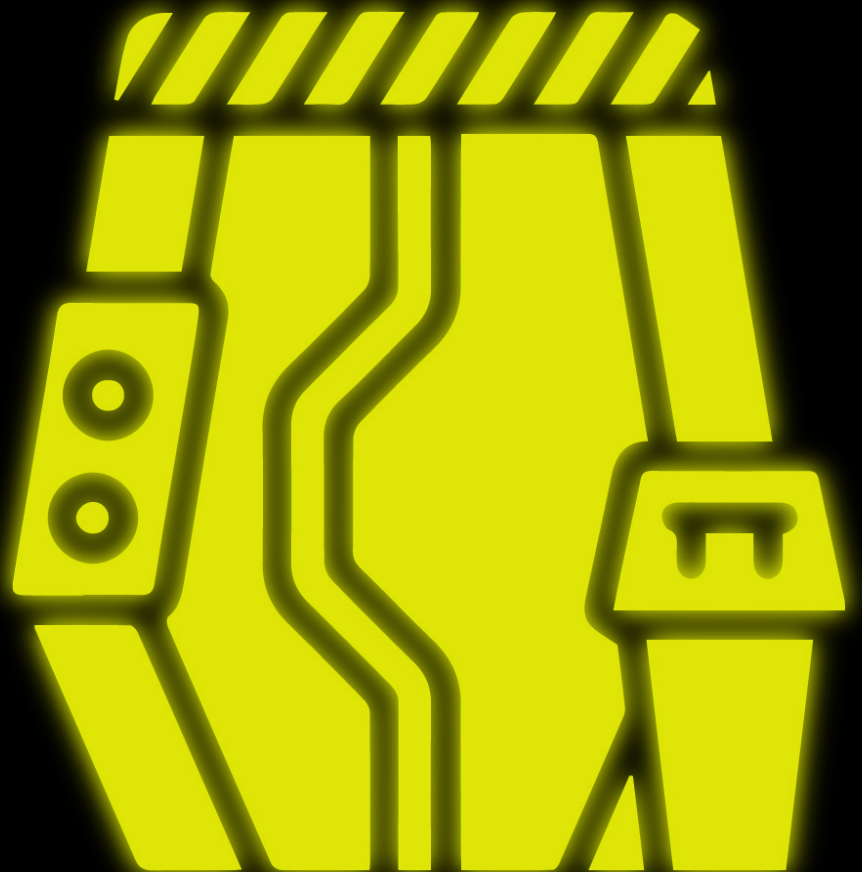


BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS



FRONTIER
PRODUCT
WHITEPAPER





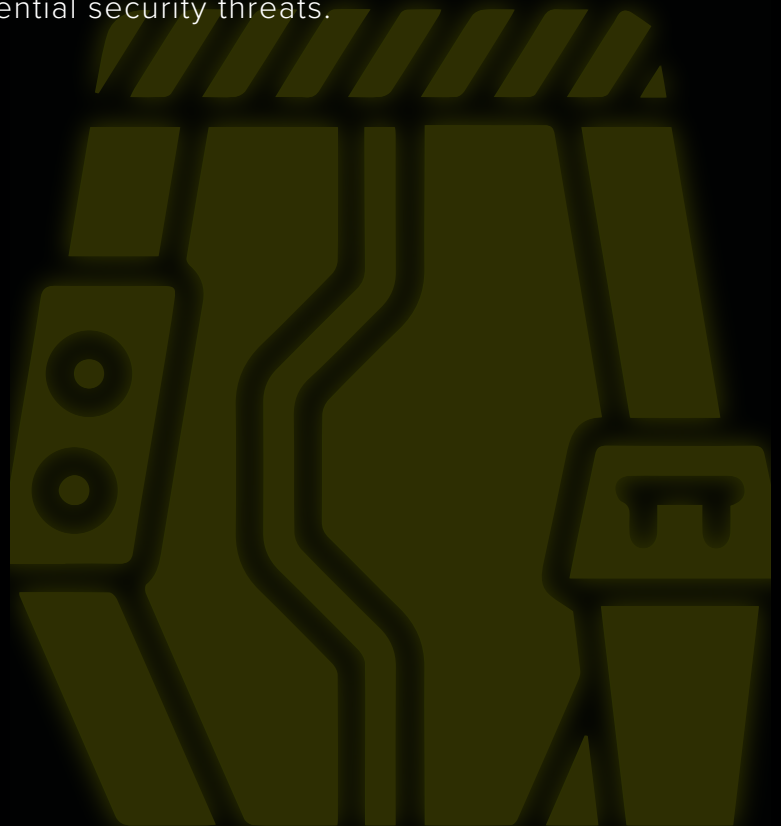
BLACKHAWK ALERT FRONTIER

INTRO

Blackhawk Alert Frontier is a SOC managed firewall. It's a network security system that monitors and controls incoming & outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network, such as the Internet. The primary purpose of a firewall is to prevent unauthorised access to or from a private network & to protect sensitive information from being disclosed to external parties. Blackhawk Frontier operates by examining each incoming & outgoing network packet and allowing or blocking it based on a set of rules that determine the source, destination, and type of traffic. This prevents security threats such as malware, hacking, and phishing attacks.

WHAT IS A “SECURITY OPERATIONS CENTRE (SOC) MANAGED FIREWALL”?

A Security Operations Center (SOC) managed firewall is an important component of an organisation's overall security posture .By having the firewall managed by Blackhawk Alert's security experts, organisations can focus on their core business objectives and reduce their risk of security incidents. A SOC - managed firewall provides organisations with the peace of mind that their critical data and systems are protected from potential security threats.



