NEXT-GEN Managed Monitored SECURITY PLATFORM Protecting YOUR BUSINESS

JT's Next-Gen Security Platform offer uses Palo Alto's Next-Generation Security Platform to provide Firewalls, advanced Endpoint Protection, and Threat Intelligence for your business including 24/7x365 remote management and monitoring of the firewall and security devices. This is delivered using JT's comprehensive ISO27001-certified, ITIL-aligned service management framework. The service includes proactive configuration, monitoring, performance and capacity management and access to JT's support capability, technical skills and vendor relationship. The offer includes one or more of the following options:

- Firewall appliances
- Traps Advanced Endpoint protection
- Prisma Access cloud-based security infrastructure
- Prisma SaaS application protection
- Annual Security Lifecycle Review

Managed Firewalls

This Next-Generation Firewall is the core of the Next-Generation Security Platform, designed from the ground up to address the most sophisticated threats. The Next-Generation Firewall inspects all traffic - inclusive of applications, threats and content and ties it to the user, regardless of location or device type. The application, content and user - the elements that run your business - become integral components of your enterprise security policy. The result is the ability to align security with your key business initiatives. This allows you reduce response times to incidents, discover unknown threats, and streamline security network deployment.

Supported Devices

Model	Capacity	Form Factor
PA-5200 series	20-68 Gbps firewall throughout	Rack mount
PA-5000 series	5-20 Gbps firewall throughout	Rack mount
PA-3200 series	5-8.8 Gbps firewall throughout	Rack mount
PA-3000 series	2-4Gbps firewall throughput	Rack mount
PA-800 series	0.94 to 1.9 Gbps firewall throughput	Rack mount
PA-500	250 Mbps firewall throughput	Rack mount
PA-220	500 Mbps firewall throughput.	Standalone
PA-220R	500 Mbps firewall throughput	Standalone
PA-200	100 Mbps firewall throughput	Standalone

Supported Configurations

Availablity	Description
Single Firewall	A standalone Firewall
High Availability (HA) Firewall configuration	Two Firewalls of compatible models in an active/passive configuration, both of them connected at the same time.
Firewall Clustering	Two Firewalls of compatible models in an active/active and automatic switch over.

Traps Advanced Endpoint Protection

The Traps™ advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. The Traps agent enforces your security policy on the endpoint and reports when it detects a threat. Traps minimizes endpoint infections by blocking malware, exploits and ransomware. Integration with your security platform delivers additional threat analysis, shared intelligence and automated containment.

Attackers must complete a certain sequence of events to successfully accomplish their objectives, whether stealing information or running ransomware. Nearly every attack relies on compromising an endpoint, and although most organizations have deployed endpoint protection, infections are still common. By combining multiple methods of prevention, Traps stands apart in its ability to protect endpoints. Traps blocks security breaches and successful ransomware attacks that leverage malware and exploits, known or unknown, before they can compromise Windows ®, macOS®, Linux or Android® endpoints, such as laptops, desktops, servers, virtual machines and cloud workloads.

Traps shares threat intelligence, as does each component of the Security Platform. The automatic conversion of this threat intelligence into prevention all but eliminates opportunities for attackers to use unknown and advanced malware to infect systems.

Lightweight Endpoint Agent

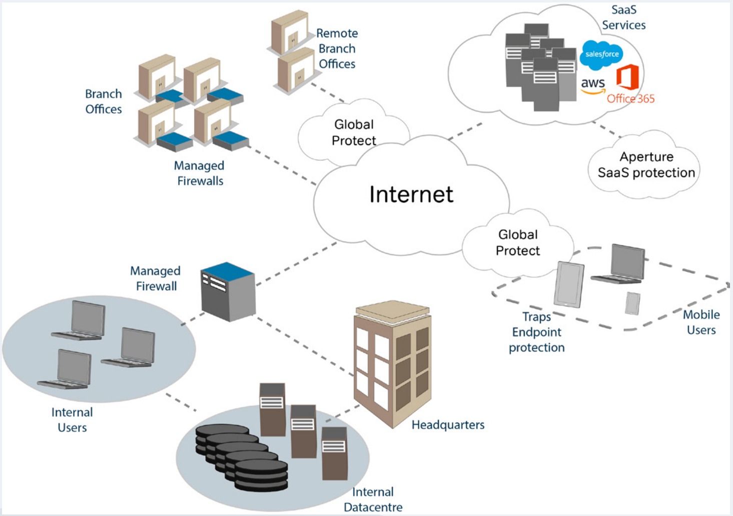
A key reason for the deployment of Traps is its lightweight, non-disruptive agent. The Traps endpoint agent consists of various drivers and services yet requires minimal memory and CPU usage. This results from it's focus on exploit prevention rather than virus identification. This ensures a non-disruptive user experience. Following its deployment, system administrators have complete control over all Traps agents in the environment through the Traps management service.

Prisma Access

Prisma Access reduces the operational burden associated with securing your remote networks and mobile users by leveraging a cloud-based security infrastructure. Based on the next generation security platform, JT manages the Prisma Access with the same Panorama platform it uses to manage your on-premise equipment. This allows us to to create and deploy consistent security policies for all remote networks and mobile users. The Prisma Access allows us to move your remote networks and mobile user security expenditures to a more efficient and predictable OPEX-based model.

Remote Networks

Using Prisma Access for remote networks allows you to extend the prevention philosophy for your corporate network to your remote networks, safely enabling commonly used applications and web access. Remote networks are connected to Prisma Access via an industry-standard IPsec VPN-capable device or SD-WAN fabric. Aperture™ SaaS security can be deployed to complement GlobalProtect cloud service.



Prisma Access for Mobile Users

Mobile users pose a unique security challenge. They need to access corporate and web resources from any device, yet they need the same protection from threats regardless of location. Prisam Access for mobile users enables you to deliver consistent security policies to all users and devices by interacting with the Prisma app on users' devices to provide user and device information for additive security policy enforcement.

Prisma SaaS application protection

Data residing in enterprise-enabled SaaS applications is not visible to an organization's network perimeter. Prisma SaaS has the ability to connect directly to sanctioned SaaS applications to provide data classification, sharing/permission visibility and threat detection within the application. This yields unparalleled visibility, allowing organizations to inspect content for data risk violations and control access to shared data via contextual policy.

Prisma SaaS builds upon the existing SaaS visibility and granular control capabilities of App-ID™ technology within the Security Platform with detailed SaaS-based reporting and granular control of SaaS access. Safely enabling SaaS applications via Aperture provides full end-to-end security without any additional software, hardware or network changes required.

Annual Security Lifecycle Review

The SLR examines your network traffic and generates a comprehensive report unique to your organization to help you discover the applications and threats exposing vulnerabilities in your security posture.

To find out more contact us at:

T +44 20 7920 2000
E sales.jtge@jtglobal.com
W www.jtglobalenterprise.co.uk