Secure Azure PMEC with VM-Series

IoT/M2M proliferation with 5G

41.6 bn IoT devices estimated to be connected by 2025, thanks to 5G. This means more targets for cyber attacks

E2E stand alone 5G networks will be cloud-native

75% of State of Cloud Native Security survey respondents believe cloud security tools and solutions are outpaced by threats to their cloud systems

67% increase in cyberattacks

5G use cases supporting business- and mission-critical services will have more definite requirements on connectivity, security and targeted SLAs

Comprehensive 5G Security

Context-driven security at scale that protects your end-to-end 5G infra-structure, with real-time correlation of threats to 5G users and devices

What is Multi-Access Edge Computing?

Multi-Access Edge Computing (MEC) enables enterprises to run workloads closer to endpoints, where data is generated, processed, and consumed. Furthermore, best suited for improving latency and throughput-sensitive user applications such as video analytics, real-time robotics, and IoT services. In many instances, MEC is leveraged with next-generation mobile networks like Private LTE and 5G to efficiently deliver ultra-low-latency networking, applications, and services at the enterprise edge. The deployment of these technologies gives opportunities for new tangible business outcomes. As time-sensitive applications and high-speed networks evolve, MEC will play an integral role in every customer journey, with approximately 75% of all application data residing at the edge by 2025. 5G, IoT, MEC, and real-time AI will liberate business-driving scenarios, with enterprises and service providers at the center of the digital transformation. MEC will enable new use cases, including immediate visibility in a supply chain, supporting augmented and virtual reality for immersive training and education, or empowering the ability to operationalize fully autonomous vehicles.

Customer challenges and needs include...

With the advent of digital transformation, the challenge will be how enterprises secure all endpoints and applications running on MEC. Anticipated benefits may go unrealized if implicit trust is not removed at the device and subscriber level for all applications, data, and protocol layers. Customer needs will include:

- Speed to adopt new services securely in an industry 4.0 environment
- Simple to procure, deploy, manage & monetize 5G & Edge for their customer.
- Simplify integration complexity and securely manage services from the cloud
- Choice of trusted, industry-tailored, and leading solutions.
- Flexibility to change or evolve services securely in an on-demand fashion
- Analyze your data for quick, actionable insights

Azure private MEC, and Private 5G Core and 5G Security:

What is it? Azure private MEC combines network functions, applications, and edge-optimized Azure services to provide enterprise customers with high-performance, ultra-low latency solutions that meet their modern business requirements.

How does it work? As localized data is produced from mobile endpoints on 5G networks, it is routed from Radio Access Network (RAN) to Azure Private 5G Core running on Azure Stack Edge devices, with Palo Alto Networks Next-generation Firewall (NGFW) VM-Series. As packets pass through the NGFW, the 5G application, data, and protocol layer of the traffic are inspected.

