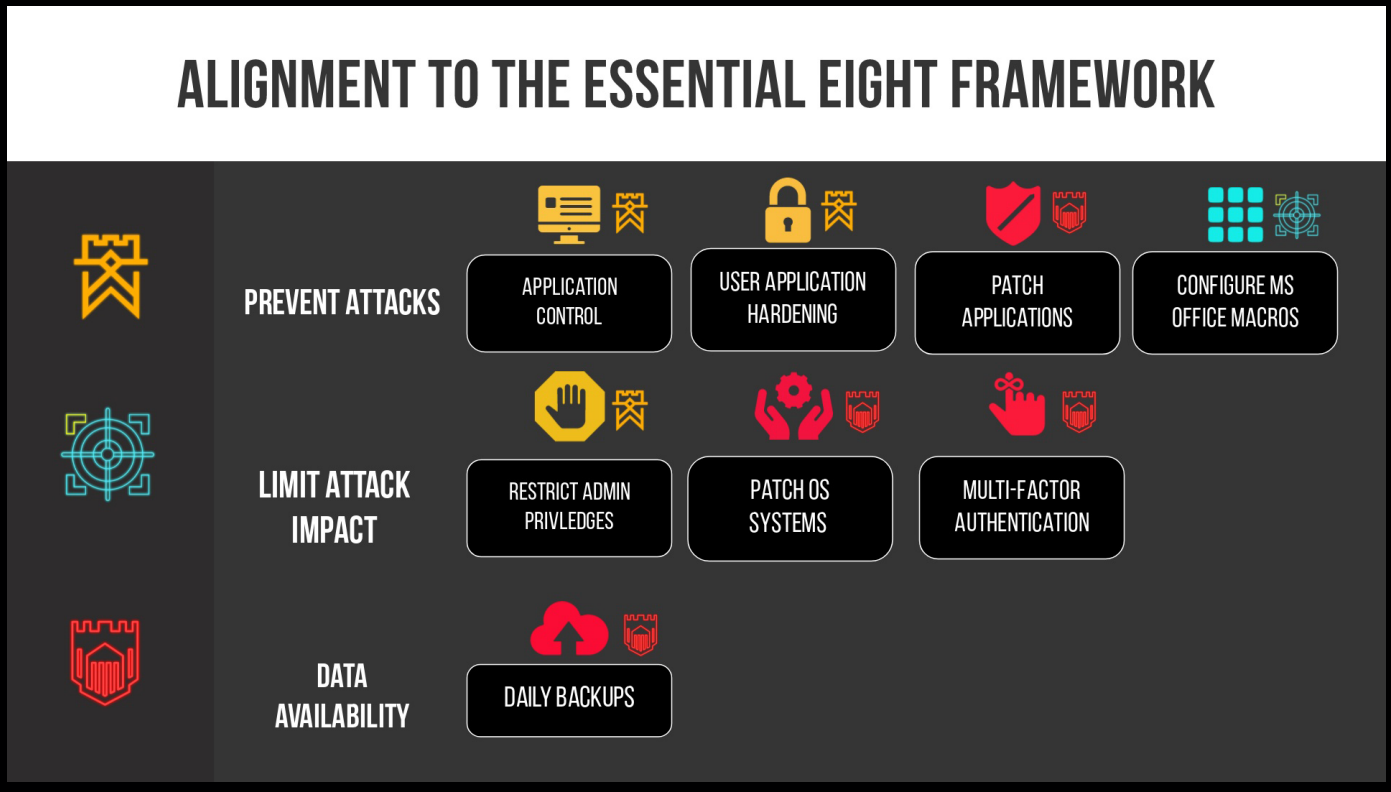
BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

FORTRESS PRODUCT WHITEPAPER

BLACKHAWK ALERT FORTRESS

Our SOC 24/7 Monitoring service provides comprehensive cybersecurity protection against threats such as malware, ransomware and exploitation. It's features include Threat Hunting & Containment, Automatic Remediation, Web Security, Email Security, Multi Factor Authentication, Login & Password Security, Backup and Disaster Recovery, Malware Protection, Ransomware Protection, Exploitation Protection, Disk Protection, Automatic Malware Removal, Software Patching, Security Health Checks, Archiving, Weekly and Monthly Reporting, Continuous Device Vulnerability Checks, and Onshore Support.



