EXHIBIT 12

Products & Services

Advanced Threat Prevention Appliance

Comprehensive threat and malware detection, consolidated security analytics, and quick threat mitigation.

DATASHEET

REQUEST A QUOTE

HOW TO BUY

Overview

The Advanced Threat Prevention Appliance provides comprehensive on-premises protection against a sophisticated, ever-changing threat landscape.

With traditional signature-based security tools, zero-day attacks often go undetected. The Juniper ATP Appliance uses advanced machine learning and behavioral analysis technologies to identify existing and unknown advanced threats in near real time. It does this through continuous, multistage detection and analysis of Web, email, and lateral spread traffic moving through the network.

The ATP Appliance ingests threat data from multiple security devices, applies analytics to identify advanced malicious traits, and aggregates the events into a single comprehensive timeline view of all the threats on the network. Your security team can quickly see how the attack unfolded and easily prioritize critical alerts.

Integrated SRX Series firewalls inspect traffic, submit suspicious files to the threat behavior engine, and update the ATP Appliance with threat status, accelerating time to detection and initiating inline blocking.

With its open API architecture, the ATP Appliance integrates with third-party security devices for seamless, automatic threat mitigation. You can quarantine emails on Google and Office 365 using REST APIs. Malicious IP addresses are pushed to firewalls to block the communication between command-and-control (C&C) servers and infected endpoints. Infected hosts are isolated through integration with network access control devices.

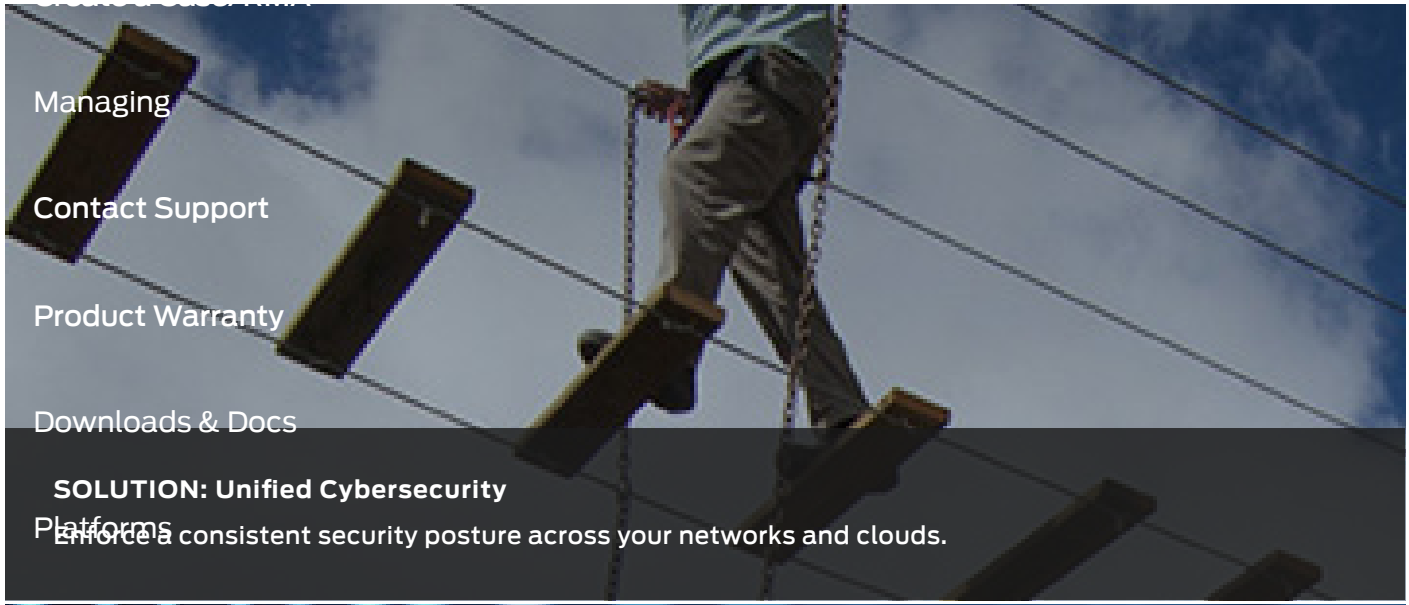
The Advanced Threat Prevention Appliance is available in physical and virtual form factors. You can deploy physical appliances in all-in-one or distributed mode, and virtual appliances in distributed mode only.

