# PALO ALTO NETWORKS APP FOR QRADAR

## Increase Visibility and Take Action on the Most Critical Security Events

### Benefits

- Complete visibility of actionable events in the QRadar dashboard
- Reduce, prioritize and correlate alerts from the Palo Alto Networks platform
- Trigger QRadar offenses with alerts from the Palo Alto Networks platform, enabling automated response workflows
- Increase QRadar's network visibility with searchable custom fields from the Palo Alto Networks platform

The widely used IBM® QRadar® SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. Now customers have a way to seamlessly integrate the Palo Alto Networks® platform into the QRadar SIEM in a way that streamlines operations and improves security. The Palo Alto Networks app for QRadar enables these capabilities by allowing the security operations team to reduce, prioritize and correlate Palo Alto Networks events using the QRadar dashboard. Furthermore, offenses and offense workflows can be created automatically, enabling rapid response to the most critical threats from a single dashboard.

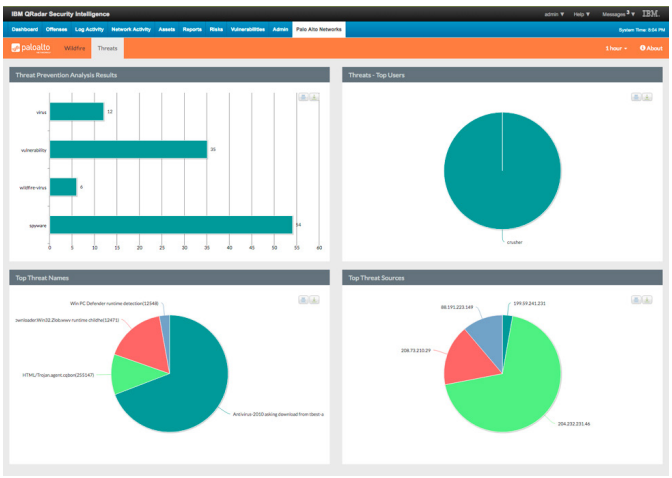
## Rapid Response Enabled by WildFire Threat Intelligence

The Palo Alto Networks platform analyzes every file that traverses the network and determines if the file is known benign, known malicious or unknown. Unknown files are passed to the WildFire™ cloud-based threat analysis service, which uses both static and dynamic analysis techniques to determine if the file is malicious or benign. WildFire will return a verdict in five minutes or less. If the verdict is malicious, it is important for the security operations team to take action and ensure that the file is removed and any associated damage mitigated. When an unknown file is downloaded and then determined to be malicious, rapid response is essential to minimize the risk.

The Palo Alto Networks app for QRadar enables an immediate response when WildFire determines that a previously unknown file is malicious. The app can automatically create an offense, show it on the QRadar dashboard, and trigger an automated workflow.

## Increased Visibility of Network Threats

Security threats are a constant in today's large distributed networks. Visibility is key to making informed decisions on the priority of threats and the best course of action to reduce risk. The Palo Alto Networks app for QRadar includes custom dashboards for both threat and WildFire activity, giving the security operations team aggregated views that can illuminate trends and enable rapid response. These dashboards provide instant visibility to top threats, top users, top source IP addresses, top malware filenames and more. Each of the graphs can be clicked to reveal the underlying log data. Drilling down brings the user to a QRadar Log Activity panel with a custom filter built to facilitate deeper analysis.




## Ready to Get Started?

Contact your IBM representative today at 877.257.5227, visit https://ibm.biz/Bd476Y, or email **ibm@paloaltonetworks**.com, and we will help you understand and overcome the security challenges your teams are facing in the digital age.

## About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow **@IBMSecurity** on Twitter, or visit the IBM Security Intelligence blog.

## About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

Find out more at www.paloaltonetworks.com.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com