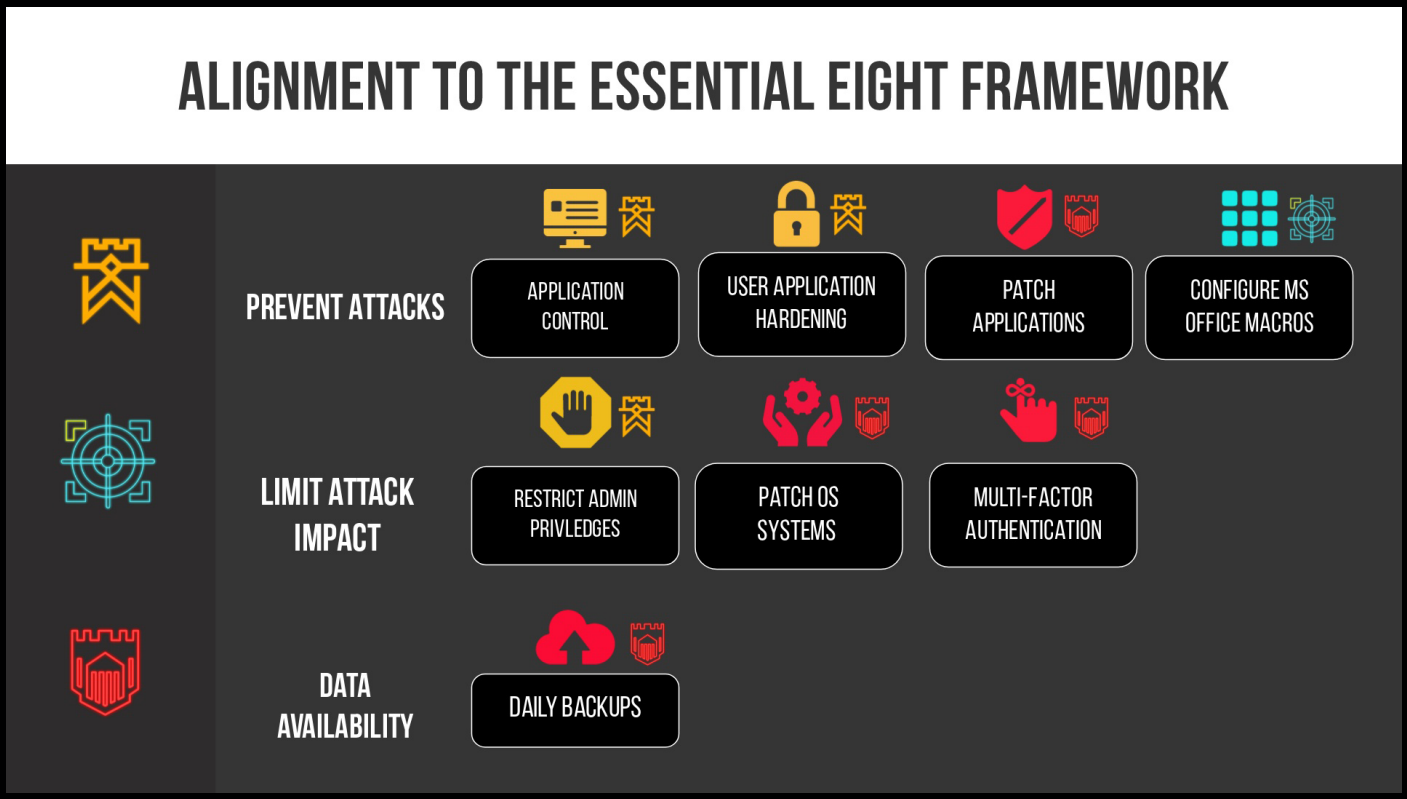
BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

BARRACKS PRODUCT WHITEPAPER

BLACKHAWK ALERT BARRACKS

Blackhawk Barracks is designed in alignment with the Essential Eight to deliver Application control. Application control can be achieved by whitelisting all applications from running except those that are explicitly allowed. This means untrusted software, including ransomware and other malware, will be denied by default.



INTRO

Small to medium-sized businesses are constantly buying into the latest technologies such as next-gen antivirus software and threat detection solutions that use machine learning, artificial intelligence, advanced heuristics, blockchain, and more. However, these solutions only protect a portion of cyber threats. Most cybersecurity protections are based on looking for, finding, and stopping threats. The problem is, cybercriminals are getting smarter and entering networks undetected. End-users are constantly inviting threats through actions such as downloading various applications without your approval, clicking on links they shouldn't, and opening attachments in emails.