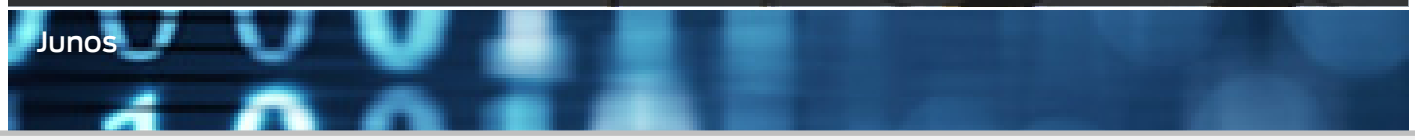
READ LESS

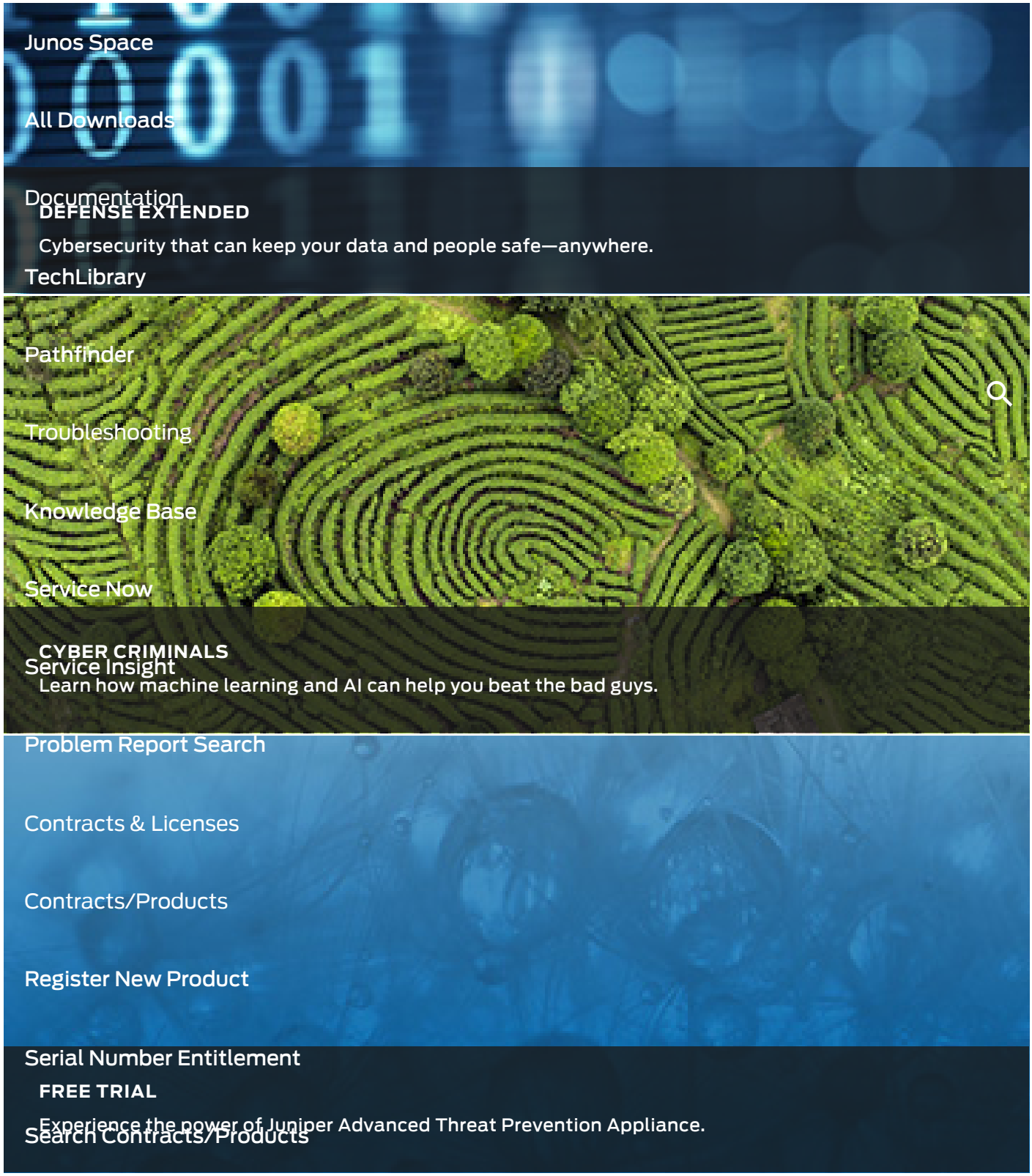
Up to
2
Gbps Performance

Up to
96
GB Memory

Up to
80K
detonations/day







Features

Multivector Traffic Inspection

Multiple File Type Analytics

Analyzes multiple file types, including executables, DLL, Mach-o, Dmg, PDF, Office, Flash, ISO, ELF, RTF, APK, Silverlight, Archive, and JAR.

Effective Detection Techniques

Employs advanced threat detection techniques, including exploit detection, payload analysis, C&C detection, YARA, and SNORT rules.

Endpoint Integration

Integrates with Carbon Black Protect and Response (endpoint solution) to allow upload of binaries executed on endpoints.

Extensive Data Correlation

Correlates events across kill chain stages to monitor threat progress and risk; visualizes malware activity and groups malware traits to help incident response teams better understand malware behavior.

Contextual Threat Prioritization

Prioritizes threats based on risk calculated from threat severity, threat progress, asset value, and other contextual data.

Host Behavior Timeline

Provides timeline host view to obtain complete context about malware events that have occurred on the host.

Automated Threat Mitigation on Email, Web, and Lateral Traffic

Quarantines malicious Office 365 and Google emails automatically; integrates with Bluecoat, Checkpoint, Cisco, Fortinet, and Palo Alto Networks solutions to automatically block malicious IP addresses and URLs.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.