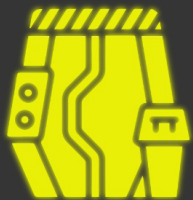


KEY FEATURES

● Telemetry with Fortress :

Blackhawk Frontier and Blackhawk Fortress have compatible technology that enables shared intelligence through observations across both the endpoint (Fortress) and Network layer (Frontier). Telemetry automatically collects and transmits data from various sources, to Blackhawk Alert's SOC for deeper security analysis and investigation.

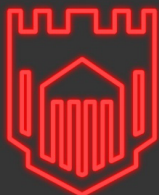
TELEMETRY WITH FORTRESS



IMPROVED NETWORK VISIBILITY: BLACKHAWK FRONTIER CAN CONTINUOUSLY SEND INFORMATION ABOUT NETWORK TRAFFIC, THREATS, AND EVENTS TO BLACKHAWK FORTRESS, PROVIDING A MORE COMPLETE AND UP-TO-DATE VIEW OF THE NETWORK'S SECURITY POSTURE.



ENHANCED THREAT DETECTION: BY ANALYSING LARGE AMOUNTS OF DATA FROM MULTIPLE SOURCES, BLACKHAWK FORTRESS CAN DETECT AND RESPOND TO THREATS MORE QUICKLY AND ACCURATELY. THIS CAN HELP REDUCE THE RISK OF DATA BREACHES AND OTHER SECURITY INCIDENTS.

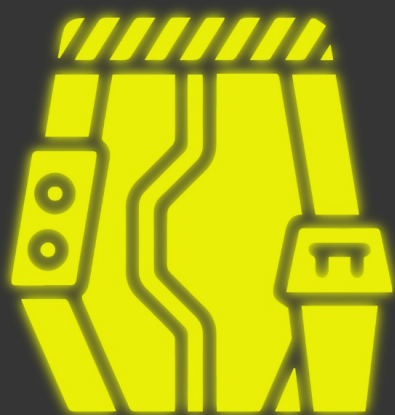


STREAMLINED MANAGEMENT: BLACKHAWK FORTRESS CAN USE TELEMETRY DATA TO AUTOMATE MANY ROUTINE TASKS, SUCH AS UPDATING BLACKHAWK FRONTIER'S FIREWALL RULES, REPORT GENERATION, AND MONITORING THE HEALTH OF BLACKHAWK FRONTIER & OTHER NETWORK DEVICES.

