BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

PATROL PRODUCT WHITEPAPER

BLACKHAWK ALERT PATROL

INTRO

Small and medium-sized businesses (SMBs) in Australia are increasingly adopting cloud services, such as Microsoft 365, to improve collaboration and productivity. With the increased reliance on cloud services comes the need for robust cybersecurity measures to protect data and prevent breaches.

As an SMB in Australia, managed cybersecurity for cloud data is an important consideration as cyber criminals are looking to target popular software such as Microsoft to weaponize and maliciously corrupt cloud data.

Cyber attacks are on the rise, and the financial impact on SMBs can be devastating. In fact, according to recent statistics:

- Cyber attacks on SMBs cost an average of $276,323 per incident.
- 60% of SMBs go out of business within six months of a cyber attack.

As more and more businesses are moving to the cloud, it's important to ensure that sensitive data is protected. Managed cybersecurity solutions for cloud data provide this protection, giving businesses the peace of mind that their data is safe.

WHAT ARE MICROSOFT MACROS?

Microsoft Office files can contain embedded codes (known as a macro) written in the programming language. A macro contains a series of commands that can be coded to automate tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity. However, a cyber criminal can also create macros to perform a variety of malicious activities.

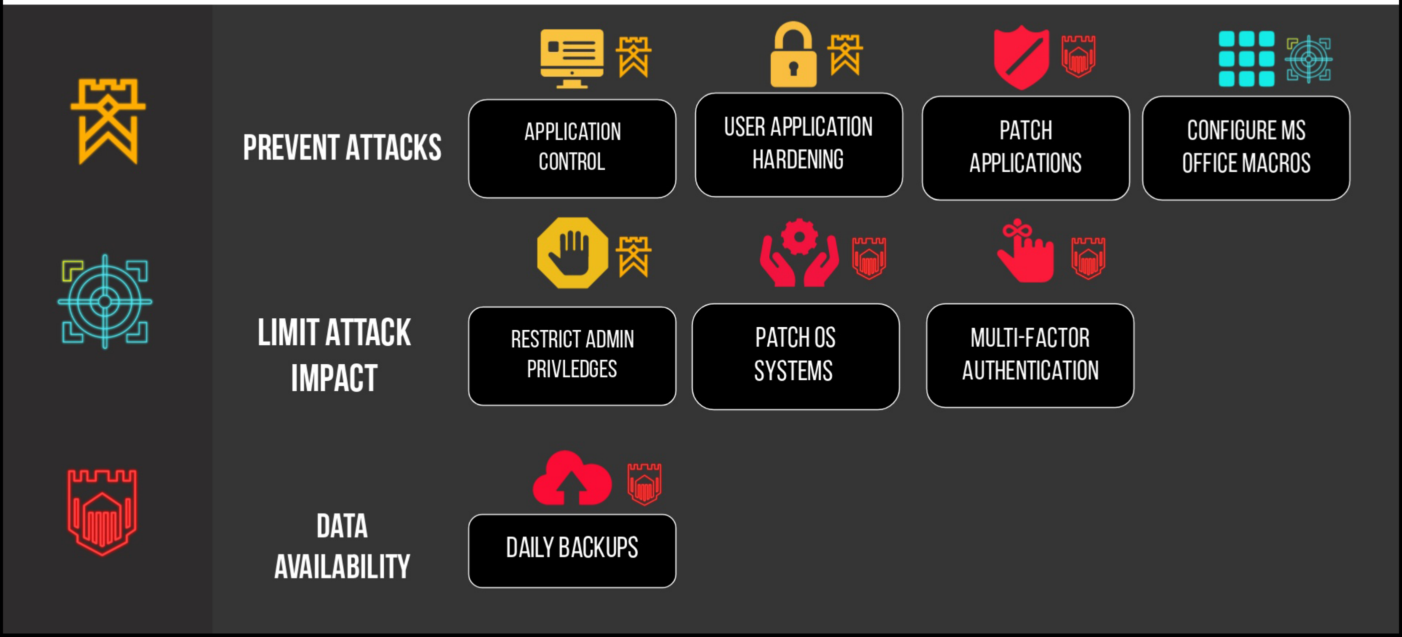
PATROL DEFINITION

Blackhawk Patrol is a managed cybersecurity solution for cloud Microsoft365 data.

Blackhawk Patrol provides comprehensive protection against potential threats, as well as expert support and guidance from experienced professionals. This means that businesses can focus on their core operations, knowing that their security is in good hands.

