Data#3 Customer Story

Westminster School

Westminster School finds "missing piece" of security strategy with Data#3 and Silverfort

Data#3

Westminster School

Data#3

Westminster School

Testimonial

“Our position now is that we are very comfortable with our progress. We have gone from seeking a solution for gaps to being one of the most secure school IT departments around, and that is a testament to the work the team has done.”

Simon Matthews, Infrastructure lead, Westminster School.

Objective

Westminster School counts cyber security among the most critical responsibilities of its IT department. The school wanted to minimise risk exposure by strengthening protection around legacy applications and systems.

Approach

The school’s IT leaders attended a cyber security session at Data#3’s annual JuiceIT event, and realised they had found the ‘missing piece’ to secure their environment.

Solutions & Services

- ☑ Unified Identity Protection Platform
- ☑ Microsoft Azure Multi-Factor Authentication
- ☑ Identity Threat Detection and Response

Benefits

- **Visibility of privileged and service accounts**
- **Extended multi-factor authentication to legacy systems**
- **Discovery, monitoring and protection of service accounts**
- **Improved cyber security maturity and posture**
- **Reduced likelihood of harm to school community**
- **Reduced risk of financial and reputation impact**

Project Highlight

“When you get the best of both worlds, with a great product and great people, hands down it’s a winner. Data#3 and Silverfort have become trusted advisors on this matter.”

Simon Matthews, Infrastructure lead, Westminster School.

Data#3 Customer Story

Westminster School

“Where there were gaps, we knew that the Data#3 and Silverfort teams could help us realise the issue to resolve it.”

Simon Matthews, Infrastructure lead, Westminster School.

The Background

Nestled between the beaches and the vibrant city of Adelaide, Westminster School is a leading co-ed day and boarding school with around 1,300 students from early learning to year 12. The school is affiliated with the Uniting Church, and is known for nurturing students to achieve more in areas such as academics, sport, and the arts.

Technology plays a key role in school life, both in administration and in the classroom. A period of modernisation meant that much of the school’s IT environment has shifted to the cloud, with some legacy and on-premises infrastructure remaining, presenting some security challenges.

The Challenge

In any organisation, protecting users and assets against cyber attacks is of high importance. The Australian Cyber Security Council (ACSC) reported a doubling of reported cyber attacks in a two-year period to June 2022, with more than two in every ten organisations impacted each year. Breaches can have a significant financial and reputational effect on organisations, but Westminster School Infrastructure lead, Simon Matthews, said that the impact on individuals is, for educators, the greatest concern.

“Breaches can affect people very deeply. The vast majority of our stakeholders are under 18, so we need to do everything we can to protect our students. We have a lot of confidential information to protect, often medical details, and information around staff, and we take that seriously.”

Much of the school’s environment had been transitioned into the cloud, but the IT team was especially conscious that the remaining on-premises environment was limited in terms of identity protection, and this could have represented a risk. Finding an answer had proven problematic.

“It was the legacy on-premises infrastructure we were looking to secure, and we were not aware of a solution on the market that would cover not only the desktop, but also the whole range of common tools that threat actors use. They will target just about any service related to Windows.”

A cyber security truism is that ‘you can’t secure what you can’t see’, and here, too, there were obstacles to overcome. Visibility was limited in the legacy environment.

“We had a lack of awareness around what accounts we had that could be compromised, and service accounts were mostly where we saw problems. A lot had built up over years, staff would create a service, and over time, wouldn’t realise that the associated service accounts existed.”

While these service accounts in themselves were typically not related to sensitive data, hackers often exploit such accounts to find their way into an environment, spending months casing out an organisation and finding opportunities for lateral movement into other systems for months before they strike.

“Back in the day, we would measure threat using our firewall’s data to measure how many attempts were made. The landscape has since changed, with client devices in many places, and a completely decentralised environment. Threat actors work every device, every app, not just what is physically here.”

“As the threat landscape changes, we have to assume a breach and mitigate risk, by stopping lateral movement at that point to protect our people.”

Data#3 Customer Story

Westminster School

“We rely on partners like Data#3 to show us the best solutions available and introduce us to emerging vendors, and they did exactly that.”

Simon Matthews, Infrastructure lead, Westminster School.

IT Outcome

When the Westminster School’s IT team attended Data#3’s annual JuiceIT event, one of the partner presentations especially resonated with them. Security specialists from Data#3 and partner, Silverfort, spoke about addressing the security gap that can emerge in the area of identity protection when dealing with legacy environments designed for a more centralised landscape.

“We saw the cyber security presentation, and it was a real lightbulb moment. We looked at each other and went ‘yes!’. This speaks volumes about JuiceIT and the vendors that Data#3 brings into the space; the events ensure that Data#3 customers are exposed to the best emerging security solutions available through their partners, and that is part of why the partnership with Data#3 is so critical to us.”

After discussions with their Data#3, Westminster School elected to conduct a brief proof of concept to make sure that the solution lived up to its promise.

“We wanted to run it in house to see what it would do, and how it would function, and we ran some stats. We then fast tracked it because we knew we needed to close any gap in security around our on-premises infrastructure and legacy apps,” recounted Matthews.