BLACKHAWK FRONTIER AND BLACKHAWK FORTRESS HAVE COMPATIBLE TECHNOLOGY THAT ENABLES SHARED INTELLIGENCE THROUGH OBSERVATIONS ACROSS BOTH THE ENDPOINT (FORTRESS) AND NETWORK LAYER (FRONTIER). TELEMETRY AUTOMATICALLY COLLECTS AND TRANSMITS DATA FROM VARIOUS SOURCES, TO BLACKHAWK ALERT'S SOC FOR DEEPER SECURITY ANALYSIS AND INVESTIGATION.

BENEFITS OF PAIRING FRONTIER AND FORTRESS TO ENABLE TELEMETRY INCLUDE:

- 1. Improved network visibility:** Blackhawk Frontier can continuously send information about network traffic, threats, and events to Blackhawk Fortress, providing a more complete and up-to-date view of the network's security posture.
- 2. Enhanced threat detection:** By analysing large amounts of data from multiple sources, Blackhawk Fortress can detect and respond to threats more quickly and accurately. This can help reduce the risk of data breaches and other security incidents.
- 3. Streamlined management:** Blackhawk Fortress can use telemetry data to automate many routine tasks, such as updating Blackhawk Frontier's firewall rules, report generation, and monitoring the health of Blackhawk Frontier & other network devices.



BLACKHAWK FRONTIER FEATURES



Threat detection and response:

Our SOC-managed firewall is monitored by security experts in detecting and responding to real-time security threats. This proactive approach prevents data breaches and other incidents before they cause harm.



Reduced costs:

More cost-effective than in-house security solutions, eliminating the need to invest in hardware, software, and personnel.



Continuous monitoring and improvement:

Blackhawk's SOC monitors 24/7/365 and keeps abreast with changing security threats & new vulnerabilities, ensuring your environment & sensitive data remains protected.



Scalability:

Blackhawk Frontier can be scaled to meet the needs of businesses of any size, from small businesses to large enterprises. This allows you to easily grow securely without impacts to the integrity of your firewall, the protective barrier.



Compliance

Many regulations, such as the PCI DSS and GDPR, require organisations to implement a firewall as part of their security measures. Frontier helps meet these compliance requirements and avoid costly fines & penalties.



Reporting:

Blackhawk Frontier access includes historical on-box logging and reporting, cloud reporting (seven-day data retention), extensive web & app reporting.

● Threat detection and response:

Our SOC-managed firewall is monitored and managed by security experts who have the expertise to detect and respond to security threats in real-time. This proactive approach helps to prevent data breaches and other security incidents before they cause harm to your organisation.

● Continuous monitoring and improvement:

Blackhawk Alert SOC monitors 24/7/365 and keeps up to date with changing security threats and new vulnerabilities. This ensures that your environment remains effective in preventing security incidents & protecting sensitive data.

● Compliance:

Many regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), require organisations to implement a firewall as part of their security measures. A SOC-managed firewall helps organisations meet these compliance requirements and avoid costly fines & penalties.

● Reduced costs:

Blackhawk Frontier is more cost-effective than in-house security solutions, as it eliminates the need for organisations to invest in hardware, software, and personnel.



- **Scalability:**

Blackhawk Frontier can be scaled to meet the needs of businesses of any size, from small businesses to large enterprises. This allows you to easily grow securely without impacts to the integrity of your firewall, the protective barrier.

- **Reporting:**

Blackhawk Frontier access includes historical on-box logging and reporting, cloud reporting (seven-day data retention), extensive web & app reporting.

ADDITIONAL FEATURES

I. FIREWALL MANAGEMENT

- **Threat detection and response:** Our SOC-managed firewall is monitored and managed by security experts who have the expertise to detect and respond to security threats in real-time. This proactive approach helps to prevent data breaches and other security incidents before they cause harm to your organisation.
- **Compliance:** Many regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), require organisations to implement a firewall as part of their security measures. A SOC-managed firewall helps organisations meet these compliance requirements and avoid costly fines & penalties.
- **Continuous monitoring and improvement:** Blackhawk Alert SOC monitors 24/7/365 and keeps up to date with changing security threats and new vulnerabilities. This ensures that your environment remains effective in preventing security incidents & protecting sensitive data.

