

EXCLUSIVE OFFER

JUNIPER NETWORKS® ADVANCED THREAT PREVENTION APPLIANCE

DETECTION

Monitors network traffic to identify external and internal threats such as exploits, malware downloads, and C&C communications.

ADVANCED THREAT ANALYTICS

Provides a holistic view of identity information and threat activity gathered from an array of diverse sources.

MITIGATION

Automatically mitigate threats inline and isolate infected hosts with one-touch mitigation through Juniper Networks SRX Series Services Gateways.

ADVANCED THREAT AND MALWARE DETECTION, CONSOLIDATED SECURITY ANALYTICS, AND QUICK THREAT MITIGATION

Around the world, organizations are increasingly unable to detect zero-day malware because traditional security devices, which rely on signature-based detection, can't see it. Adding to the problem, security teams—overwhelmed by large volumes of alerts—often fail to recognize and act on critical incidents.

Combining advanced threat detection, consolidated security analytics, and one-touch threat mitigation, Juniper ATP Appliance is a distributed software platform that protects organizations from cyber attacks and improves the productivity of security teams. The ATP Appliance detects threats across web, email, and lateral traffic and can ingest logs from security devices to present a consolidated view of all threats in the environment.



STATIC ANALYSIS

Applies continuously updated rules and signatures to find known threats that may have eluded inline devices.



PAYLOAD ANALYSIS

Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious web and file content that would otherwise target Windows, OSX, or Android endpoint devices.



MACHINE LEARNING AND BEHAVIORAL ANALYSIS

Employs patent-pending technologies to recognize the latest threat behaviors (such as multicomponent attacks over time), and quickly detect previously unknown threats.



MALWARE REPUTATION ANALYSIS

Compares analysis results with similar known threats to determine whether a newly detected threat is a variant of an existing issue or something completely new.



PRIORITIZATION, RISK ANALYSIS, CORRELATION

Prioritizes threats based on threat severity, asset targets in the network, endpoint environment, and the threat's progression along the kill chain.

HOW TO REGISTER

Contact the partner to find out more about the offer

ABOUT JUNIPER NETWORKS

Juniper Networks simplifies the complexities of networking with products, solutions and services in the cloud era to transform the way we connect, work and live. Through engineering and innovation, we remove the traditional constraints of networking to enable our customers and partners to deliver automated, scalable and secure networks that connect the world.

Engineering Simplicity

www.juniper.net

Copyright 2018 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.