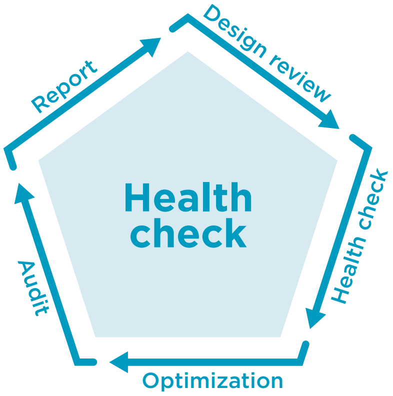
DATASHEET

Palo Alto Health Check

Maximize your investment in Palo Alto Networks next-generation firewalls

Purchasing a Palo Alto Networks firewall is only the first step to securing your network perimeter. At Coalfire, we are dedicated to helping you maximize your investment.

One of our consultants will review your deployment and make recommendations to ensure adherence to best practices when implementing your Palo Alto firewall.



DESIGN REVIEW

Coalfire will analyze the architecture and design of your Palo Alto firewalls. During the review, we will:

- Review design requirements, priorities, and your organization's objectives.
- Review and provide PAN-OS version recommendations based on the latest security advisories.
- Review and provide recommendations for any applicable design issues.

HEALTH CHECK AND CONFIGURATION AUDIT

Our consultants will examine:

- Hardware performance and the general health of your firewalls
- Traffic, Application Command Center (ACC), WildFire, and system logs – and then make recommendations where appropriate
- App-ID, User-ID, Content-ID, WildFire, high availability, security policy, and GlobalProtect configurations

OPTIMIZATION

Our consultants make recommendations on ways to efficiently utilize everything that a Palo Alto firewall has to offer, such as Panorama, logging solutions (i.e., security information and event management), botnet reports, and WildFire reports for emailing notifications to network and security operations center (SOC) teams.

REPORTING

We conclude our formal assessment with a health check report, which details our findings, areas for improvement, and why it is important to remediate. In addition, a summary of our recommendations will be sorted according to priority.

Whether you are new to Palo Alto firewalls, or need to prepare for a regulatory audit, Coalfire will provide you with the expertise required to improve your ability to make full use out of next-generation firewall capabilities.

Maximize your ROI and protect your network with help from Coalfire. | coalfire.com | 877-224-8077

About Coalfire

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe. **Coalfire.com**

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.