Summer Working Connections Palo Alto Networks Topics

- Cybersecurity Academy program
- Application Framework Introduction
PALO ALTO NETWORKS AT A GLANCE

Founded in 2005; first customer shipment in 2007

More than 48,000 customers in 150+ countries

FY18 Q2 $542M revenue,

28.4% YoY growth that significantly outpaced the industry

Over 85 of the Fortune 100 and 63% of the Global 2000 rely on us

Ranked an enterprise firewall market leader by Gartner six times

Excellent global support, awarded by J.D. Power and TSIA

Experienced team of more than 4,900 employees
**Security Operating Platform**

**Next-Generation Firewall**
- Identifies and inspects all traffic
- Blocks known threats
- Sends unknown to cloud
- Extensible to mobile and virtual networks

**Threat Intelligence Cloud**
- Gathers potential threats from network and endpoints
- Analyzes and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

**Advanced Endpoint Protection**
- Inspects all processes and files
- Prevents both known and unknown exploits
- Integrates with cloud to prevent known and unknown malware
Palo Alto Networks Cybersecurity Academy

- We provide training to your faculty on our security operating platform
- We provide course curricula for your students to use on our Academy Moodle
  - We use the NIST/NICE cybersecurity framework for our student learning outcomes
  - We have Pearson VUE exams aligning with our academy curricula
  - We provide student lab instructions
- We provide our fully licensed virtual firewall appliances for your student labs
- We do all this currently at no cost
Academy Curriculum Roadmap with Integrated Tracks

Academic Track
- Aligns to the U.S. National Initiative for Cybersecurity Education (NICE) framework and cybersecurity work roles

Technical Track
- Aligns to Palo Alto Networks job roles
- Must be taught over an academic term

PCCT – Certified Cyber Security Technician Certification
- Cybersecurity Prevention & Countermeasures
- Cybersecurity Infrastructure Configuration
- Firewall Essentials – Configuration and Management (210)
- Firewall Troubleshooting (330)
- Panorama Managing Firewalls at Scale (220)
- Optimizing Firewall Threat Prevention (214)

PCNSE – Certified Network Security Engineer
- Firewall Essentials – Configuration and Management (210)
- Cybersecurity Essentials (Network Security Essentials)
- Cybersecurity Gateway (Networking Fundamentals)
- Cybersecurity Foundation (Introduction to Cybersecurity)

PCEC – Cybersecurity Essentials Certification
- Cybersecurity Essentials (Network Security Essentials)
- Cybersecurity Gateway (Networking Fundamentals)
- Cybersecurity Foundation (Introduction to Cybersecurity)
Authorized Academy Centers – 335+ in 45 Countries

Available to any degree-granting, nationally accredited university or college
Cybersecurity Academy Student Lab Environments – 4 Options

1. Use NetDevGroup’s online Netlab+ appliance PANW lab pod
   •  [https://www.netdevgroup.com/online/content/paloalto/](https://www.netdevgroup.com/online/content/paloalto/)
   •  $50 per student per semester

2. Purchase your own Netlab+ appliance to run on your vCenter/ESXi datacenter.
   •  Acquire our lab pod master VMs from CSSIA, [www.cssia.org](http://www.cssia.org), and installation instructions
   •  Contact Agata at CSSIA, Rawdanik@morainevalley.edu
Cybersecurity Academy Student Lab Environments – 4 Options (cont)

3. Use VMware Workstation lab pod
   • Workstation labs documents are in Moodle courses
   • Workstation ova’s can be downloaded from our Box share folder

4. Use our VM firewall virtual appliance and Lab VMs on your hypervisor of choice
How to become a Cybersecurity Academy

- Have an authorized representative sign our Authorized Academy Center (AAC) Agreement
  - [https://www.paloaltonetworks.com/services/education/academy](https://www.paloaltonetworks.com/services/education/academy)
Palo Alto Networks
Application Framework
Introduction
The challenges of a changing threat landscape

Changing threat landscape requires rapid deployment of new technologies
Complex and manual workflows across dozens of security products
New security product deployments have up-front ROI risk and cost
The state of delivering and consuming security innovation

Customer challenges

• Evaluating and deploying the latest security innovations to keep up with the changing threat landscape

• Cost and management overhead of deploying yet another product on the network or endpoints

• Large up-front risk of investment in time and security budget with each new rollout

Security vendor challenges

• Overhead of re-inventing network, endpoint, and SaaS sensors/enforcers

• Convincing customers to deploy another product on the network or endpoints

• Infrastructure cost and complexity of data collection, storage, and compute over large customer data sets
CHANGING THE CONSUMPTION MODEL OF SECURITY
Introducing Logging Service
Introducing the Application Framework
Application Framework use-case
3rd Party Application Interaction Overview

User interacts with application
- Add/remove apps
- Jump to apps

App Portal
- Instantiate/destroy
- Setup API auth

Application Framework 1.0
- API Auth Service APIs
- Orchestration Service APIs
- Logging Service APIs
- Event Service APIs
- Directory Sync APIs

Vendor's Cloud
- Web Front-end
- Application

Logging Service
- PAN-OS
- Traps
- Aperture

WRITE
READ
PUB
SUB
READ

AutoFocus
WildFire
Native API
Java API
Application Framework ecosystem
Value for customers

**Superior security:** Innovative new security capabilities from leading providers extend the Palo Alto Networks platform, with consistent enforcement across all users and locations.

**App collaboration:** Apps trigger a single workflow across different providers, including identification, analysis and response actions.

**SaaS-based consumption model:** Cloud-delivered apps can be consumed and updated quickly with no additional infrastructure & offer predictable OpEx.
Value for app developers

**Seamless customer adoption:** Reach nearly 40,000 Palo Alto Networks customers without having to develop, sell and deploy additional hardware.

**Data access:** Tune your machine learning, threat intelligence or other application logic with access to our customer-specific data store.

**Speed to market:** Accelerate the delivery of innovative apps with a unique SaaS-based consumption model.
Palo Alto Networks Venture Fund

$20M innovation fund
In collaboration with Greylock Partners and Sequoia Capital
Driving entrepreneurship for the Application Framework
Application Framework summary

- **Superior security** with high degrees of consistency by reinventing how customers rapidly **access, evaluate and adopt** the most compelling new security technologies.

- An **extension** of the Next-Generation Security Platform they **already own** and operate.

- Allows the adoption of **compelling cloud-based apps** developed by Palo Alto Networks and today’s most **innovative** security providers, large and small.
Prevention is possible with the real security platform