CISCO SECURE

Case Study
Cisco Public

How a leading oil and energy services company delivers direct-to-internet access in challenging locations

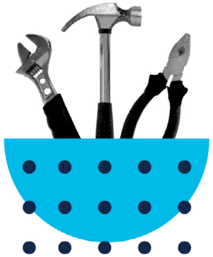
Organization
KCA Deutag

Headquarters:
Portlethen,
Aberdeenshire, Scotland

Users:
9,000 employees at 110 sites in 25 countries

Industry:
Oil and energy services

The bridge to possible



Objective

KCA Deutag needed a unified cloud security approach to secure endpoints and users, regardless of their location. The company also wanted to avoid the capacity limitations and expense of backhauling traffic to centralized locations and minimize additional hardware investments.

Solution

Cisco Umbrella

Cisco Duo

Cisco AMP for Endpoints

Cisco Threat Grid

Cisco Identity Services Engine (ISE)

Impact

- Improved the security of direct-to-internet access at multiple sites that had been difficult to secure, with no added latency
- Gained the capability to inspect encrypted traffic and to avoid risk with more granular controls
- Saw immediate results by blocking malicious traffic at DNS level
- Accelerated speed of deployment with customer success team
- Reduced risk by enforcing precise policies and controls around access management

Challenge

Securing remote, inaccessible locations

KCA Deutag is an international oil and gas services company that employs 9,000 people at 110 sites in 25 countries. As one of the world's leading drilling and engineering contractors, the company is focused on delivering safe and effective operations. But its diverse geographic locations make security a challenge, and backhauling internet traffic to central locations was expensive and negatively impacted user experience.

"A lot of our rigs are in remote locations, drilling in Sub-Saharan Africa or Arctic Russia. They're very challenging environments from a safety, accessibility, and connectivity point of view," says Mark McRitchie, KCA Deutag's IT and security architect. "So the security of the sites is quite important to us because they're very inaccessible and if there are any problems, it can take us a long time to get an engineer to a site."

To avoid placing appliances at every site and backhauling traffic to centralized locations, KCA Deutag sought a solution that didn't require an investment in additional hardware. The company needed a unified cloud security approach to consistently enforce policies and to secure endpoints and users, regardless of their location.

KCA Deutag lacked important capabilities that would enable the security team to discover and block hidden threats, reduce the risks of shadow IT apps, and simplify policy enforcement for user access across all sites.

"We were very keen to inspect as much traffic from our endpoints as possible, which included all the HTTPS traffic, and have more granular controls that we couldn't get at the DNS level," McRitchie says.

> "A lot of our rigs are in remote locations, drilling in Sub-Saharan Africa or Arctic Russia. They're very challenging environments from a safety, accessibility, and connectivity point of view."
>
> Mark McRitchie,
> IT & Security Architect, KCA Deutag

KCA DEUTAG

Solution

A unified, cloud-delivered solution that simplifies security

KCA Deutag liked the fact Cisco Umbrella offered a secure web gateway, cloud-delivered firewall, cloud access security broker (CASB) functionality, DNS-layer security, and interactive threat intelligence all in a single, integrated cloud service. The company particularly valued gaining complete visibility into internet activity across all users, devices, and locations, along with employing granular application controls to prevent risky activities.

“Being able to inspect HTTPS traffic, which we weren’t able to do before, is a massive benefit for us,” McRitchie says. “Umbrella’s secure web gateway is letting us look at the encrypted traffic that is going to our endpoints, whether that’s user-driven or something else on the endpoint that is accessing the internet.”

The simplicity of managing the solution was another key driver. McRitchie’s team felt Umbrella answered the question: “How can we make this simple and easy, improve the experience for our users, all while meeting our business requirements around data loss prevention?”

The organization saw additional benefits in Cisco’s integrated security architecture, which allows threat intelligence sharing between Umbrella and other solutions. This streamlines investigations and threat response because threats detected in Umbrella are automatically blocked across the environment.

“The fact that these products–Cisco Umbrella, AMP for Endpoints, Threat Grid, Email Security, and Stealthwatch–all interact with each other meant that we didn’t need to look at a series of point products and then have to build the integrations ourselves,” McRitchie says.

Deploying the solution during the pandemic presented challenges because KCA Deutag had to both accelerate the project and finish it remotely. They relied on the help of Cisco’s Cloud Security Customer Success team. “The Customer Success team made our rollout and deployment a lot smoother than it would have been without their help,” McRitchie says. “They expedited issues for us, enabled us to get timely access to support, and connected us with the product team so we could get more in-depth understanding of new features.”

> “The Customer Success team made our rollout and deployment a lot smoother than it would have been without their help.”
>
> Mark McRitchie,
> IT & Security Architect, KCA Deutag

Results

Securing the cloud edge

KCA Deutag uses Cisco Umbrella's secure web gateway (SWG) to inspect and control web traffic to ensure compliance with policies and block hidden threats. In addition to better visibility, advanced malware protection, sandboxing, decryption, and content control, the SWG provides the ability to apply granular application controls–all from one interface.

"For example, users can download, but not upload, from cloud storage. They can read their web email but can't send attachments," McRitchie explains. "And we have a more restrictive policy for our rig sites that prevents them from doing things like streaming media."

KCA Deutag can block applications at Layer 7 and then see the destinations of those applications. If a destination is safe, they can create a rule to allow the application access to that destination. "The cloud-delivered firewall with Layer 7 application visibility and control is quite good because we can now look at specific applications that we had problems with," McRitchie says. "We can create rules specifically for those apps, and Umbrella detects them regardless of which ports they use." Because this is done from Umbrella's single console, without requiring onsite appliances, the functionality is both effective plus simple to deploy and manage. Additionally, with Duo, KCA Deutag reduces security risks by enforcing precise policies and controls. Duo helps the IT team define and enforce rules on who can access what applications and under what conditions. It also allows teams to define access policies by user group and per application to increase security without compromising end-user experience. "The team finds Duo very easy to use," McRitchie says. "All that users need to do is approve sign-ins to push notifications on smartphones."

With direct internet access, KCA Deutag now enjoys faster access to cloud applications and workloads, instead of backhauling all traffic through the corporate network. Additionally, Umbrella helped the company reduce complexity and improve security. According to McRitchie, "We no longer need to break out traffic at every one of our sites. We can simplify our firewall rule set, which gives us an easier and quicker way to deploy templates for all of our sites as we onboard them to our new security platform," he says. "Umbrella has definitely improved our security posture by an order of magnitude from where we were before."

> "Umbrella has definitely improved our security posture by an order of magnitude from where we were before."
>
> Mark McRitchie,
> IT & Security Architect, KCA Deutag