II. ADVANCED THREAT PROTECTION

- **Exposes hidden risks:** Blackhawk Frontier possesses superior visibility into unknown applications, risky activity, suspicious traffic, and advanced threats to ensure only your business retains control of your network and gets deeper insights.
- **Blocks unknown threats:** Blackhawk Frontier leverages powerful next-gen protection technologies like deep learning and intrusion prevention to keep your organisation secure from the latest hacks and attacks.



- Automatically responds to incidents: Blackhawk Frontier's Synchronized Security automatic threat response instantly identifies and isolates compromised systems on your network to prevent breaches and lateral movement.

III. NETWORK SECURITY

- Firewall, Networking, and Routing
- VPN (IPsec, SSL, etc)
- Intrusion Prevention (IPS): Next-gen Intrusion Prevention
- Advanced Threat Protection (ATP) and Security Heartbeat™
- DPI (Deep Packet Inspection) Engine: Streaming deep-packet inspection
- TLS Inspection: TLS 1.3 inspection with prepackaged exceptions

IV. WIRELESS SECURITY

- Secure Wireless

V. Web and App Security Features

- Web Protection and Control: by user, group, category, URL, keyword
- Web Threat Protection: malware, PUA, malicious JavaScript, phishing
- Application Protection and Control: by user, group, category, risk, and more
- Synchronized Application Control: integration with endpoints to identify unknown apps
- Cloud Application Visibility

VI. TRAFFIC SHAPING AND QUOTAS

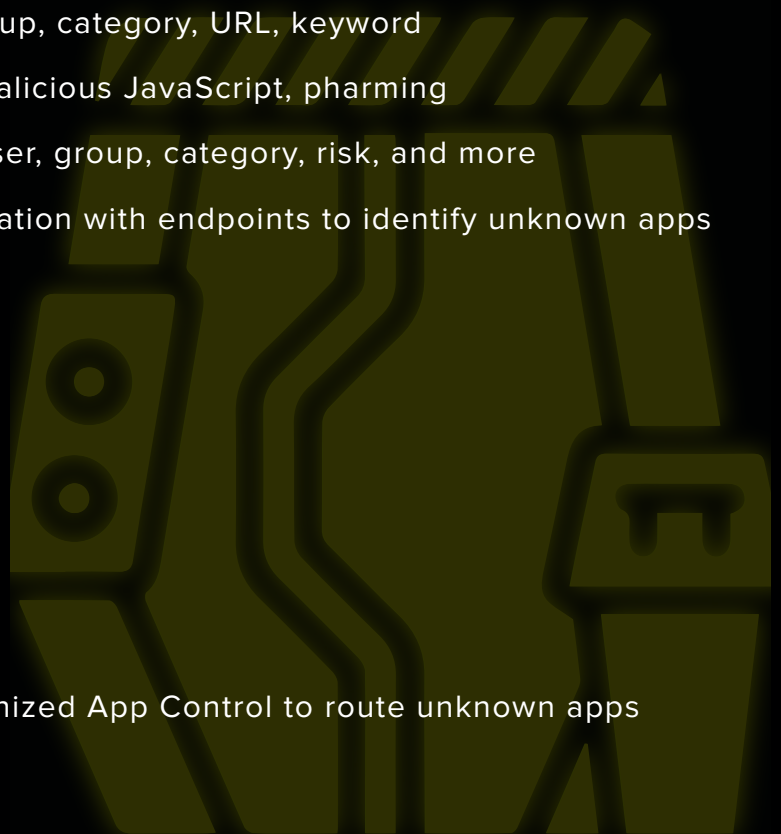
- Base Traffic Shaping & Quotas
- Web and App Traffic Shaping

VII. SD-WAN MANAGEMENT

- SD-RED Device Management
- Synchronized SD-WAN: utilizing Synchronized App Control to route unknown apps