INTRO

As a small or medium-sized business (SMB) in Australia, cybersecurity is an increasingly important consideration. Cyber attacks are on the rise, and the financial impact on SMBs can be devastating. In fact, according to recent statistics:

As a small or medium-sized business (SMB) in Australia, cybersecurity is an increasingly important consideration. Cyber attacks are on the rise, and the financial impact on SMBs can be devastating. In fact, according to recent statistics:

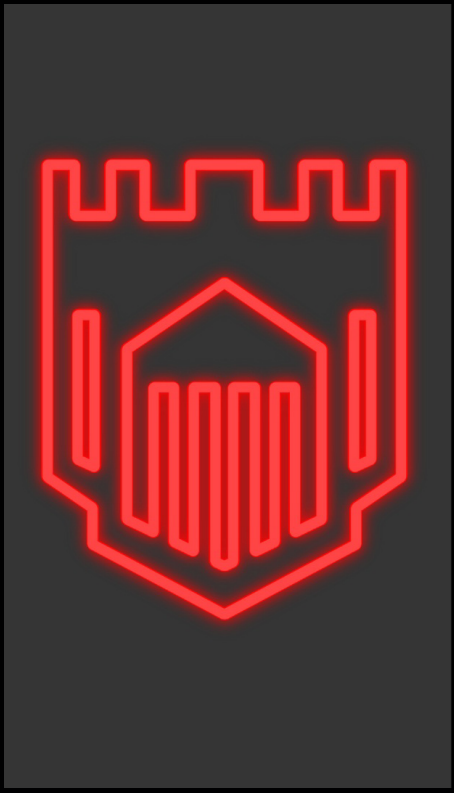
- Cyber attacks on SMBs cost an average of $39,000 - $62,000 per incident.
- 60% of SMBs go out of business within six months of a cyber attack.

To protect against these threats, many businesses are turning to managed detection and response solutions. Managed detection and response, or MDR, is a type of cybersecurity solution that provides continuous monitoring and real-time response to potential threats. With MDR, businesses can proactively defend against attacks and quickly respond to any incidents that do occur.

FORTRESS DEFINITION

One such solution is Blackhawk Fortress, a SOC-backed MDR solution for endpoints. Blackhawk Fortress provides continuous monitoring and real-time response to potential threats, as well as expert support and guidance to help businesses respond to incidents quickly and effectively. This means that businesses can focus on their core operations, knowing that their security is in good hands.

FEATURES



BLACKHAWK FORTRESS FEATURES

24/7 Monitoring & Remediation
with Threat Hunting

Backup:
Endpoint file level backup on a 48 hour cycle

Secure Endpoints
via Managed Detection & Response & Behavioral Analysis

Password Management:
Securely manage and store user credentials

Email Security
phishing prevention, archiving & scanning

Multi-Factor Authentication
Configure MFA for all critical applications

Web Security
DNS Filtering to block access to malicious sites

Software Patching
Updates all out-dated software to avoid exploitation

- 24/7 human-led threat hunting: Unfortunately, businesses generally rely either exclusively or primarily on software when implementing a cyber strategy. Blackhawk Alert puts human experts at the centre of every hunt, investigation and response action. While most SOCs applied a reactive approach to protecting against cyber incidents, Blackhawk's SOC proactively seeks out potential threats through hunting.
- Targeted actions to neutralise threats: we investigate suspicious activity, not just detections. We don't just investigate known threats, we investigate the behaviours, tactics, techniques and processes that attackers engage in to evade detection and execute successful attacks.
- Complete transparency and control: while others stop at threat monitoring and notification, Blackhawk Fortress takes targeted actions to neutralise threats.

