Data#3 Customer Story

Main Roads Western Australia

Main Roads Western Australia Boosts Visibility and Security with Microsoft Defender for Identity Solution from Data#3

Data#3

mainroads
WESTERN AUSTRALIA

Data#3 | mainroads WESTERN AUSTRALIA

Project Highlight

“The project significantly uplifted our security posture. We are now able to get security signals from our on-premises infrastructure and feed that into our cloud security platform. This in turn allows us to rapidly identify and respond to any security risks.”

Andries Martins, ICT Security Architect,
Main Roads Western Australia.

Objective

As Main Roads Western Australia followed its modernisation roadmap, it determined that it was time to update from its existing on-premises Advanced Threat Analytics (ATA).

Benefits

- Increased visibility in the cloud across| on-premises identities and endpoint devices
- Real-time insights into suspicious activities
- 24/7 notifications
- Integrates into Security Information and Event Management (SIEM)
- Reduced administration burden
- Reduced risk
- Supports digital transformation goals

Solutions & Services

☑ Microsoft Defender for Identity

☑ Microsoft Defender for Endpoint

☑ Real-time security insight

☑ Integrated with SIEM

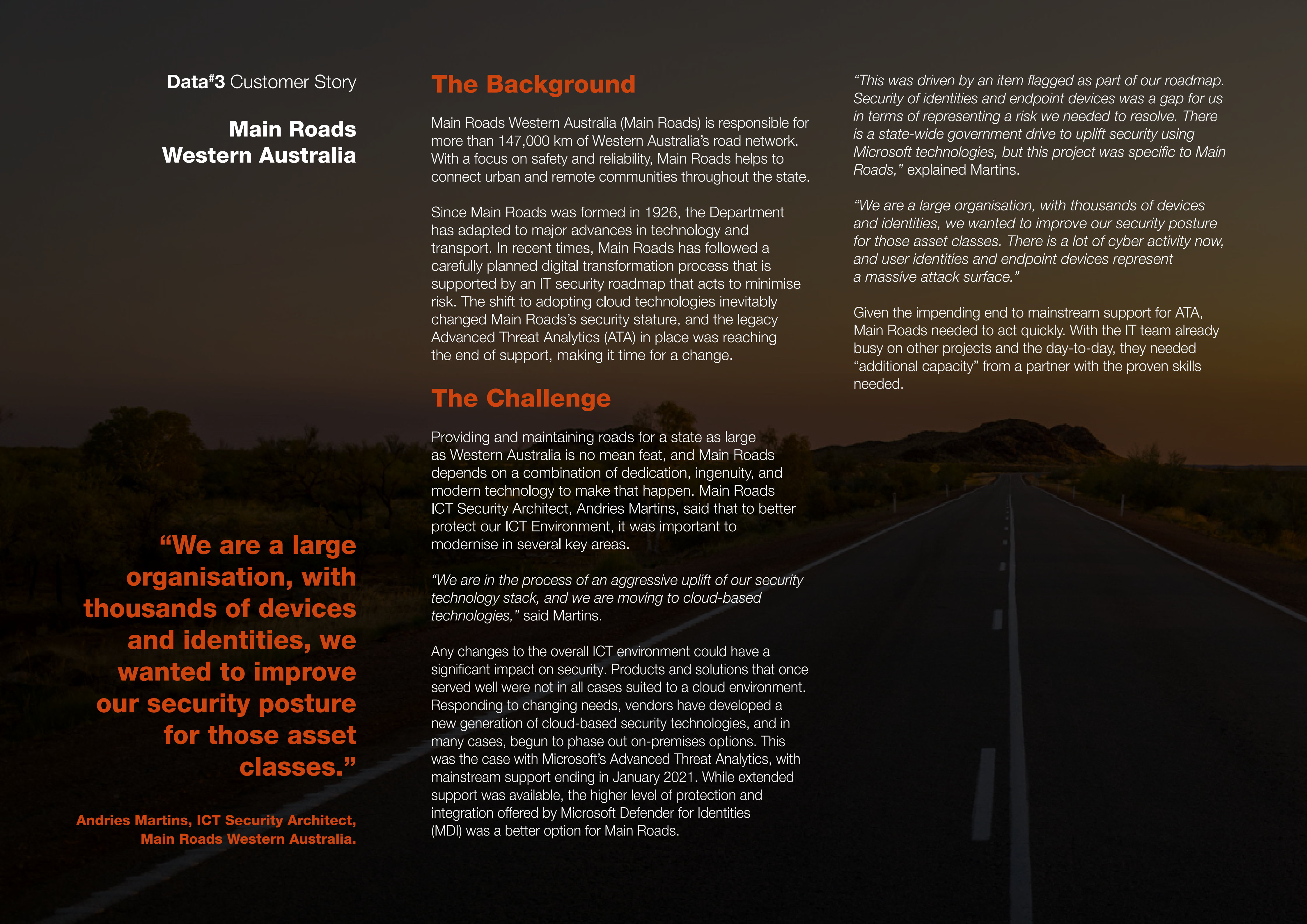
Approach

Main Roads Western Australia prioritised identity and endpoint security within its IT security roadmap, and after researching options, determined that transitioning from legacy on-premises ATA to cloud-based Microsoft Defender for Identity (MDI) would enable rapid threat detection. Additionally, Microsoft Defender for Endpoint (MDE) was also deployed to onboard endpoint device signals into the Microsoft’s cloud security stack for XDR Capability. With Data#3 already in place as the Department’s preferred Microsoft provider, it was logical to enlist their help.

Testimonial

“The technical expertise of Data#3 was excellent, and the impact to us in terms of the time we had to spend was minimal. They implemented the solution successfully and efficiently ran within the constraints of our processes.”

Andries Martins, ICT Security Architect,
Main Roads Western Australia.



Data#3 Customer Story

Main Roads Western Australia

> **“We are a large organisation, with thousands of devices and identities, we wanted to improve our security posture for those asset classes.”**
>
> **Andries Martins, ICT Security Architect, Main Roads Western Australia.**

The Background

Main Roads Western Australia (Main Roads) is responsible for more than 147,000 km of Western Australia’s road network. With a focus on safety and reliability, Main Roads helps to connect urban and remote communities throughout the state.