That's why a new Zero-trust approach of blocking everything that is not trusted and only allowing those applications that are approved is a far cleaner and more comprehensive approach to securing your environment. Barracks whitelisting with Ring Fencing and StorageControl in ways that make security simple.

WHAT IS APPLICATION CONTROL & WHITELISTING?

Application Allowlisting denies all applications from running except those that are explicitly allowed. This means untrusted software, including ransomware and other malware, will be denied by default.

When the Barracks was first installed, it operated in “Learning Mode.” During this period, all applications and their dependencies that are found or running on the computer are catalogued, and policies are created to permit them.

After the learning period, we review the list of applications, remove those that are not required, and secure the computer. Once the computer is secured, any application, script, or library that tries to execute that is not trusted will be denied.

The user can request new software from Barracks to be approved in 60 seconds. Application Allowlisting has long been considered the gold standard in protecting businesses from known and unknown malware. Unlike antivirus or traditional EDR, Application Allowlisting puts you in control of what software, scripts, executables, and libraries can run on your devices. This approach stops not only malicious software but also stops other unpermitted applications from running. This process greatly minimises cyber threats and other rogue applications running on your network.

WHAT IS ZERO TRUST?

Zero Trust is a security framework that states that organisations should not trust any entity inside or outside their perimeter at any time. Today’s environment must provide the visibility, and IT controls needed to secure, manage and monitor every device, user, app, and network used to access business data.

KEY FEATURES

BLACKHAWK BARRACKS FEATURES

Application Allowlisting:
denies any application from running on your device that is not a part of the Allowlist, stopping cyber attacks from happening on your devices or across your network.

Storage Control:
Storage Control allows granular policies to be set, which could be as simple as blocking USB drives, or as detailed as blocking access to your backup share, unless accessed by your backup application.

Firewall-like Application Policies:
A powerful firewall-like policy engine that allows you to permit, deny or restrict application access at any level.

Ring Fencing:
controls what applications are able to do when running, reducing the likelihood of an exploit being successful or an attacker weaponizing legitimate software.

Granular Application Policies:
Stop applications from adversely interacting with other applications, network resources, registry keys, files, and more.

ALLOWLISTING:

- Using the Barracks solution, Blackhawk Alert denies any application from running on your device that is not a part of the Allowlist. This helps to mitigate and stop cyberattacks from happening on your devices or across your network.

FIREWALL-LIKE APPLICATION POLICIES:

- A powerful firewall-like policy engine that allows you to permit, deny or restrict application access at any level.

TIME-BASED POLICIES:

- Permit access to applications for a specified amount of time. Automatically block the application after the policy has expired.

BUILT-IN APPLICATIONS:

- Barracks automatically adds new hashes when application and system updates are released, allowing your applications to update without interference while preventing updates from being blocked.

RING FENCING:

- Ring Fencing controls what applications are able to do once they are running. By limiting what software can do, Barracks can reduce the likelihood of an exploit being successful or an attacker weaponizing legitimate software such as Microsoft office.

STORAGE CONTROL:

- Storage Control provides policy-driven control over storage devices, whether the storage device is a local folder, a network share, or external storage such as a USB drive. Storage Control allows granular policies to be set, which could be as simple as blocking USB drives, or as detailed as blocking access to your backup share, except when accessed by your backup application. Unified Audit provides a central log of all storage access by users on the network and those working remotely, right down to the files that were copied and the serial number of the device.

SECURE APPLICATION INTEGRATION:

- RingfencingTM, ensures that once applications are elevated, users cannot jump to infiltrate connected applications within the network.

ADDITIONAL FEATURES

MITIGATE AGAINST FILELESS MALWARE:

- Stop fileless malware by limiting what applications are allowed to do.

GRANULAR APPLICATION POLICIES:

- Stop applications from interacting with other applications, network resources, registry keys, files, and more.

LIMIT APPLICATION ATTACKS:

- Limit application attacks like application hopping by limiting what applications can access.

LIMIT TO YOUR FILES:

- The average computer has over 500 applications, and only a handful of those need to access your files. With Ring Fencing, you can choose which applications need to see which files.

AUDIT ACCESS TO FILES:

- A full detailed audit of all file access on USB, Network, and Local Hard Drives is centrally accessible within minutes of a file being opened.

GRANULAR STORAGE POLICIES:

- Users can request permission to elevate applications and attach files and notes to support their requests.