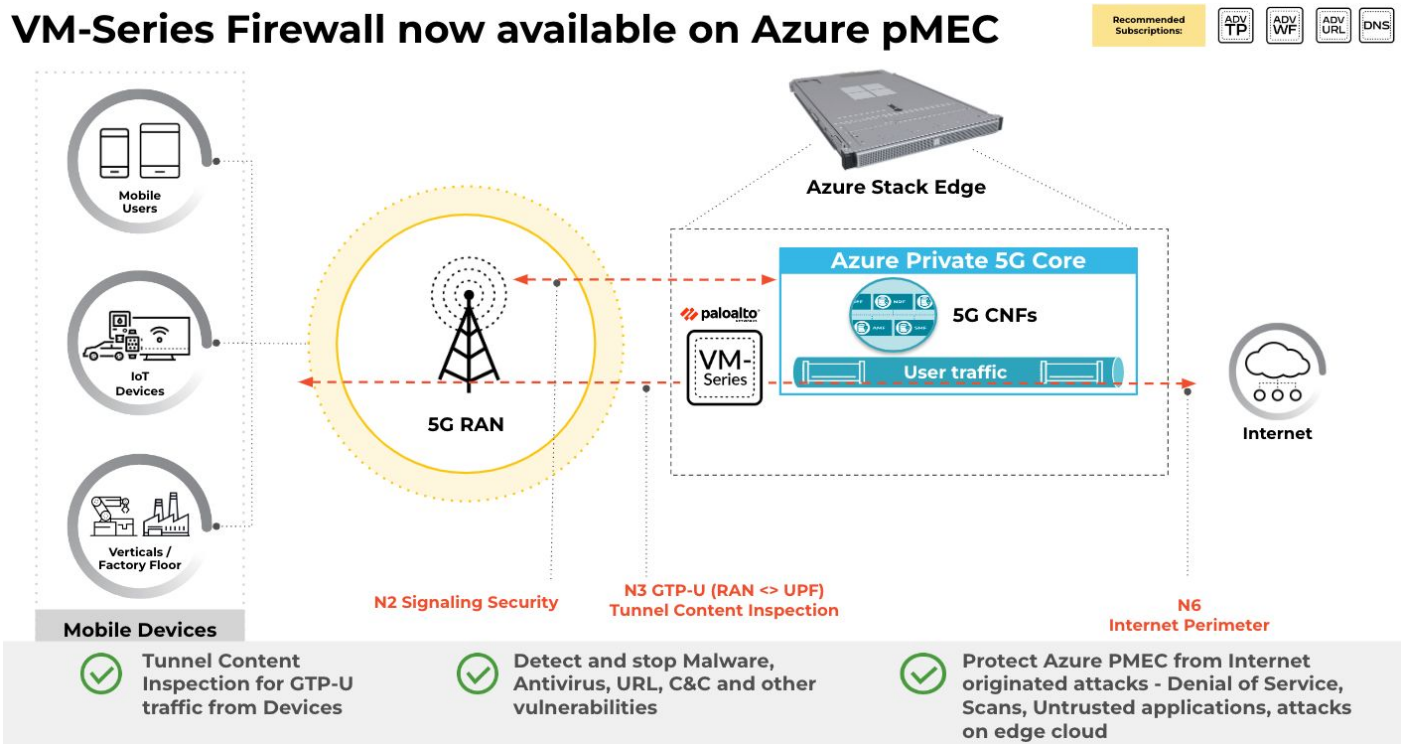
Why it matters? Key enterprise stakeholders are not only responsible for deploying new technologies but also for maintaining compliance through zero-trust network initiatives. As Mobile endpoints, IoT, and new services leveraging MEC continues to grow; it will be critical to deploy new security policies protecting against all attack vectors. Deploy and connect for coverage with 4G or 5G standalone radios in minutes and centrally manage private 5G networks across global sites.

Secure Azure PMEC with VM-Series

What's included ...

Palo Alto Network's capabilities are fully integrated with Azure private MEC solution leveraging ML-NGFW appliances in the form of the VM-Series Edge Azure Application to secure 5G by enforcing security within a GTP-U tunneled User Plane traffic on the N3 interface. The internet perimeter N6 interface of the Azure Private 5G network functions within Azure Stack Edge deployments, including layer-7 app-ID security and threat inspection. This level of granularity ensures real-time inspection through the use of behavioral analytics-based signatures.

- Watch the Product Pitch Video summarizing '*better together*' story for securing Microsoft Azure 5G private MEC with Palo Alto Networks 5G-native security.



Conversations Starters

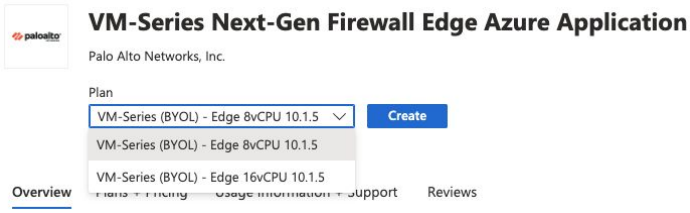
Understanding your customer's business and their digital transformation expedition will be key as you identify and qualify Azure private MEC opportunities with our shared customers. Here are key qualifiers that can help any Core rep or SE/CE to articulate conversations regarding emerging technologies, like MEC and 5G, that will be foundational for enterprises pursuing industry 4.0 solutions.

- Are you a Microsoft Azure user/customer? What Azure Cloud services are you using today?
- Has your organization evaluated private LTE/5G networks to replace or augment your WiFi network?
- Are you planning on deploying a private 5G solution, a managed 5G service (GSI), or both?
- What workloads are running on the edge today? If not, is there a plan to do so?
- How do you plan to protect outbound connections, unknown/unpatched vulnerabilities, and lateral movement?
- How will you monitor your security perimeter as you deploy 5G?
- How do you plan to address the expansion of your security perimeter as 5G fuels the widespread use of IoT devices and the use of new applications?
- How does your organization support data sovereignty and zero trust today?
- What security tools has your organization implemented to meet wireless protocol and compliance?