The Data#3 and Silverfort team addressed a blind spot that was not protected well by existing identity and access management products. The proposed solution solves the technology challenge of enforcing secure authentication on all users, resources and protocols, both in on-premises and multi-cloud environments, thwarting efforts at lateral movement by malicious actors. To do this, it uses a unified identity protection platform that gives real-time protection against attacks that use compromised privileged or unprivileged credentials. It extends Microsoft Azure multi-factor authentication (MFA) to any sensitive resources, even to legacy environments that lacked the option for MFA previously.

The discovery capabilities of this technology were among the aspects that most impressed Matthews.

“It gave us exposure to service accounts, or accounts acting as service accounts, that we were unaware of. It also lets us enforce MFA that is policy based. The service account module has been critical to see the accounts we weren’t aware of and introduce controls around them, and we can do this by a granular process to make sure we aren’t breaking things elsewhere. Where there were gaps, we knew that the Data#3 and Silverfort teams could help us realise the issue to resolve it,” stated Matthews.

“It is very simple. The additional scope we get through insights gives us really useful information and helps us to troubleshoot daily.”

Data#3 Customer Story

Westminster School

“Our position now is that we are very comfortable with our progress. We have gone from seeking a solution for gaps to being one of the most secure school IT departments around, and that is a testament to the work the team has done.”

Simon Matthews, Infrastructure lead, Westminster School.

Business Outcome

For the majority of Westminster School users, there was no difference in their experience of logging on. Outside the IT department and leadership, none were aware that their security had been raised.

“There is nothing to put on our devices, no additional software on the servers, no integration pieces with SaaS or legacy applications. It just ties back into the simple all-in-one system, where we set policy to enable a type of traffic and block everything else,” explained Matthews.

“There was no user interaction, no apps deployed, no testing on client devices – just a few people may get prompted for higher access at times. No change management was needed.”

Matthews described a leadership culture at the school that is wholly supportive of cyber security measures, something he said is a “necessity” when facing a complex and sophisticated range of threats. This was helpful when proposing introduction of the new security solution, and the faith has been repaid.

“When we implemented the solution, we could instantaneously sleep better because we had that peace of mind. This is a last layer of protection to stop anything that gets past other layers – when it hits a server, for example, that stops the lateral movement.”

The level of discovery that the solution introduced, and the visibility that resulted, has given the IT team another vital tool as it strives to offer the school community the best possible protection.

“We use the Microsoft Cybersecurity Reference Architecture (MCRA) as our cyber security reference, where we go to help order our next steps. Microsoft suggests Silverfort as a method of closing gaps, which speaks volumes about their confidence. Everyone should be looking at consolidating their security stack, and given Microsoft invests $3 billion a year in security, we are confident in their recommendation,” explained Matthews.

“Our position now is that we are very comfortable with our progress. We have gone from seeking a solution for gaps to being one of the most secure school IT departments around, and that is a testament to the work the team has done.”

Data#3 Customer Story

Westminster School

“Data#3 and Silverfort have become and will continue to be trusted advisors on the matter of cyber security.”

Simon Matthews, Infrastructure lead, Westminster School.

Conclusion

As a very security aware educator, Westminster School had wrestled with the common challenge of identity protection around legacy and on-premises resources, so the security solution from Data#3 and Silverfort, caused a stir among the IT team. Matthews recalls a buzz of excitement at the end of the JuiceIT event session.

“We rely on partners like Data#3 to show us the best solutions available and introduce us to emerging vendors, and they did exactly that. They are a great company to have in Australia. We walked away saying that we didn’t realise there was a solution to this problem, and that we are grateful they have JuiceIT to bring the best technology to the industry.”

While Matthews gathers information from partner activities such as Microsoft webinars and Data#3 events, he recommends that other schools facing similar challenges make sure they talk to others within the sector to share experiences.

“Talk to other schools to get recommendations and reviews. Anyone can say how good their product is, but we can give real-life experience of working with Data#3 and Silverfort. If it is not in your security stack in the next six to twelve months, or not in your budget for next year, you’ve probably still got a big gap in security.”

The final piece of the picture, said Matthews, is working with knowledgeable partners who take time to understand your environment and the outcome you’re aiming for, and have their fingers on the pulse of emerging technologies.

“When we first learned about the new solution, there was a great buzz in our office, and we were all talking about it. When you get the best of both worlds, with a great product and great people, hands down it’s a winner. Data#3 and Silverfort have become and will continue to be trusted advisors on the matter of cyber security.”

Data#3 Customer Story

Westminster School

Data#3 and Silverfort

Data#3 partners with Silverfort to bring innovative solutions to our customers and help address identity security blind spots that attackers relish exploiting to help organisations deliver the digital future, securely.

Silverfort is the provider of the first Unified Identity Protection Platform that consolidates security controls across corporate networks and cloud environments to block identity-based attacks. Using innovative agentless and proxy less technology, Silverfort seamlessly integrates with all existing IAM solutions to continuously monitor all access of users and service accounts both cloud and on-premises environments, analysing risks in real time using an AI-based engine, and enforces adaptive authentication and access policies.

Data#3 | SILVERFORT