



## L'EVOLUZIONE DELLA CYBERSECURITY PER UNA SANITÀ DIGITALE SOSTENIBILE

*«Redefining curricula and educational path is one of the major challenges regarding the cybersecurity skill shortage».*  
Source: ENISA | Challenge in Cybersecurity Education and Training

**Pietro CARUSO**  
Public Sector Team Lead, Italy & Malta  
[pcarus@paloaltonetworks.com](mailto:pcarus@paloaltonetworks.com)

#sanita2030



[www.sanita2030.it](http://www.sanita2030.it)



### 3 Major Trends drive the Cybersecurity Landscape forward



#### Geopolitics

Nation-state actors, hired guns and hacktivists **target critical infrastructure** in energy, finance, healthcare, etc.

**Supply chain** disruption and **component shortages** impact hardware delivery lead time



#### Digitization

**60%+** corporate data is **stored in the cloud**, and 80% have hybrid strategies mixing public & private clouds

**188%** yoy increase in **Cloud Incidents**



#### New Work Paradigm

**76%** employees want to keep **working from home** part of the week

**61%** organizations say they are struggling to **secure the hybrid workforce**





## The world's security leader

#1

in Enterprise Security  
 by revenue size

**95k+**

Customers globally  
 in 150+ Countries

**\$5.5B**

Revenue in FY'22  
 with 29% growth yoy

**\$7.4B**

Total Billings in FY'22  
 with 40% growth yoy

**90**

of Fortune 100 rely on  
 Palo Alto Networks

**9/10** avg CSAT

rated Outstanding  
 Customer Service  
 7 years in a row

**14k+**

Employees globally

#sanita2030

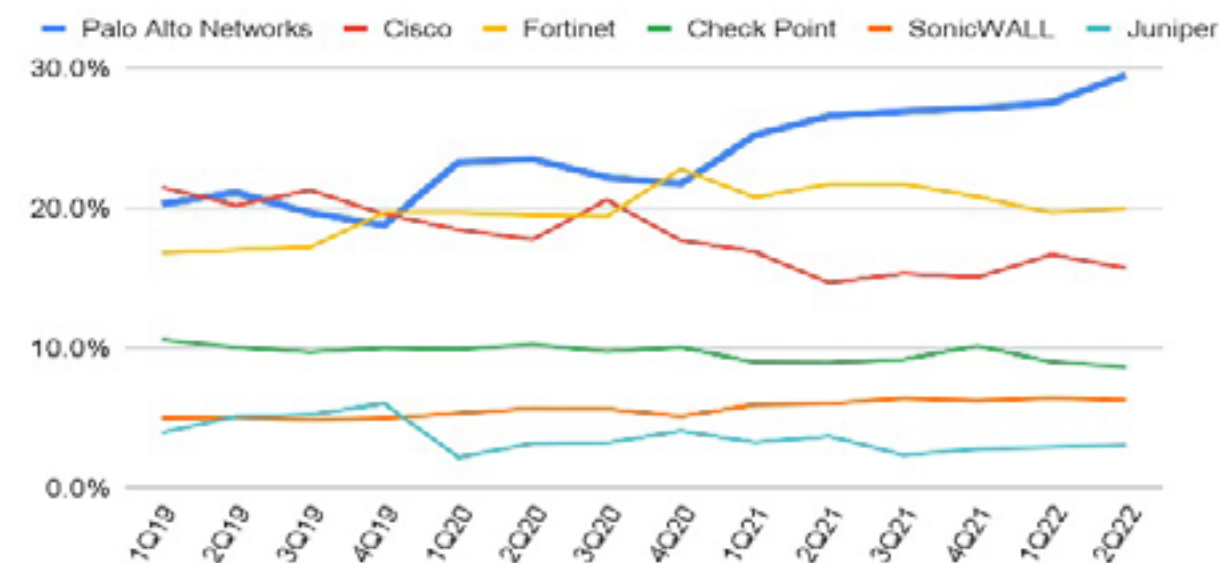


www.sanita2030.it



The strength of Palo Alto: **enviable financial position**

NGFW Market Share



Palo Alto Networks Annual Research and Development Expenses (Millions of US \$)

