Protection
- Microsoft Cloud App Security
- Windows Hello
- Microsoft Defender Advanced Threat Protection

Threatscape Services

- Athena M365 Security Assessment
- Consultancy
- Design and deployment services
- Optimisation and remediation services

When John Sisk founded his construction business in Ireland in 1859, his vision was to provide exceptional construction expertise by training and motivating employees. One hundred and sixty years later, those principles are still important, but with approximately 1,700 employees working on projects all over the globe, mobile productivity and protection against data leakage and cyberthreats are more critical than ever. That's why John Sisk & Son chose the flexible, highly secure cloud services built into Microsoft 365.

John Sisk & Son is responsible for large-scale, diverse construction projects, such as Aviva Stadium in Dublin, the Limerick Tunnel, and the Dublin Convention Centre—places that draw thousands of people every day. As a result, it believes in maintaining the very highest standards of safety. Security is equally as important for the company's IT team as it is for employees working at construction sites.

Furthermore, security and compliance have moved to the top of IT's agenda, not only due to regulatory requirements like General Data Protection Regulation (GDPR), but also because of the ever-increasing presence of sophisticated cyber threats. However, mobility and agility are still key for employees travelling between work sites. With employees working across more than 100 locations, the Sisk IT team must balance security and compliance with a productive user experience.

> "The benefit that we're getting out of these security products of these security products is quicker response. We have a much better ability to pull together the data for our investigation process and respond to threats quickly."
>
> Stephen Parsons
> Head of Information Security

Seeing the cracks in the foundation

Looking to improve processes and reduce costs, Sisk began its digital transformation three years ago with Microsoft Office 365 and several other third-party cloud products. It moved employee mailboxes to Microsoft Exchange Online, making email more accessible to employees on mobile devices, and adopted Microsoft OneDrive as the standard application for storing and sharing files.

For a short time, the company relied on point solutions to secure its environment. However, as it began to investigate the best ways to implement GDPR compliance and undertook the process of becoming ISO 27001 certified for security management, the company decided to take a best-of-suite approach. It sought a solution that could provide a comprehensive security environment across identity, threat protection, and information protection. Sisk made the decision to deploy Microsoft 365 E5, which brings together Office 365, Windows 10, and Enterprise Mobility + Security. The cloud-based service includes the advanced security and compliance capabilities required to better safeguard client, employee, and company data.

"For me, a key driver for adopting Microsoft security was minimising security suppliers and solutions," says Stephen Parsons, Head of Information Security at Sisk. "When there's a possible breach, I don't want my team trying to correlate information from five or six different sources. Now if we see an employee saving a lot of information on a local machine, and some of it is sensitive and encrypted, we can effectively block access to that data until we've investigated what's actually going on."

Sisk wanted to move quickly to upgrade its security environment, so it brought in Threatscape, an experienced, Microsoft Gold Certified partner, to assist with the deployment and configuration of the security workloads. Working together, the team deployed Microsoft Azure Information Protection, Azure Advanced Threat Protection (ATP), Microsoft Defender ATP, and Microsoft Cloud App Security in about three months. Sisk also upgraded the use of Azure Active Directory (Azure AD) to include multifactor authentication, Conditional Access, and Privileged Identity Management during this short time.

Colin Reid, Commercial Director with Threatscape, explains how they were able to move so quickly, "Since these solutions are cloud-based, we could enable the security solutions and run pilot tests for a predefined set of users in less than a month, allowing us to plan a smooth roll-out across the company."

"Threatscape has worked hard to help us achieve what we needed by the dates we set," says Parsons. "It worked collaboratively with us so my team could learn how to deploy these products on their own as we roll out to other business units—which was incredibly helpful."

Building a more secure identity

With so many users working at remote job sites, identity management is central to Sisk's security needs. The Conditional Access and multifactor authentication features of Azure AD provided significant improvements to the group's security posture. Using Conditional Access, the Information Security team can configure permissions based not only on role but also on user location or device.

"Conditional Access is a big win for us from a usability point of view. When a user is on the corporate network and using a corporate device, we can provide a simpler access method but enforce more stringent requirements when they are called for," says Parsons. One challenge the team solved with Conditional Access was ensuring highly secure user enrolment to multifactor authentication. In order to mitigate this risk, Sisk has set up Conditional Access rules to block multifactor authentication registration from untrusted locations and devices.

"There has been minimal impact on our users with these additional signing precautions, and they've been helpful in changing the mindset around security," continues Parsons. "In the beginning of our deployment, we asked for volunteers for multifactor authentication and got very little response. So we set up a simulated phishing campaign, and that opened a lot of people's eyes to the need for this technology."

"With privileged access management in Office 365, we can add extra precautions when a team member wants to access Office 365 as an administrator and they need to request permission for a specific task and time frame," adds Parsons. "We haven't had any security incidents since we installed these capabilities. We've had alerts but are now able to react to them before we have an incident."

Keeping information more secure inside and outside company walls

To meet GDPR requirements, Sisk needed a way to classify and protect documents and emails containing sensitive information. Working with Threatscape, the GDPR team created four classification labels in Azure Information Protection with varying levels of protection based on the label selected. In addition, Sisk uses the Azure Information Protection scanner to automatically discover when documents in on-premises repositories need to be labelled.