VIII. USER ACCESS

- Authentication
- Self-Serve User Portal

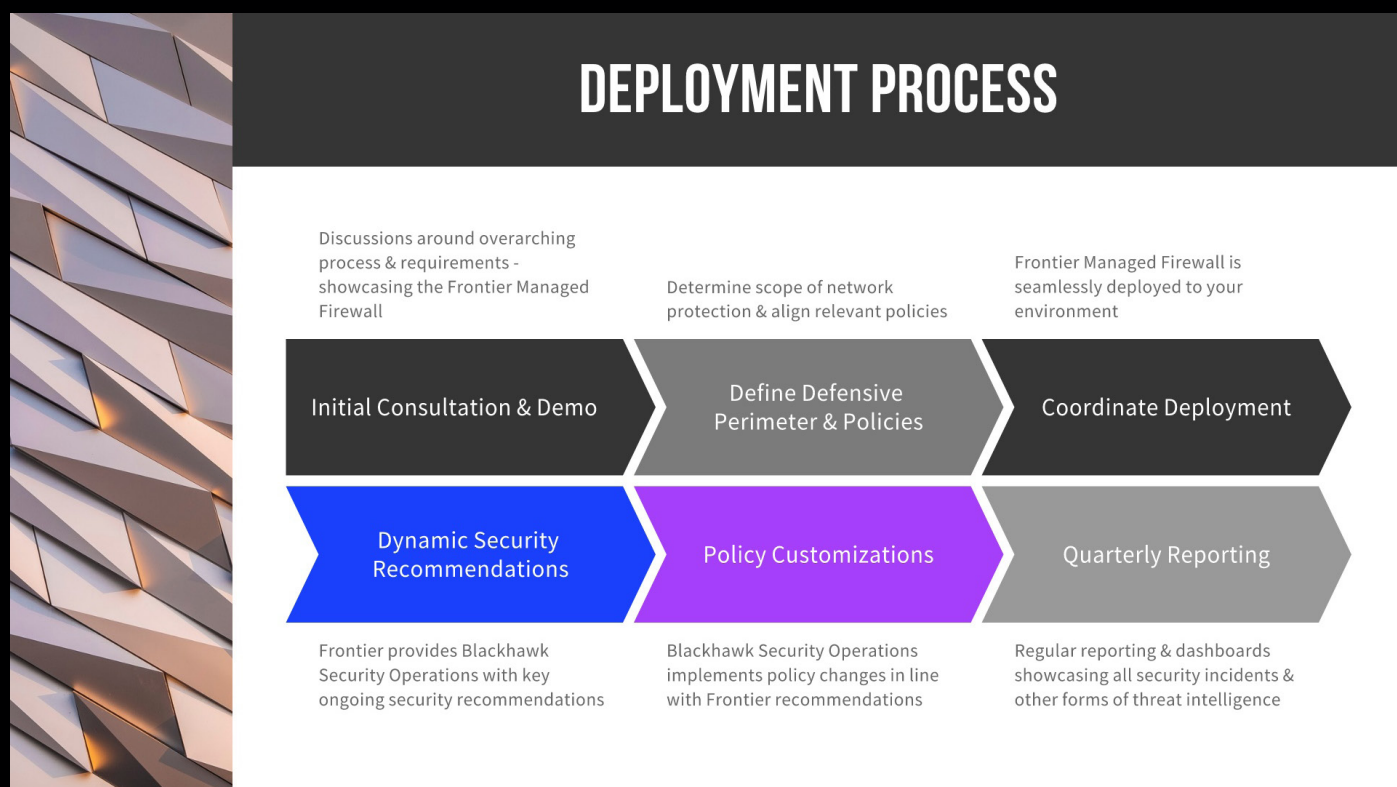




DEPLOYMENT

Deployment for Blackhawk Frontier is incredibly straightforward and seamless.

Blackhawk Alert's service delivery team will remote into your business network in order to install Blackhawk Frontier.



CONCLUSION

Blackhawk Frontier combines best-in-class firewall protection with 24/7/365 security monitoring & remediation. Telemetry with Blackhawk Fortress improves the security and management of your network by maximising visibility into network activity and enabling more efficient threat detection & response.

Blackhawk Frontier provides organisations with the peace of mind that their critical data & systems are protected from potential security threats. By outsourcing firewall management to our security operations experts, organisations reduce their risk of security incidents and can instead focus on their core business objectives.