2022	\$1,418
2021	\$1,140
2020	\$768
2019	\$540
2018	\$401
2017	\$347
2016	\$284
2015	\$186
2014	\$105
2013	\$62
2012	\$39
2011	\$21
2010	\$13

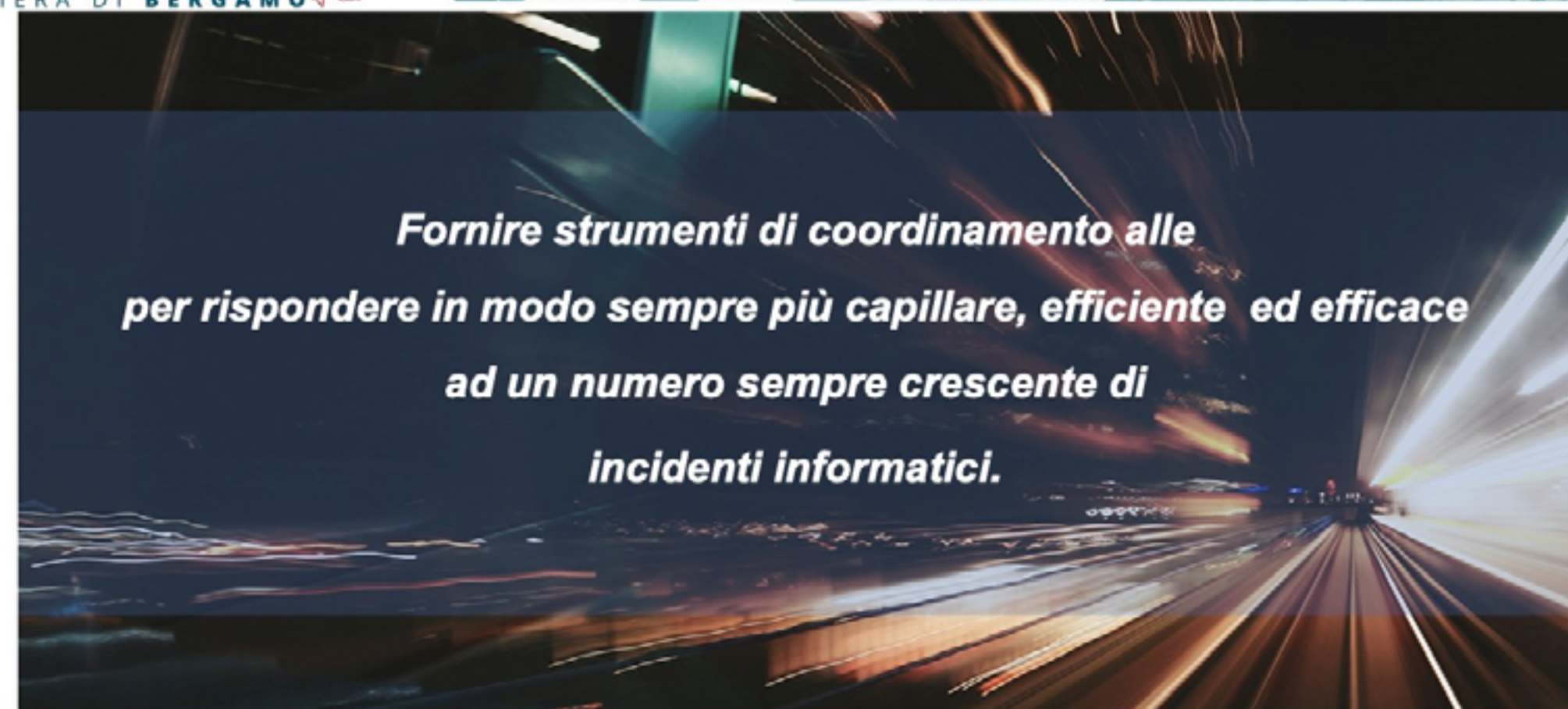
#sanita2030



www.sanita2030.it







#sanita2030



[www.sanita2030.it](http://www.sanita2030.it)







