10FOUR SOLUTIONS

Redefine **Next ...**

Company profile and Solutions Portfolio

January 2024

10Four Solutions - Technology capabilities and Solutions Brief

10Four Solutions (https://10four.org/) is a Cyber-Security Technology and Services Provider of Next-Gen Network Security and Privileged Identity Security solutions that services customers in North America.

Our Technology Solutions Portfolio - built in partnership with leading Cyber Security providers such as Palo Alto Networks and CyberArk - Protects customer applications from zero-day threats with agile, best-in-class security for all IT infrastructure clouds — public, private and hybrid.

The 10Four Solutions Technology practice:

- Resells, builds/integrates and remotely manages Network and Identity Cyber-Security services that deliver business outcomes for customers.

- Provides services (Consulting, Professional and Training) to address customer demand for networking and identity security solutions.

- Partners with leading cloud-based network and identity security solution platforms, infrastructure and/or storage services to provide Technical Pre-Sales, Post-Sales support to solutions deployed at customer premises or in-cloud.

- Works with our Vendors to identify customer opportunities, manage deal registrations and provide solution technical support through the entire project life-cycle.

- Our Engineers implement Zero-Trust-Network-Access security solutions to protect customer assets in accordance with US Govt. recommended security guidelines.

- Provides Enterprise Identity Security solutions and blueprints for identity asset protection.

Design and assessment
Design your enterprise protection roll-out

QuickStart and migration
Quickly deploy and adopt capabilities for control of you network

Optimization and automation
Enable your operations team and provide incident automation

Ongoing consulting
Provide continuous expertise and consulting for extended projects

10Four Solutions NSS Portfolio – Network Security Services (NSS)

Hardware PA-Series	Software VM-Series / CN-Series	Cloud Service Prisma Access

High Performance Physical Appliances

Virtual Software VM & CN Series

Cloud Delivered Security

Network Security Platform - Cloud Delivered Security Subscriptions

TP
Threat Prevention

Prevent all known threats across all traffic in a single pass

UF
URL Filtering

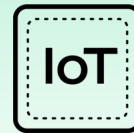Prevent access to known and new malicious websites

WF
WildFire

Ensures files are safe with automatic detection and prevention of unknown malware

DNS
DNS Security

Disrupts attacks that use DNS for command-and-control and data theft

IoT
IoT Security

Visibility and protection of IoT and OT devices

DLP
Data Loss Prevention

Consistent protection from sensitive data loss

GP
Global Protect

VPN service to extends NGFW capabilities everywhere

SD-WAN
SD-WAN

Networking and security natively integrated

3

10Four Solutions NSS Portfolio – Threat Prevention Capabilities

10Four Solutions Security Framework prevents successful cyber attacks. We make sure that deployed protection capabilities are best in class.

"Rule of All": We protect **all** ports, **all** protocols, **all** applications, **all** users, **all** devices, with **all** security features enabled, **all the time**. Our firewalls only run in a single mode - "secure", unlike other Vendor solutions, which require constant trade-offs between security and performance.

Gain Complete Visibility	Reduce Attack Surface Area	Prevent All Known Threats	Prevent and Detect Unknown Threats
• All Applications	• Block "Bad" Apps	• Exploits	• Dynamic Analysis
• All Users	• Limit App Functions	• Malware	• Exploit Techniques
• All Content	• Limit File Types	• Command & Control	• Malware Techniques
• All Devices	• Block High-risk Websites	• Malicious Websites	• Machine Learning
• All Endpoints	• Verify Users	• Bad Domains	• Static Analysis
• Encrypted Traffic	• Limit Devices	• Stolen Credentials	• Anomaly Detection
• Saas & Cloud	• Control Sharing		• Analytics
• Mobile			

Consistent Across all Locations

Headquarters	Branch Offices	Data Center/ Private Cloud	Public Cloud	SaaS	Mobile Users	IoT

