BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

RECON
PRODUCT
WHITEPAPER

BLACKHAWK ALERT RECON

INTRO

As a small or medium-sized business (SMB) in Australia, cybersecurity is an increasingly important consideration. With the rise of cyber attacks, SMBs need to be proactive in protecting their businesses from potential threats. Fortunately, there are solutions like Blackhawk Alert that can help.

As large commercial businesses are getting harder and harder to hack, cyber-criminals are turning their attention to small or medium-sized businesses.

The SMB market is a target for cybercrime because small and medium-sized businesses often have fewer resources and less robust security measures in place compared to larger companies. This makes them more vulnerable to cyber attacks, and attackers see them as an easier target.

Additionally, SMBs hold valuable data and customer information that can be used for financial gain or other malicious purposes.

Another reason that cyber criminals are targeting SMB is that SMBs are often part of a supply chain, and by targeting them, attackers can gain access to the larger companies they are associated with. This is called a supply chain attack.

Furthermore, many SMBs may not have dedicated IT staff or cybersecurity professionals on staff, making it harder for them to detect and respond to cyber threats.

Cyber criminals often view SMBs as an easy target, they know that these organisations usually have fewer resources and less robust security measures than large enterprise companies and therefore, they have a higher chance of success.

Business owners should understand the following when considering cyber risk:

1. Cyber threats are always changing, and businesses must adapt to stay secure.

2. Every business is a potential target, regardless of size or industry.

3. Employees can be a weak link in security, so education and policies are important

4. Cybersecurity requires ongoing investment.

5.A cyber attack can have a severe impact on operations and reputation.

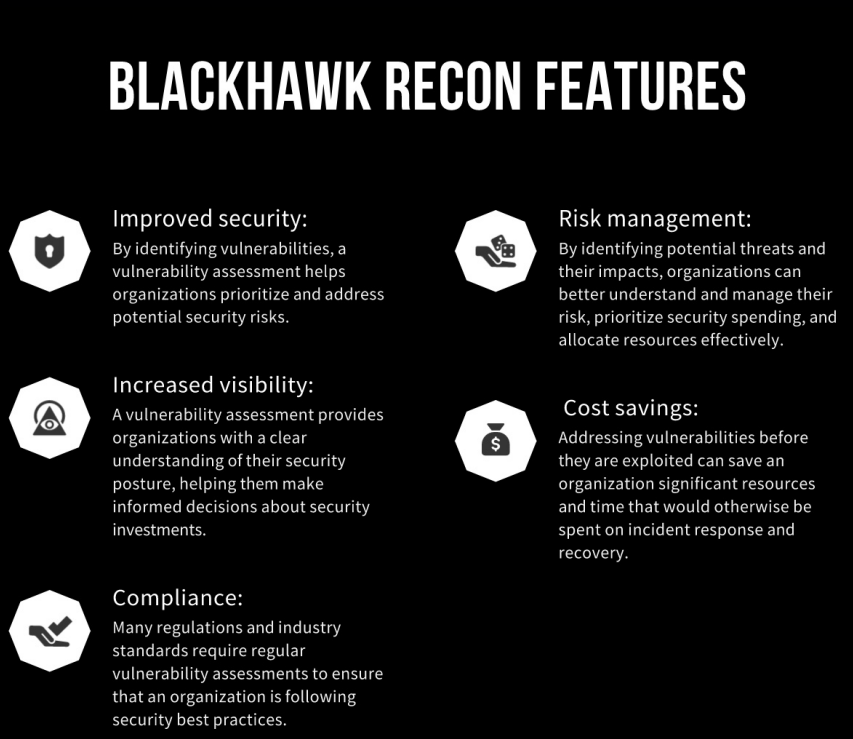
6.Compliance with laws and regulations is necessary.

7.Cyber insurance can help mitigate financial losses.

KEY FEATURES

Risk is just a possibility—until it isn't.

Blackhawk Recon can help you identify, locate, and monitor your sensitive data across the dark web. It also provides detailed analysis of potential breach scenarios and the associated costs, helping you to understand the importance of prioritising security and what action is needed to prevent loss. With Recon, you can rest assured knowing that your organisation is safe and secure.



FEATURES INCLUDE:

- **Deep vulnerability scanning**

Deep vulnerability scanning is a type of security testing that involves a thorough examination of the business technology components for identifying any existing vulnerabilities or future exploitable gaps. Recon's deep vulnerability scanning analyses potential security threats and weaknesses in a business environment.