**UNIT42: cooperazione verticale ed orizzontale**

178 ORGANIZATIONS	FOUNDING INDUSTRY PARTNERS
	<p><b>TIPS</b> Trusted Information Partner Sharing</p>

#sanita2030

Principio di Solidarietà Digitale: + analisi, + telemetriA, + ML, + AI



www.sanita2030.it







**Palo Alto Networks Italy: collaborazioni istituzionali**

 <b>CERT-AGID</b> Computer Emergency Response Team AGID	IoC Sharing National Platform
 <b>MINISTRO</b> PER L'INNOVAZIONE TECNOLOGICA E LA DIGITALIZZAZIONE	Solidarieta' Digitale
 <b>MINISTERO</b> DELLA DIFESA	XSOAR: Soc Automation Defence platform (COR, SMD, NAVY, ARMY, AIR FORCE, CARABINIERI)
 <b>AGENZIA PER LA</b> CYBERSICUREZZA NAZIONALE	SaaS Marketplace Certified
 <b>Cybersecurity</b> Academy	Cybersecurity Academies

#sanita2030



[www.sanita2030.it](http://www.sanita2030.it)



## 1° National MOU in Public Sector: 2019



### AGID National MoU includes collaboration on specific issues related to Cyber Threat Intelligence

- Development of National Pilot – STIX & TAXII protocols
- Use & Integration of open source tools between **CERT AGID** and **Regional CERTs** for automated IoC sharing
- **Info-sharing** of sensitive Cybersecurity related to potential threat ([UNIT42](#))
- TISP Program subscription – **Threat Information Sharing Program** by Palo Alto Networks ([UNIT42](#))
- Trusted Advisory role on **"National Platform"** to contrast **Cyber attacks** (technical collaboration)
- Awareness on Info-sharing between Central and Local Public Administrations to improve cyber security through the use of CORTEX service platform

#sanita2030



www.sanita2030.it







Programma Nazionale di Threat Information Sharing: TISP

Condivisione delle **Best Practices** e diffusione del modello di **Infosharing**  
 tra servizi anticrimine, agenzie, strutture diplomatiche, servizi militari, aziende

- Actionable Threat Object Mitigations (ATOMs) via MISP, TAXII, ...
- Comunicazioni di **Early Warning** via email
- **Report** trimestrali sulle minacce
- **Scambio** di sample di malware
- **Ricerca** collaborativa
- Review **Meeting**
- **Formazione**

#sanita2030



www.sanita2030.it







## Qualificazione nel Cloud Marketplace della PA

**IT** Il cloud della PA

Soluzioni e servizi Cloud di Palo Alto Networks certificate presso il Marketplace di AGID

**CSA** cloud security alliance<sup>®</sup>

Riconoscimento Cloud Security Alliance

**ISO 27001**

ISO-27001 compliant

**ACN**

Qualificazione di tutte le soluzioni SaaS nel Cloud della PA secondo specifiche dettate dall'ACN

The screenshot shows the AGID Cloud Marketplace interface for Palo Alto Networks. It lists various products such as Prisma Cloud, Prisma SaaS, Prisma Access, Cortex XDR, Cortex XSIAM, and Panorama. Each product entry includes a brief description, the provider (Palo Alto Networks Italia S.p.A.), and the qualification date (18/11/2019).

#sanita2030

www.sanita2030.it





Cloud Marketplace La piattaforma che espone i servizi e le infrastrutture qualificate da ACN secondo quanto disposto nel [Decreto direttoriale prot. N. 29 del 02/01/2023](#).

TIPOLOGIA

- Infrastruttura
- SaaS
- PaaS
- IaaS

LIVELLO DI QUALIFICAZIONE

CAMPI

STATO

- qualificata
- scadenza
- in attesa
- qualificata ma non disponibile

FORNITORI

palo

Numero risultati: 19

[Continua a pagina 2](#)

Visualizza come griglia Ultimo aggiornamento

QUALIFICATA	QUALIFICATA	QUALIFICATA	QUALIFICATA	QUALIFICATA	QUALIFICATA	QUALIFICATA
<b>SAAS</b>	<b>SAAS</b>	<b>SAAS</b>	<b>SAAS</b>	<b>SAAS</b>	<b>SAAS</b>	<b>SAAS</b>
<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Firewall &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>	<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Cisco Duo Security &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>	<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Cisco Duo Security &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>	<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Cisco Duo Security &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>	<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Cisco Duo Security &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>	<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Cisco Duo Security &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>	<p>Tipologia: SaaS</p> <p>Livello di qualificazione: CC1</p> <p>Denominazione servizio: Cisco Duo Security &amp; Palo Alto Networks</p> <p>Fornitore: Palo Alto Networks (Bentley&amp;Bentley) S.p.A.</p> <p>Data qualificazione: 22/3/2023</p> <p>Data scadenza qualificazione: 21/9/2024</p> <p>VEDI SCHEDA</p>