FEATURES ALSO INCLUDE:

- SOC 24/7 Monitoring:

SOC (Security Operations Center) 24/7 monitoring is a process of constantly monitoring the security systems of an organization. It involves the use of automated tools and manual processes to detect and respond to cyber threats, malicious activities, and security incidents. The purpose of this type of monitoring included within Blackhawk Fortress is

to detect threats and intrusions quickly, so that the appropriate response can be taken. This process is often carried out by a dedicated team of security professionals who monitor the system around the clock.

- SOC Threat hunting & Containment:

Threat hunting & Containment is the process of proactively searching for malicious activity on the network and containing any malicious activity found. This typically involves using a combination of tools, techniques, and processes to search for known malicious activity as well as unknown threats. One of Blackhawk Fortress' goals is to identify, contain and mitigate potential threats before they can cause serious damage. Common techniques used in threat hunting & containment include malware analysis, log analysis, and network monitoring.

- SOC Automatic Remediation:

SOC (Security Operations Center) Automatic Remediation is a process that automatically takes action to respond to security events and incidents. Blackhawk Fortress uses automation to detect, analyse and respond to potential threats or malicious behaviour. It also helps in minimising the amount of manual labour required to identify and respond to security incidents. Automatic remediation helps reduce the time to respond and can even prevent incidents from occurring. It can also improve the security posture of an organization by responding quickly to threats and helping to identify attack patterns.

- Web Security:

Web security is the process of ensuring that users are protected from malicious web applications, websites, as well as unauthorised access and data theft. Blackhawk Fortress offers web security filters that block access to specific internet domains in line with cybersecurity best practices, and assists with content filtering for compliance, legal or organisational policies. Web security also involves monitoring and responding to potential security threats to ensure that users and data remain safe.

- Email Security:

Blackhawk Fortress prevents phishing and imposter threats. Many cyberattacks start with phishing. The danger is not the email itself but rather what it gets people to do. Emails can include malicious links or malware that attackers try to trick you into triggering malicious processes. Fortress keeps phishing imposters out and blocks attacks by leveraging machine learning analysis of message content, sender authentication, URL protection, and cloud sandboxing. Fortress also stops malware From reaching your inbox by applying threat intelligence, reputational and behavioural analysis, and state-of-the-art machine learning to eliminate malware and malicious URLs from ever reaching your employees. Fortress analyses all files, activity, and network connections to block ransomware, and other forms of malware. It uses deep learning to block zero-day (never before seen) threats.

- Multi Factor Authentication:

Multi Factor Authentication (MFA) is an authentication method that requires multiple factors to verify the identity of a user. These factors typically include

something a user knows (like a password), something a user has (like a token or an ID card) and something a user has (like a fingerprint). The combination of these factors provides a more secure authentication process than a single factor authentication & is included within Blackhawk Fortress

- Login & Password Security:

Login & password security is the practice of protecting user accounts with strong passwords and the ability to control access to such accounts. It ensures that only authorised users gain access to the system and the data contained within it. This security is essential for any organisation that stores confidential data, as it prevents unauthorised access to that data and guards against potential malicious attacks. Login & password security also helps to protect users from phishing and other cyber-attacks. Create and control strong credentials and user access to devices, networks, and applications with Blackhawk Alert's password management. The console is a cloud-based, encrypted password management system that generates strong passwords, eliminates re-using passwords, and automates password updates and maintenance. Increase productivity with fast onboarding, and automated workflows. Work smarter with centralised documentation.

- Device File Backup:

Device file backup is the process of Blackhawk Fortress seamlessly backing up your device's data - this includes all files, documents and Microsoft365 data. Backing up your data serves the purpose of protecting the data in case of an unexpected event such as a system crash or power outage. This data is stored in Blackhawk Alert's Cloud. Device file backup is important for mitigating data loss, ensuring the continuity of operations, and meeting compliance regulations (AES 256-bit encryption). Cloud storage is included in your Blackhawk Fortress licensing at no additional cost.

- Ransomware, Malware, Exploitation Protection:

Stop unknown threats with Blackhawk Fortress' deep learning AI that excels at detecting and blocking never-before-seen malware. It does this by scrutinising file attributes from hundreds of millions of samples to identify threats.