- **Reports detailing the financial impact of risks**

  - Recon itemises vulnerabilities and converts that risk into the estimated cost of a potential breach. When the security issues are detailed in black and white, there's a measurable cost associated with inaction.

- Recon also generates a report detailing the financial impact of cybersecurity risks that your business carries and enables us to consult you through ways to minimise your risk.
- The report can be used to help organisations understand the potential financial impacts of not investing in cybersecurity, as well as the value of investing in security solutions.

● Identification of inappropriate user access

Identification of inappropriate user access involves the process of detecting users who are accessing data and resources they do not have the proper authorization for

Recon identifies what users have access to what data. From a security standpoint, if an individual is compromised - everything they have access to can be exploited.

This is especially important in companies that handle sensitive information as protection against malicious actors or internal threats (purposeful or accidental) is a top priority.

● Leaked User emails and passwords

Recon breach scan gives your business clear visibility of which user credentials have been exposed in known data breaches and are easily accessible to cyber criminals in hacker hotspots - this data can be used to launch ultra-targeted phishing attacks

The scan will generate a list of all employees within your organisation. This is then sorted by the number of breaches that their information has been found within, and their total breach count visible.

● At-risk data

Recon enables us to explore your compromised data and learn which service/ breach led to the exposure. Businesses can determine which employee's data has been exposed, when the breach occurred, and the type of information that was exposed.

At-risk data can include bank account details, address, security questions and answers, credit card, login credentials for applications.

STEPS FOR REMEDIATION

We will provide a snapshot as a valuable starting point for strategies around security.

1. Identify the vulnerability: The first step is to identify the security vulnerability or breach. This is done by performing an audit or a security scan to detect any weaknesses in the system.

2. Assess the impact: Once the vulnerability has been identified, the next step is to assess the potential impact of the vulnerability. This may include the type of data that could be compromised, the number of users that could be affected, and the financial or reputational damage that could occur.

In the even that recon detects a malicious live threat in your environment we can deploy our Blackhawk Alert Airstrike. This service "Airstrike" is our Security analysis finding and removing the threat in your environment and providing documentation of what it was and what the threat was doing. The process of Airstrike consists of 4 phases. 1) identifying, 2) containing, and 3) removing a security threat. 4) provide reports and documentation.

3. Develop a remediation plan: The third step is to develop a remediation plan to address the identified vulnerability. This should include the steps required to fix the issue, the resources needed, and the timeline for completion.

4. Implement the remediation plan: The fourth step is to implement the remediation plan. This includes making any necessary changes to the network or system configuration, deploying security patches or upgrades, and any other steps required to fix the vulnerability.

5. Monitor results: The fifth step is to monitor the results of the remediation plan to ensure that the vulnerability has been successfully addressed. This may involve running additional scans and tests to check for any remaining weaknesses.

BENEFITS

An initial cybersecurity assessment should also include an evaluation of the company's current security processes and procedures. This includes reviewing existing policies and procedures, such as those related to user access, patching and updating, password management, and user education. This review can help identify areas where improvements are needed and can be used to develop a comprehensive security strategy.

Finally, an initial cybersecurity assessment should also include an analysis of the company's overall security posture. This includes a review of the security measures in place to protect the company's data, networks, and systems. This can include a review of the company's existing security protocols, such as firewalls, antivirus software, and intrusion detection systems. It is also important to review the company's disaster recovery plan and backup processes.

By conducting an initial cybersecurity assessment, Australian SMBs can identify potential vulnerabilities and threats and develop a comprehensive security strategy to meet their security needs. This assessment is essential to ensure the safety and security of their digital assets and networks.

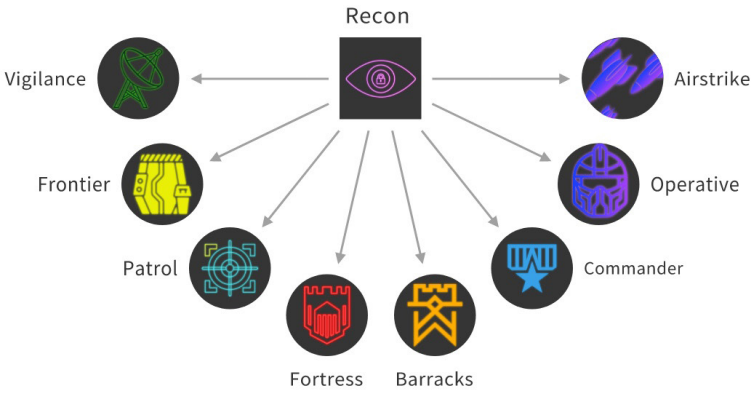
In addition to providing comprehensive protection against potential threats, Blackhawk Alert is compliant with industry and framework standards. This means that businesses can trust that their security is in good hands, and that they meet compliance requirements.