Since Main Roads was formed in 1926, the Department has adapted to major advances in technology and transport. In recent times, Main Roads has followed a carefully planned digital transformation process that is supported by an IT security roadmap that acts to minimise risk. The shift to adopting cloud technologies inevitably changed Main Roads’s security stature, and the legacy Advanced Threat Analytics (ATA) in place was reaching the end of support, making it time for a change.

The Challenge

Providing and maintaining roads for a state as large as Western Australia is no mean feat, and Main Roads depends on a combination of dedication, ingenuity, and modern technology to make that happen. Main Roads ICT Security Architect, Andries Martins, said that to better protect our ICT Environment, it was important to modernise in several key areas.

“We are in the process of an aggressive uplift of our security technology stack, and we are moving to cloud-based technologies,” said Martins.

Any changes to the overall ICT environment could have a significant impact on security. Products and solutions that once served well were not in all cases suited to a cloud environment. Responding to changing needs, vendors have developed a new generation of cloud-based security technologies, and in many cases, begun to phase out on-premises options. This was the case with Microsoft’s Advanced Threat Analytics, with mainstream support ending in January 2021. While extended support was available, the higher level of protection and integration offered by Microsoft Defender for Identities (MDI) was a better option for Main Roads.

“This was driven by an item flagged as part of our roadmap. Security of identities and endpoint devices was a gap for us in terms of representing a risk we needed to resolve. There is a state-wide government drive to uplift security using Microsoft technologies, but this project was specific to Main Roads,” explained Martins.

“We are a large organisation, with thousands of devices and identities, we wanted to improve our security posture for those asset classes. There is a lot of cyber activity now, and user identities and endpoint devices represent a massive attack surface.”

Given the impending end to mainstream support for ATA, Main Roads needed to act quickly. With the IT team already busy on other projects and the day-to-day, they needed “additional capacity” from a partner with the proven skills needed.

“We now get visibility on the security posture of the devices in real time, we get alerted on security incidents as they happen, and this allows us to get on the front foot in our response.”

Andries Martins, ICT Security Architect, Main Roads Western Australia.

IT Outcome

Replacing ATA with Microsoft Defender for Identity (MDI) and implementing Microsoft Defender for Endpoint (MDE) aligned well with Main Roads’s overall strategy. These cloud-based products offers considerable progression from their predecessors and it eliminates the need for on-premises infrastructure.

“Data#3 was engaged to assist in rolling out and implementing the project,” stated Martins.