#sanita2030



[www.sanita2030.it](http://www.sanita2030.it)





**Supply Chain Integrity = manufactured in the U.S.A.**

**Why not ship off the manufacturing and engineering to China as many security vendors do?**

At Palo Alto Networks, we pride ourselves in providing premium security products that not only deliver the highest levels of security but are also developed and manufactured with the highest standards of supply chain integrity.

Network vendors that outsource their products to China for manufacture are at risk of manufacturing or supply chain infiltration.

**At Palo Alto Networks, our premium security products include the hardware manufacturing process.** Security and data protection are at the heart of the Palo Alto Networks mission, ingrained in our hardware product path from design through service. With a wide range of threats possible at any stage in this path, it's vital to have practices and processes in place to prevent potential exposure and keep the product and data secure.

**Next-Generation Firewall hardware design and development are both done in one place!**

Our United States corporate headquarters is in Santa Clara, California. Our hardware manufacturing is done in Milpitas, California, a mere 10 miles from our corporate headquarters.

Palo Alto Networks implements internal and external security controls based on various well-established standards, including but not limited to those from the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) 27001.



#sanita2030



www.sanita2030.it





First time ever in Consip (Cyber2)!

Sicurezza on Premises



Le sei soluzioni proposte in Cyber2 includono i seguenti servizi:

- Threat Prevention (IPS/IDS)
- Wildfire (Sandbox)
- ADVURL (Advanced URL Filtering)
- Panorama (sistema di gestione centralizzato)
- Site-to-Site VPN e Client-to-Site VPN
- Default VSYS
- SDWAN e DNS inclusi (Fascia 1)

Inoltre è previsto di default l'aggiornamento del PANOS, con tutte le sue release come descritto in A. Q. ID-2367.

I NGFW offerti prevedono una **garanzia di 24 mesi**

#sanita2030



www.sanita2030.it





## education



**Redefining curricula and educational paths!**  
Sustain ENISA competences' certification process



#sanita2030



www.sanita2030.it







### Come supportiamo le Aziende Sanitarie Digitali

- **5100 clienti** nel settore sanitario in tutto il mondo, tra cui:
  - 8 dei 10 principali ospedali USA
  - 5 maggiori fornitori di servizi sanitari USA
  - 5 principali organizzazioni farmaceutiche globali
- **Un team dedicato** di esperti del settore sanitario
- Fornitore scelto di servizi di cybersecurity per l'**American Hospital Association**
- Partecipazione attiva ai consorzi del settore
  - **H-ISAC** (Healthcare Information Sharing and Analysis Center)
  - **HIMSS** (Health Information and Management Systems Society)
  - **NIST & NCCoE** (National Cybersecurity Center of Excellence)
  - US Health Sector Cyber Council **405(d) Task Group**
  - **CSA** (Cloud Security Alliance)



#sanita2030



www.sanita2030.it



paloalto | **IGNITE**  
ON TOUR

Ignite On Tour Milano

20 giugno 2023  
Orario: 09:30 - 18:30

East End Studios - Studio Novanta

Registrati

«Guidato dall'intelligence, pronto alla risposta»

Wendy Whitmore, Senior VP Unit 42, Palo Alto Networks

In passato gli stati nazionali erano trendsetter nell'innovazione del threat. Le cose però cambiano velocemente e oggi ci sono nuovi aspetti da valutare. La buona notizia è che Unit 42 sa cosa succederà in futuro. In questa sessione daremo uno sguardo a Unit 42, threat intelligence e incident response riconosciuta a livello mondiale. Vi riveleremo le tecniche emergenti nell'ambito delle minacce per prepararvi al futuro.

La sessione sarà in inglese con traduzione simultanea

#sanita2030



www.sanita2030.it







**THANK YOU**



#sanita2030



[www.sanita2030.it](http://www.sanita2030.it)



### **Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]**

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

**[Torna all'inizio](#)**