Borderless CS
CYBER SAFE TOGETHER

Microsoft Defender for Endpoint
Customer success story

CLIENT: **BRIMBANK CITY COUNCIL**

INDUSTRY: **LOCAL GOVERNMENT**

SOLUTION PROVIDER: **BORDERLESS CS**

SERVICE: **MICROSOFT DEFENDER FOR ENDPOINT IMPLEMENTATION FOR ADVANCED THREAT PROTECTION AND ENDPOINT SECURITY**

Overview

Brimbank City Council, a local government authority in the western suburbs of Melbourne, Australia, needed a solution to enhance its cybersecurity posture in the face of increasing cyber threats. The council was managing a wide array of endpoints and was particularly concerned with protecting its sensitive government data from emerging and sophisticated threats. To address these challenges, Brimbank City Council engaged Borderless CS, a leading cybersecurity company in Australia, to implement **Microsoft Defender for Endpoint** (formerly known as Microsoft Defender Advanced Threat Protection, or ATP).

The Challenge

Brimbank City Council faced several significant cybersecurity challenges that prompted the need for a more advanced, comprehensive security solution:

1. **Increased Cyber Threats**: The rise in cybercrime targeting local governments, especially ransomware and phishing attacks, necessitated the adoption of advanced threat detection and response tools.
2. **Diverse IT Environment**: Brimbank's IT environment included a mix of desktops, laptops, and mobile devices, all of which needed to be protected against security vulnerabilities.
3. **Compliance and Data Protection**: As a government organisation, the council was subject to strict data protection regulations, requiring proactive measures to ensure data integrity and avoid breaches.
4. **Lack of Visibility and Threat Detection**: The council's existing endpoint security solutions were not providing the level of threat visibility or actionable insights necessary to detect and respond to sophisticated threats in real-time.

The Solution

Borderless CS recommended **Microsoft Defender for Endpoint**, an integrated, cloud-delivered endpoint security platform that would deliver robust protection against modern cyber threats. The implementation involved setting up the solution across Brimbank's endpoints and integrating it with their existing Microsoft environment, including **Azure Active Directory** and **Microsoft 365**.

Key Implementation Features:

1. **Advanced Threat Detection**: Microsoft Defender for Endpoint uses AI-driven technology to detect a wide range of threats, including zero-day attacks, fileless malware, ransomware, and phishing attempts. The system continuously monitors endpoints for suspicious activity and provides detailed alerts for investigation.

2. **Threat & Vulnerability Management**: The solution included automated vulnerability scanning, providing the council's IT team with visibility into security gaps and the tools to remediate issues before they could be exploited by attackers.
3. **Endpoint Behavioral Analytics**: Defender for Endpoint utilised machine learning and behavioural analysis to detect anomalies that might indicate a potential security breach. This allowed Brimbank to catch even the most subtle indicators of compromise.
4. **Automated Response and Remediation**: In case of an attack or security breach, Defender for Endpoint allows for rapid automatic response actions, such as isolating compromised devices, blocking malicious files, and remediating the attack in real time.
5. **Centralized Dashboard**: The solution provided a unified security dashboard, giving Brimbank's IT team real-time visibility into the security status of all endpoints, with actionable insights and recommendations for improving the overall security posture.
6. **Integration with Microsoft 365 Defender**: Borderless CS integrated Defender for Endpoint with Microsoft 365 Defender, which allowed Brimbank to correlate endpoint data with email, identity, and cloud data for more effective threat hunting and investigation.
7. **Comprehensive Reporting and Compliance**: The platform also provided detailed compliance reports, helping Brimbank meet regulatory requirements and giving them greater control over their data protection practices.

Results

The deployment of **Microsoft Defender for Endpoint** by Borderless CS had a significant impact on Brimbank City Council's cybersecurity capabilities:

1. **Enhanced Protection Against Advanced Threats**: The council saw a noticeable reduction in successful cyberattacks. Microsoft Defender for Endpoint's proactive threat detection capabilities enabled Brimbank to quickly identify and neutralise security threats, preventing breaches and downtime.
2. **Increased Operational Efficiency**: Automated detection, response, and remediation processes reduced the burden on Brimbank's IT team, freeing them up to focus on other strategic initiatives. Real-time alerts and an intuitive management console helped streamline incident response times.
3. **Proactive Vulnerability Management**: With automated vulnerability management, Brimbank was able to identify and patch vulnerabilities in their endpoints before they could be exploited, reducing their risk surface.

4. **Improved Visibility and Threat Intelligence**: Microsoft Defender for Endpoint provided the IT team with detailed insights into endpoint activities, giving them better visibility into potential threats and helping them take swift, informed actions.
5. **Regulatory Compliance**: The solution enabled Brimbank to meet stringent local government cybersecurity standards and data protection regulations by providing comprehensive security reporting and audit trails.
6. **Peace of Mind for Remote Work**: As a result of the solution's advanced protection, Brimbank was able to confidently support remote working and mobile access, ensuring that its employees could safely access council systems from any location without compromising security.

Conclusion

The implementation of **Microsoft Defender for Endpoint** by Borderless CS significantly strengthened Brimbank City Council's cybersecurity posture. The advanced threat protection features, combined with automated response and real-time monitoring, ensured that the council's endpoints were well-protected against the growing risk of cyber threats. By partnering with Borderless CS, Brimbank was able to deploy a cutting-edge security solution that not only addressed their immediate cybersecurity needs but also set the foundation for secure, scalable operations in the future.

This success story highlights how **Microsoft Defender for Endpoint** can provide local government organisations like Brimbank with the security and visibility needed to protect sensitive data, comply with regulatory requirements, and safeguard against emerging cyber risks in an increasingly digital world.