Where previously, the IT team had a limited view of the desktops, the integration of MDI and MDE with the wider Microsoft ecosystem gave far greater enterprise-wide visibility. This led to setting rules and policies that were tailored to suit the unique Main Roads environment and users.

“The technology allows us to integrate with a bigger technology stack, which is important because we are getting visibility of what is happening across the organisation. Now we have a central place that we can view, manage, and implement additional rules, and we can be more proactive. There are additional features and functions that we didn’t have, and these help us to reduce the attack surface on the devices,” outlined Martins.

“We now get visibility on the security posture of the devices in real time, we get alerted on security incidents as they happen, and this allows us to get on the front foot in our response.”

The real time information is fed into Main Roads’s Security Information and Event Management (SIEM) software, so that the Security Operations team can quickly respond to any security event. This enables greater insights into the threat landscape, and the team is better positioned to pinpoint any vulnerabilities.

“We get various reports now – for example, we didn’t have reports on threat protection, real time vulnerability scanning for endpoints and device compliance. We can see vulnerable devices and address them. We can get reports for the entire organisation, or specific devices, whatever is needed. If a user has clicked a malicious link, we can drill down into details and see what has happened, whether any payload has been delivered or blocked, and work out the next steps, such as isolating any device before damage is done.”

Data#3 Customer Story

Main Roads Western Australia

"They were a very professional outfit to deal with, we never at any point felt things would not go well because they always seemed in control of the situation, and they provided very technically capable resources for the project."

Andries Martins, ICT Security Architect, Main Roads Western Australia.

Business Outcome

With a digital transformation underway, and with the unique challenges of preparing to support the organisation through the next phase of the COVID-19 pandemic, it was important that Data#3, as the chosen technology partner, was able to work independently. A good understanding of the government environment was also essential.

"Being government, we have a lot of processes to go through, but they easily coped with those processes. I was the technical escalation and coordination point but the project was driven by Data#3. There was quite a bit of work involved but dealing with Data#3's team of experts made it seamless for us to transition from one technology to the other," described Martins.

"They held workshops, scoped it up, got all necessary teams involved, and they guided us through it from a technical perspective, right from initiating the project to signing it off."

On the one occasion the project hit a minor snag, the Data#3 expert was "on-site within half an hour" and quickly had everything running smoothly. Through the process, it was important to ensure the Main Roads team was prepared to take on the new technology. An initial pilot program gave them the chance to work with MDI under Data#3's guidance, before the technology was implemented more widely.

"There was no disruption to our business operations. Data#3 did a full handover, and a bit of hand-holding to make sure that everything worked as it should, and made sure we were ready to manage and operate the new technology going forward," said Martins.

"They were a very professional outfit to deal with, we never at any point felt things would not go well because they always seemed in control of the situation, and they provided very technically capable resources for the project."

In spite of rising attack numbers hitting all industry sectors, Martins said that the greater level of insight and visibility achieved puts Main Roads in a better position.

"When we know more, the faster we can increase protection."

Conclusion

With the new MDI technology in place, Main Roads has another tool to protect its environment. To achieve a similarly smooth transition to the cloud-based security essential, Martins offered some important advice.

"Do the proper planning, and where possible, reach out to the tech experts in the field. We would not have been able to implement this in-house in such a short time frame and we didn't have the capacity in any case. As it was, the impact on us was minimal," said Martins.

Finding a partner that can take initiative, and work well with the Main Roads team, made the project a positive experience for Martins.

"The technical expertise of Data#3 was excellent, and the impact to us in terms of the time we had to spend was minimal. They implemented the solution successfully and efficiently ran within the constraints of our processes."

"Seeing it all work, and seeing how much value the software is adding, is a real highlight, and getting that visibility of security incidents into our SIEM product, our central security management tool, means we can manage alerts through it originating from our endpoint devices. We have lowered risk, which is what it is about," concluded Martins.

Data#3 and Microsoft

Since 1994, Data#3 has combined forces with Microsoft to help our customers adapt and grow. Today, we are Microsoft's largest Australian business partner with the highest level of competency across the Microsoft ecosystem. Our hundreds of accredited consultants are ready to help our customers deliver the digital future; from enhancing productivity and collaboration with Microsoft 365 and the latest Surface devices, to transforming business processes with Dynamics 365, to ensuring our customers get the most value from Azure cloud. Our scale and expertise enable our unparalleled support to customers selecting, deploying, managing and securing Microsoft applications, products and devices.

Data#3 | Microsoft