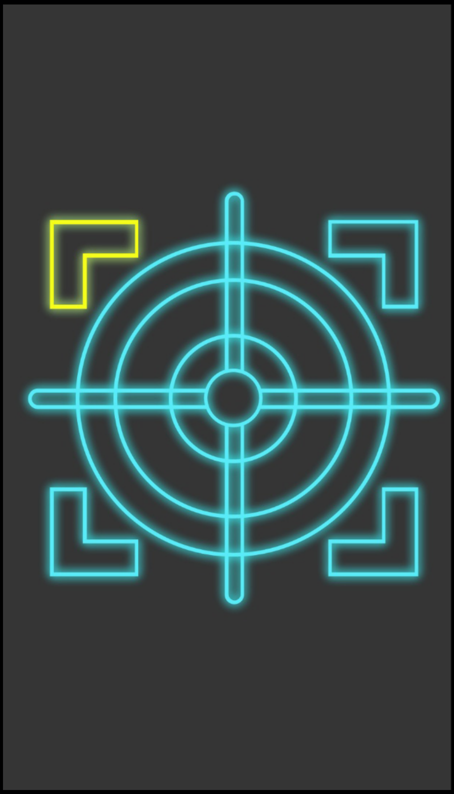
One of the biggest benefits of using cloud services like Microsoft 365 is the ability to access data from anywhere and on any device. This flexibility and convenience can greatly improve the efficiency of SMBs, but it also means that they are more vulnerable to be targeted. Cybercriminals can easily target remote data and gain access to sensitive information, such as customer and financial records. Blackhawk patrol is designed in alignment with the Essential Eight to configure and establish hardened Macro settings.

ALIGNMENT TO THE ESSENTIAL EIGHT FRAMEWORK



PREVENT ATTACKS	APPLICATION CONTROL	USER APPLICATION HARDENING	PATCH APPLICATIONS	CONFIGURE MS OFFICE MACROS
LIMIT ATTACK IMPACT	RESTRICT ADMIN PRIVLEDGES	PATCH OS SYSTEMS	MULTI-FACTOR AUTHENTICATION	
DATA AVAILABILITY	DAILY BACKUPS			

KEY FEATURES



BLACKHAWK PATROL FEATURES

Harden Microsoft Macros:
Setting controls that are trusted, disable and block malicious files.

Lock Security Settings:
Disable user access allowing change of Microsoft365 security settings

Security Operations Centre:
Continuously monitors for and mitigates threats aimed to target your Microsoft environment.

Log & User Behaviour Analysis:
Data records on both incidents and user behaviour

Internal & External Threat Detection:
Monitors for threats originating within & outside your Microsoft environment

Blackhawk Patrol minimises risk and thwarts cyber criminals by

Configuring Microsoft Macro settings to:

- Harden the Microsoft macro environment and setting controls that are trusted to significantly minimise risk.
- Define which macros are going to be trusted.
- Disable Macros that do not demonstrate a business requirement.
- Enable Macros only from trusted locations.
- Enable Macros only from trusted publishers that are digitally signed.
- Block Macros Files originating from the internet.
- Disable users access to changing these security settings.

Implementing Security Monitoring and compliance:

- Our Security Operations Center (SOC) will monitor (24x7x365) and continuously mitigate threats that aim to weaponize and target your Microsoft environment.

Providing Office365 Security Monitoring with:

- Analysis of logs for incidents
- Analysis of user behaviour & activity on sensitive systems
- Detection of both internal & external cyber-threats
- Human intervention & remediation by Blackhawk's Security Operations Centre (SOC)

ADDITIONAL FEATURES:

24/7 Security Operations Centre SOC

In order to respond effectively and prevent threats from escalating and causing massive financial damage, our SOC is staffed with knowledgeable and well-trained experts. At Blackhawk Alert, we are committed to pairing the right technology with the right people to ensure that threats are detected and responded to as quickly as possible, whilst guaranteeing the highest regard to accuracy and quality of service.