10Four Solutions NSS Portfolio – Managed Security Services (MSSP)
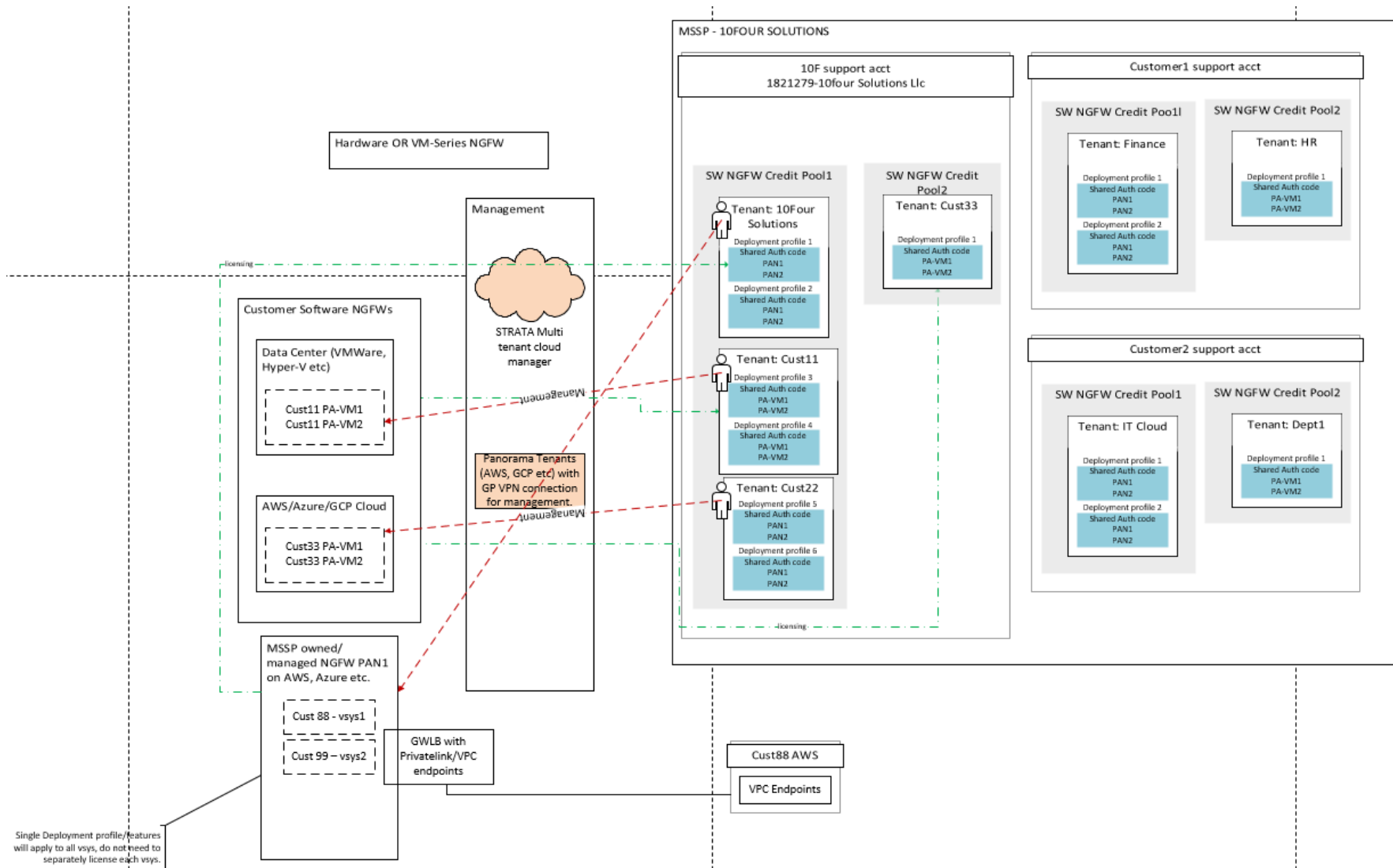
10Four Solutions provides end-to-end hands-off Managed Network and Managed Identity Security Services to our Customers.

- **Managed Firewalls** – 10Four-owned, Customer-owned, Co-owned Software Licensing, Firewall Hardware, private/public Cloud Virtual Firewall Infrastructure.
- **10Four-Managed Hosted Next-Generation Firewall solutions** on Amazon Web Services, Google Cloud Services or Microsoft Azure
- **10Four-Managed Firewall Management products** such as Panorama, Strata Multi-Tenant Cloud Manager.
- **Managed Support** for Customer Tenants.
- Managed Security Service Credit pools.

10Four Solutions NSS Portfolio – Next-Gen AI-powered Firewall hardware

10Four Solutions provides Best of breed modern NGFWs that prevent known and unknown threats by embedding Artificial-Intelligent in-line, deploy security services to protect all applications, and decrypt traffic to prevent threats.