Ransomware: Fortress also uses advanced anti-ransomware capabilities that detect and block the malicious encryption processes used in ransomware attacks. Files that have been encrypted will be rolled back to a safe state, minimising any impact to business productivity.

Exploits: Fortress prevents exploits through embedded anti-exploit technology, thwarting techniques that attackers rely on to compromise devices, steal credentials and distribute malware. By stopping the techniques used throughout the attack chain, Fortress keeps your organisation secure against file-less attacks and zero-day exploits.

Synchronized Security solutions work better together. For example, Blackhawk Fortress and Frontier share data to automatically isolate compromised devices while cleanups are performed, then re-enable network access only once the threat is neutralised. All without the need

for manual intervention.

- Software patching:

Blackhawk Fortress includes software patching - the process of updating software with a piece of code known as a patch. Patches are released by software vendors to fix bugs and security vulnerabilities in existing software products. Patches can be released as standalone files or as part of a larger software update. Patching is a necessary but often time-consuming task for IT administrators, as patches must be tested before being applied to production systems - Fortress takes on this lift.

- Security Health Checks:

Blackhawk Fortress' security health checks are assessments that are conducted to identify weaknesses in an organization's security policies, procedures and systems. The purpose of a security health check is to ensure that the organization is compliant with industry standards and best practices. It can also help identify potential security issues and vulnerabilities in the organization's infrastructure, such as insecure applications, unpatched software, and improper user access controls. A security health check typically includes an assessment of the organization's overall security posture and compliance with relevant laws, regulations and standards, as well as a review of the organization's security policies and procedures.

- Continuous device vulnerability checks:

Blackhawk Fortress includes continuous device vulnerability checks - a type of security measure that involves regularly scanning and monitoring the security of connected devices on a network. It helps to identify potential security flaws that could be exploited by malicious actors and then take the necessary steps to address them. The process involves detecting and reporting on any changes in the network or devices that could indicate a potential vulnerability. This helps to ensure that the system is constantly monitored and any potential threats are identified and addressed in a timely fashion.

- Support:

Blackhawk Alert Fortress includes the highest levels of onshore customer service and technical support offered. When an incident has occured, time is of the essence - Blackhawk's support service standardises our approach in working with you by first notifying, collaborating and authorising necessary actions based on your requirements.

Blackhawk's support team will always notify of any assistance required, ensuring your business remains protected around the clock.Case tickets can be raised easily through our customer portal and issues are resolved quickly via case assignment as priorised SLA's.

BENEFITS

Blackhawk Alert Fortress doesn't just monitor and notify - it takes action: we remotely initiate actions to disrupt, contain, and neutralise threats.

- Offers better, more proactive protection: the technology upon which Fortress is built catches threats that other technology wouldn't notice.
- Provides effective automated response: Fortress catches more threats, it's better able to automate response actions for known threats.
- Focused human response: automations in threat detection narrow our security operations team's focus to responding to, and taking action on more important threats.
- Robust threat hunting: Fortress conducts lead-driven and lead-less threat hunts to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.
- Clear visibility on Cyber Incidents: Organisations are notified in the event of an incident - able to transparently view how Blackhawk's SOC has used Fortress to detect, respond to and remediate the potential threat.

In addition to providing comprehensive protection against potential threats, Blackhawk Fortress is also compliant with industry and framework standards. This means that businesses can trust that their security is in good hands, and that they are meeting their compliance requirements.