RECON: YOUR ENTRY POINT INTO BLACKHAWK SOLUTIONS

Effective cybersecurity assessment is essential for any business looking to protect their assets and data from threats.

Recon by Blackhawk Alert offers a tailored approach to understanding the current state of your company's cybersecurity. With fast turnaround and comprehensive results, our solution includes a presentation of findings from our team to provide supported analysis and easily interpret recommendations for addressing vulnerabilities.

Don't leave your business at risk - utilize Recon and our team to stay ahead of potential threats and ensure the safety of your company's valuable assets.



BLACKHAWK ALERT

MORE THAN SOFTWARE

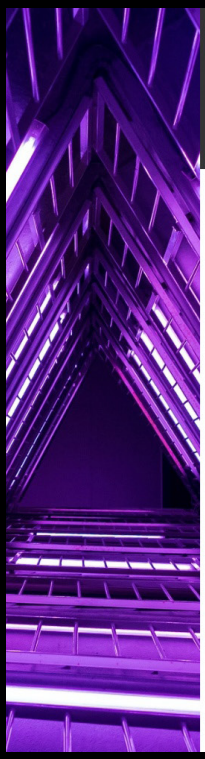
Protect your business with enterprise-grade managed cyber security solutions aligning with Essential 8 & NIST Frameworks

DEPLOYMENT

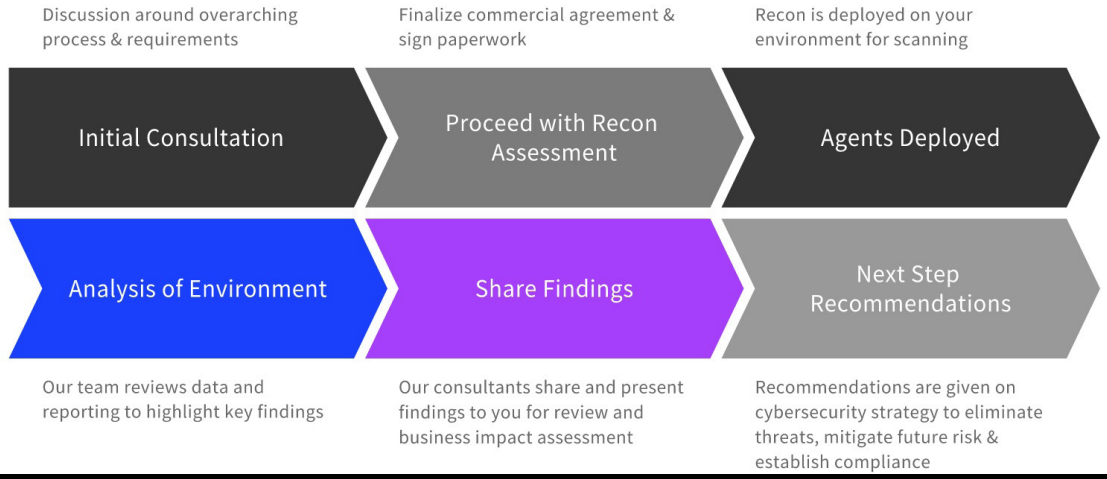
One of the key benefits of the Recon solution is its ease of deployment. Once purchased, we provide clear instructions for deploying the necessary agents, programs, and applications onto devices. This process is designed to be straightforward and hassle-free, allowing you to set it and forget it.

By automating this critical step, we ensure that your business is protected and can focus on more important tasks.

Trust our solution to handle the heavy lifting of cybersecurity deployment, so you can rest easy knowing your assets are secure.



DEPLOYMENT PROCESS



CONCLUSION

Overall, Blackhawk Recon is an essential solution for Australian SMBs looking to protect their businesses from the growing threat of cyber-attacks.

With its comprehensive scanning, diagnosis and reporting capabilities, Blackhawk Recon is more than just a tool - for the SMB, it serves as an entry point into defining what it means to be Cyber Ready.