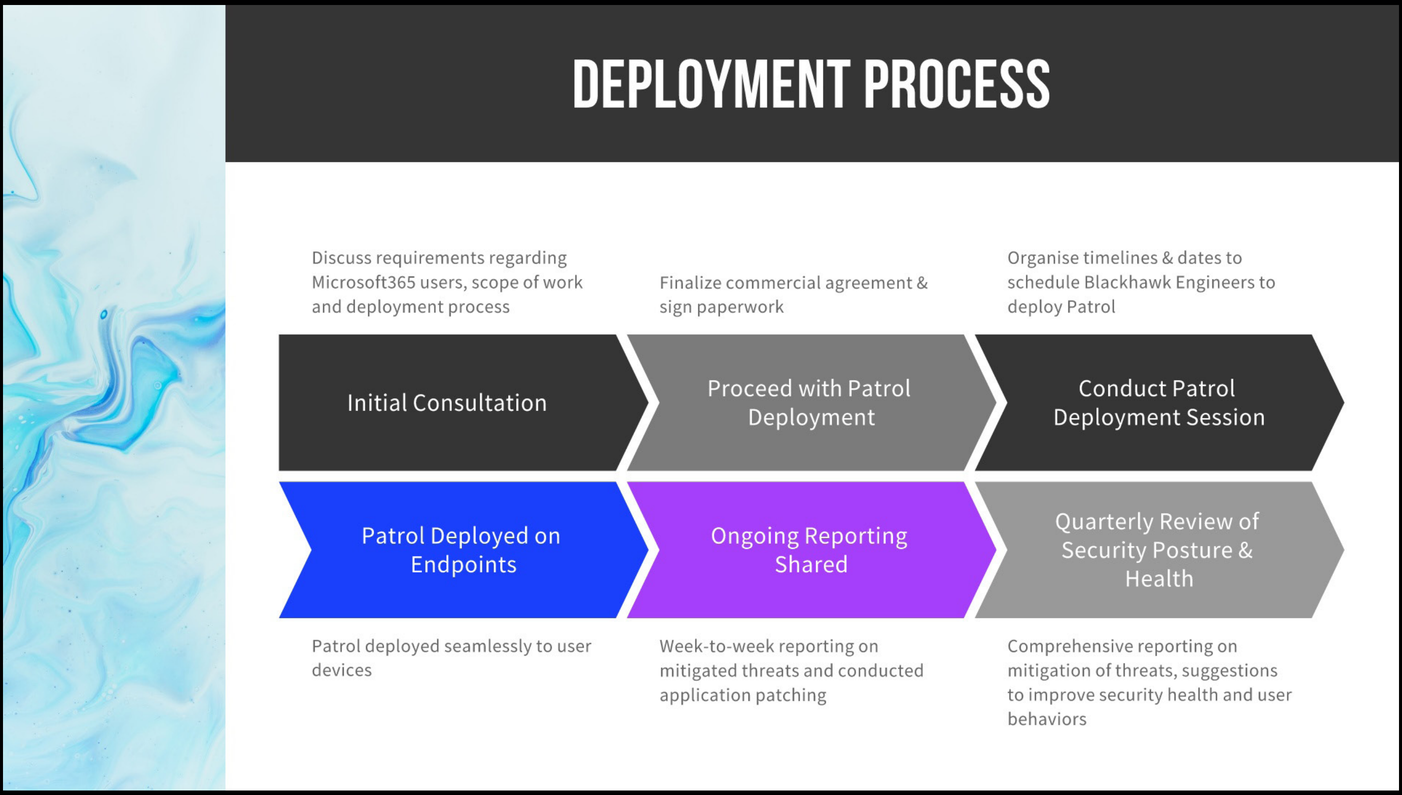
> *The experts who staff our 24/7 SOC are responsible for tasks that help ensure not only our ability to detect and respond to threats, but our consistency to evolve in the face of an ever-changing threat landscape.*

Blackhawk's SOC focus on 4 key areas:

- Applying threat intelligence provided by our automated detection solutions.
- Monitoring user behaviour to detect internal threats.
- Understanding how threat actors attack and their preferred vectors of attack.
- Learning and developing their ability to hunt new forms and methods of attack.

DEPLOYMENT

Deployment of Blackhawk Patrol is simple and seamless. Our support engineers will deploy Patrol software and connect your employee's devices to our SOC.



DEPLOYMENT PROCESS

Discuss requirements regarding Microsoft365 users, scope of work and deployment process

Initial Consultation

Finalize commercial agreement & sign paperwork

Proceed with Patrol Deployment

Organise timelines & dates to schedule Blackhawk Engineers to deploy Patrol

Conduct Patrol Deployment Session

Patrol Deployed on Endpoints

Patrol deployed seamlessly to user devices

Ongoing Reporting Shared

Week-to-week reporting on mitigated threats and conducted application patching

Quarterly Review of Security Posture & Health

Comprehensive reporting on mitigation of threats, suggestions to improve security health and user behaviors

CONCLUSION

Blackhawk Patrol is important because it helps to ensure the security and stability of the Microsoft environment. Malicious macros can pose a significant threat to computer systems by spreading viruses, stealing sensitive information, or making unauthorized changes to the system.

By implementing Blackhawk Patrol to lock down your Microsoft applications ensures your macro security settings and users can control the execution of macros and prevent unauthorised or malicious macros from running on their systems. This helps to minimize the risk of security breaches and improve the overall stability and reliability of the systems and ensures you business remains Cyber Ready.