Now, if an employee tries to send an email or attachment that contains words such as "credit card" or "national insurance number," they are prompted to mark the document as confidential or restricted. Parsons was pleased at the fact that Azure Information Protection was both easy for his team to configure and for employees to begin using right away. He says, "With Azure Information Protection, we quickly met our GDPR requirements without requiring extensive training or disrupting productivity."

Turning on the lights to erase shadow IT

Today, Sisk uses Cloud App Security to monitor and manage shadow IT, or applications used without the knowledge of the IT department, and to better protect data in the cloud. Parsons explains, "The minute we turned on Cloud App Security, we got a better understanding of how much shadow IT existed and how much of our data is stored within cloud apps, approved or not." His team could also see whether apps had the proper certificates or encryption levels. He continues, "Once we saw Cloud App Security in action, it became part of our daily operations to check alerts and see where people are putting their data online."

Cloud App Security also works together with Azure AD and Azure Information Protection to scan encrypted information and provide real-time data loss prevention and conditional access. For instance, if an employee uses Microsoft Teams to send a chat message containing sensitive information, that message can be blocked. Cloud App Security can also scan documents for sensitive information and require that they be labelled using Azure Information Protection.

With Cloud App Security, the IT team not only benefits from another layer of data protection, it can deepen its engagement with the business. "A lot of traffic in a particular app can highlight a key business process of which we were effectively unaware," notes Parsons. "Now we can go directly to the business and start a conversation around what they need and help them find a better tool to support their needs."

"Since these solutions are cloud-based, we could enable the security solutions and run pilot tests for a predefined set of users in less than a month, allowing us to plan a smooth roll-out across the company."

Colin Reid
Commercial Director, Threatscape

Inspecting the gaps in attack surfaces

Sisk has also deployed Microsoft Defender ATP and Azure ATP to improve its response to threats. "With Microsoft Defender ATP, we are able to see who has signed in from an endpoint and what they have done on the machine," says Parsons. "Azure ATP gives us information about network access attempts to help mitigate the potential impact of compromised identities." All of the information feeds into the company's security information and event management (SIEM) system and is monitored by the Security Operations Center (SOC) team. "The benefit that we're getting out of these security products is quicker response," explains Parsons. "We have a much better ability to pull together the data for our investigation process and respond to threats quickly."

When Parsons was testing Azure ATP, he set up a penetration test without telling his team, which had just begun using Azure ATP, or the SOC team, which didn't have access to it yet. During the test, Azure ATP detected the access attempts, and the IT team began investigating them immediately, whereas the SOC team never knew what was happening. "This test highlighted the need for us to provide the SOC with better information and alerts. Now, with Azure ATP and Microsoft Defender ATP, they can correlate all the data and get a clearer picture of what's happening," he says.

Fortifying what they've built

For Sisk, using Microsoft Secure Score to gain greater visibility into the state of its security posture across identity, devices, apps, data, and infrastructure has been a game-changer. Because Secure Score identifies top recommendations and improvement opportunities, the team can continually make incremental changes to improve the company's posture. "We can identify and share quick wins with the business, which gives the team a real sense of achievement," observes Parsons. "We can also make more informed decisions and ensure we're putting resources in the right places."

Having a better sense of the company's security posture also increases overall confidence for Parsons when pursuing new business opportunities. He explains, "I feel much more confident responding to RFPs and other security surveys, because we can see how our increased investment in Microsoft security is benefiting us and our clients."

Framing future opportunities

Sisk is moving into the next phases of its security configuration with support from Threatscape. It plans to focus more on security automation, orchestration, and response to speed responses and remove some of the burden from its security team. "We want to create policies to automatically isolate a user, require them to change their password, or use multifactor authentication to validate who they are based on the activity we see," Parsons explains. "We also have biometrics on most of our machines, so we'd like to set up Windows Hello and move toward a password-less environment."

For now, Parsons feels like he and his team can provide the peace of mind that company leadership needs to know that company and client information is better protected. Parsons concludes, "Our time to respond to security incidents is certainly much shorter, and our time to detect is decreasing. Knowing that we're proactively doing more removes a lot of pressure and stress from the team."

Why Threatscape

Threatscape is the trusted security partner of enterprise clients who rely on us to secure critical IT assets in over 100 countries around the world. Our mission is to create a secure and certain future for our clients. Keeping them protected so that they can go about their business is how we know we're delivering on our promise. To do this, our expert team of engineers and consultants use their skills alongside best-in-class solutions to protect, detect and respond to the growing threat of cyberattacks.

We are one of very few dedicated cyber security companies with a separate Microsoft Security Practice, and our expertise in this space is reflected in our status as the global Microsoft Security & Compliance Partner of the Year in 2020.

Want to know more about Microsoft security solutions? Talk to our team today.

0203 653 0000 (UK) or 01 901 7000 (Ireland)

FIND US ONLINE

@threatscape company/threatscape www.threatscape.com