SIMPLE REQUESTS FOR ACCESS:

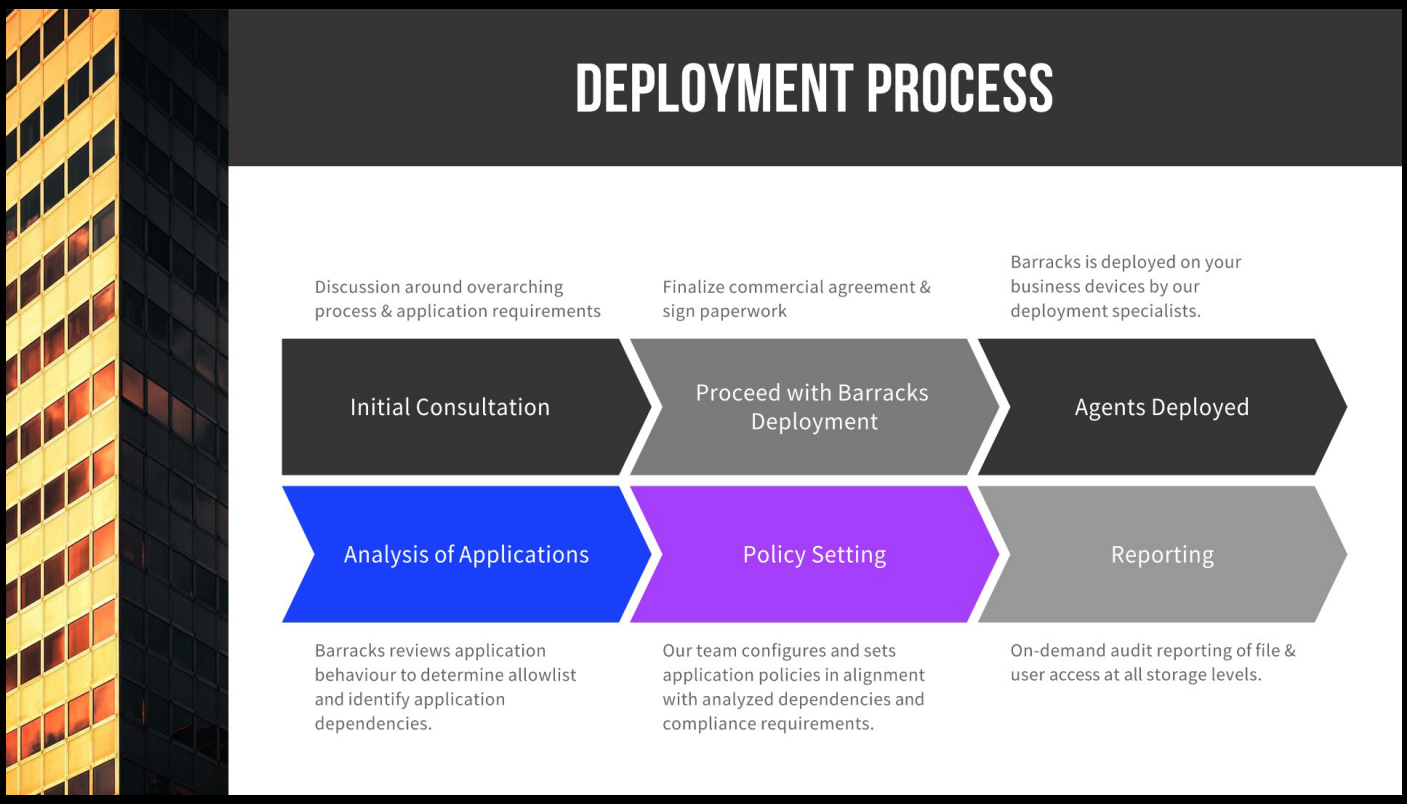
- A pop-up with the option to request access to the storage device

SIMPLE USB BLOCKING:

- USB Policies allow access based on device serial number, vendor, and/ or file type.

ENHANCED NETWORK SECURITY:

- Ensure rogue devices on your network cannot access your servers or endpoints with Dynamic ACLs.



CONCLUSION

Application controls and application allow listing are important security measures in protecting computer systems and networks from unauthorised access or malicious activities. Application controls ensure that the applications running on a system adhere to specific security policies and rules, such as access controls, input validation, and data protection. Application allow listing allows only approved applications to run on a system, preventing the execution of malicious software. These measures help maintain the confidentiality, integrity, and availability of sensitive data and systems.