CUSTOMER JOURNEY

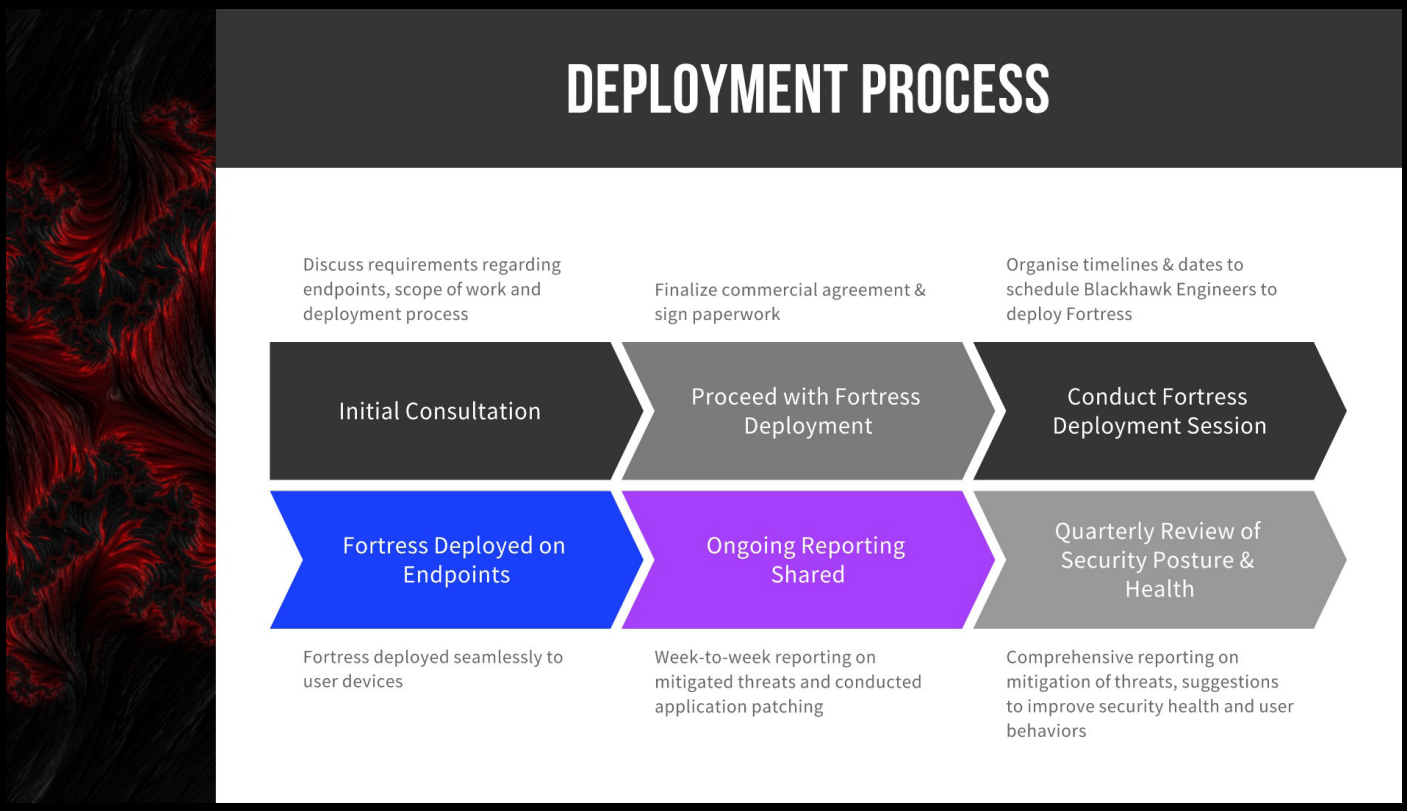
As our consultants support your businesses need for a managed detection response solution & understand how Fortress will align, here are a few questions to consider:

- How do you know if your business is under attack?
- What tools do you have in place to understand the scope and impact of an attack?
- How long does it typically take you to investigate a security incident?
- Do you have the ability to hire skilled analysts to conduct endpoint detection and response?
- How do you know when you are out of compliance?
- What data do you have to confirm you are in compliance?
- Do you have enough visibility into your endpoints to report on your security posture?

DEPLOYMENT

Deployment for Blackhawk Fortress is incredibly straightforward and seamless.

Blackhawk Alert's service delivery team will remote into your businesses endpoints (devices) in order to install Fortress licences.



CONCLUSION

Overall, a cybersecurity-as-a-service solution like Blackhawk Fortress is an essential tool for SMBs in Australia looking to protect their businesses from the growing threat of cyber attacks. With its comprehensive protection and industry compliance, Blackhawk Fortress is an important solution for any business looking to safeguard their data and operations.