Secure Azure PMEC with VM-Series

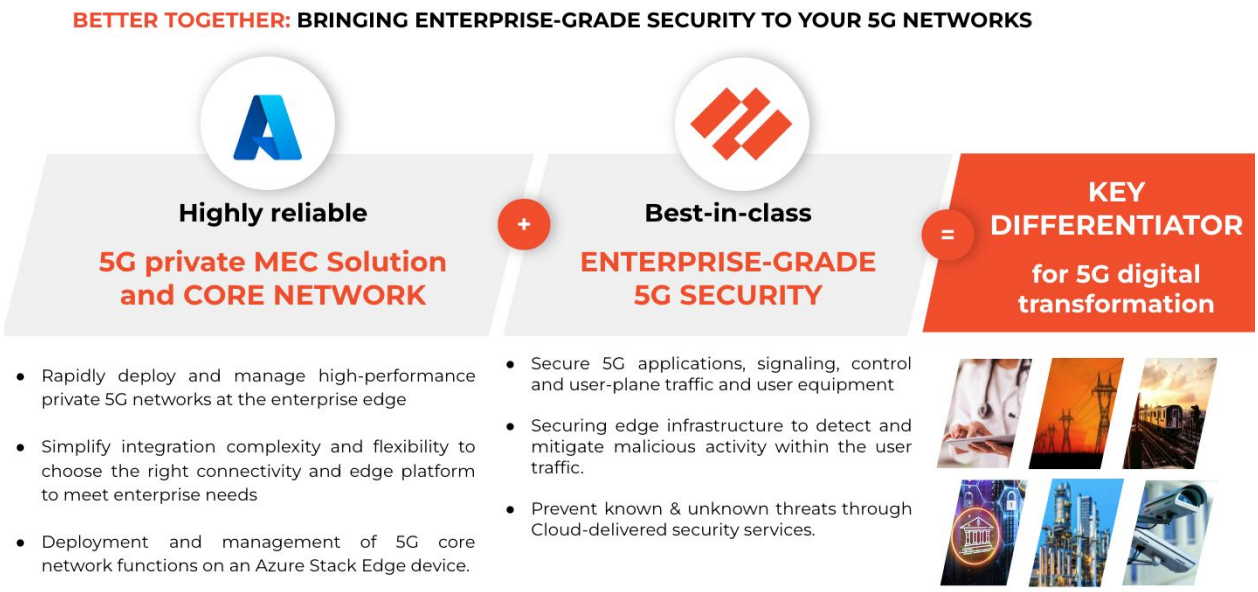
How and When ..

- **Availability: Now , ** See Press-Release **(**accepting proof of concept, discovery phase dialogues with customers**)**
- **Purchase:** Available through Microsoft Azure Marketplace
- **License:** BYOL
- **Choose** VM-series (vCPUs, memory)
  - 8 vCPU VM-Series (need portal access to view)
  - 16 vCPU VM-Series (need portal access to view)



- **PANOS** - 10.2.4 and forward
- **Panorama**: Panorama is required to centrally manage VM-Series instances alongside alongside other Palo Alto Networks firewall appliances to maintain security policy that is consistent with on-premises environments.
- **Deployment of VM-Series -** VM-Series Deployment Guide and Solution Templates

Summary and Bottom Line..



Digital transformation starts with network transformation. As 5G and MEC are adopted at scale to drive innovation, transformation, and growth, enterprises need to ensure that zero-trust environments are employed to support the massive growth in mobility, IoT, and new application enablement. Our unique capabilities include securing 5G RAN, Core and Internet perimeter infrastructure, and 5G signaling and user plane (3GPP N2 and N3). Egress traffic from external to the core network (3GPP N6) with known, unknown & evasive threats through Cloud-delivered Intrusion Prevention, Malware, Web, and DNS security is an industry first. Furthermore, the partnership with Azure provides an unprecedented offer that delivers real value to the enterprise.

For any questions and direct access to 5G subject matter experts, **please email: azurepmec@paloaltonetworks.com**
Additional info on Palo Alto Networks Azure Partner Page and Palo Alto Internal 5G Security Page