PA-410

PA-450

PA-440

PA-460

PA-445

PA-415

PA-455

PA-415-5G
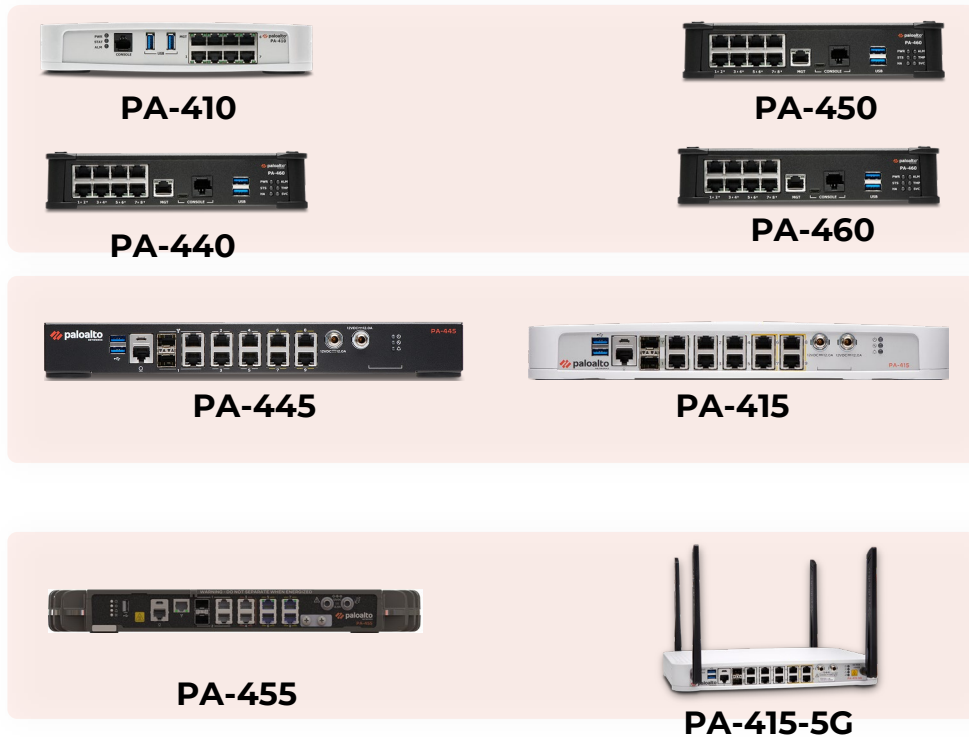
- **Lower TCO** and simplified operations with **zero touch provisioning** and **Panorama Centralized Management**

- **Up to 3.5x performance** over the PA-220, threat performance ranging from **600 Mbps to 3.6 Gbps**

- **Power over Ethernet (PoE) and Fiber** ports enable on PA-445 and PA-415

- **Dual Fiber and PoE ports** for PA-455 enable flexible service deployment

- **5G Modem and Fiber port** for PA-415-5G allows deployment with more service connection options

10Four Solutions Portfolio – Identity Security Services (ISS)

10Four Solutions works with Customers to provide a risk-based approach to Identity Security built around the three most prevalent 'Privileged Identity Risk Pillars':

- **Credential Theft** – The use of techniques such as social engineering, keystroke logging, RAM scraping, and more to harvest passwords, hashes, SSH Keys, or hard coded credentials.
- **Lateral & Vertical Movement** – The movement from machine to machine, both within the same "risk tier" (lateral) (e.g. workstation to workstation) or between risk tiers (vertical) (e.g. workstation to server).
- **Privilege Escalation & Abuse** – The process of elevating privileges to then carry out malicious actions against the organization.

We closely interface with customers to develop, implement and manage an 'Identity Security Blueprint' based on well-understood Identity-Security Recommendations.

Phase 1
- Domain Admins
- Cloud Admins

Phase 2
- Local Admins
- Server Admins
- Workstation Admins

Phase 4
- 3rd Party Vendor Access
- Apps Stage 1: Dynamic
- Cloud VM Instances
- PaaS Admins

Phase 7
- Core Web Applications
- Business Applications

CP1*	CP2	CP3	CP4	CP1	CP2	CP3	CP4	CP1	CP2	CP3	CP4	...
Milestone 1				Milestone 2				Milestone 3				M4

CP = Checkpoint

Phase 3
- Root (including SSH Keys)
- CI/CD Consoles
- Mission Critical Web Apps

Phase 5
- Built-in DBA Accounts
- Personal DBA Accounts

Phase 6
- Least Privilege for Workstations
- Least Privilege for Servers

Phase 8
- Apps Stage 2: Static Applications
- Advanced Authentication for Static
- Windows Services