GUIA DE LICENCIAMIENTO DE PRODUTOS

Exclusive Networks | Praça Nuno Rodrigues dos Santos 7 214, 1600-171 Lisboa, Portugal | exclusive-networks.com/es

NETWORK SECURITY

Produto/Solução	Tipo	Descrição	Licenciamiento	Requisitos / Detalhes Adicionais
Next-Generation Firewall	Hardware	Inspeciona e controla o tráfego da rede para detetar e bloquear ameaças conhecidas e desconhecidas utilizando o modelo single-pass.	Plataforma base em formato físico. Nas arquiteturas HÁ, ambas equipas devem ter as mesmas licenças. Existem licenças em formato bundle para HÁ com um preço redizído. Subscrições associadas: Threat Prevention, URL Filtering, Wildfire, Global Protect y DNS Security Service.	Disponível em formato físico e virtual. Dimensionamento com base no rendimento/largura de banda requerida. Pode ser estimado em base aos usuários, sessões simultâneas, descodificação SSL, etc.
App-ID	PAN-OS	Identifica nativamente aplicativos utilizando múltiplos mecanismos de identificação.	Incluido na NGFW	Incluído como parte do sistema operacional da plataforma
User-ID	PAN-OS	Permite que as políticas sejam aplicadas para permitir, com segurança, aplicações baseadas em utilizadores ou grupos em ligações de entrada ou saída.	Incluido na NGFW	Incluído como parte do sistema operacional da plataforma
Content-ID	PAN-OS	Inspeciona e filtra o conteúdo no tráfego que passa pelo NGFW, reduzindo os riscos associados à transferência não autorizada de dados e ficheiros. Inclui bloqueio de ficheiros por tipo, permitindo-lhe definir os aplicativos autorizados a transferir ficheiros. Previne a entrada ou saída indesejada de ficheiros, e dispõe de filtragem de dados para controlar a transferência de dados sensíveis (cartões de crédito...)	Incluido na NGFW	Incluído como parte do sistema operacional da plataforma
DoS	PAN-OS	A proteção de DoS, protege sistemas e ambientes críticos de ataques de inundação, especialmente dos serviços acessíveis a partir de Internet, tais como servidores web e servidores de bases de dados, protegendo assim os recursos de possíveis inundações de sessões.	Incluido na NGFW	Incluído como parte do sistema operacional da plataforma
Threat Prevention	Subscription	Protege contra ameaças e vulnerabilidades através da funcionalidade do Sistema de Prevenção de Intrusão (IPS), previne atividades de C&C através do módulo antispyware e impede a transferência de ficheiros maliciosos com a proteção anti-malware.	Associado com o NGFW. Licenciamento independente.	- -
URL Filtering	Subscription	Proporciona uma navegação segura através da Internet, incluindo a proteção dos usuários contra sítios maliciosos e de phishing.	Associado com o NGFW. Licenciamento independente.	- -
DNS Security Service	Subscription	Aplica a análise preditiva para impedir ataques que utilizam o DNS para se ligarem a servidores C&C ou para filtrar informação. A integração estreita com NGFW proporciona proteção automatizada e elimina a necessidade de ferramentas independentes. As ameaças ocultas no tráfego DNS são rapidamente identificadas através da utilização de inteligência partilhada de ameaças e aprendizagem de máquinas. Sendo uma proteção baseada na Cloud, o serviço executa atualizações totalmente dinâmicas, permitindo às organizações um novo ponto de controlo crítico para parar os ataques através do protocolo DNS.	Associado com o NGFW. Licenciamento independente.	Bloqueia novos domínios maliciosos através da aprendizagem automática.. Neutraliza o DNS Tunneling. Substitui os instrumentos stand-alone e melhora os tempos de actualização das ameaças mediante a utilização do Cloud. Requer subscrição Threat Prevention y version PAN-OS 9.0 en NGFW.
Global Protect	Secure Remote Access - VPN	Proporciona segurança a qualquer usuário e dispositivo, em qualquer lugar, através da funcionalidade VPN.	As características básicas de acesso remoto SSL VPN para computadores Windows e Mac estão incluídas como standard sem a necessidade de uma licença adicional. A licença dglobal protect acrescenta funcionalidades SSL VPN aos endpoints com iOS, android, Linux, Chromebooks, Windows 10 UWP, as funções HIP checks e clientless SSL VPN.	"Solução baseada em SaaS; sem implantação de HW Opex offering" Acesso remoto seguro "always-on". Requer NGFW..
Prisma Access	Distributed Enterprise Security	Previne ataques informáticos em sedes, implementações SD-WAN e usuários móveis com todas as capacidades do NGFW, oferecido como um serviço; automatiza a implementação e orquestração de serviços de segurança.	Sedes Remotas: Licenciamento por throughput (minimo 200 Mb) Usuarios: Licenciamento por número de usuarios (200 usuarios)	"Solução baseada em SaaS; sem implantação de HW Opex offering" Requer Cortex Data Lake e se recomenda Panorama
Panorama	Management	Administra e monitoriza centralmente as NGFW. Permite definir configurações, políticas, atualizações e informes de todo o entorno e a partir de uma única consola.	é proposto por numero de FW´s. 3 opções de licença: 25 NGFW, 100 NGFW, +1000 NGFW. Opções de upgrade disponível: 25>100, 100>+1.000 Disponível em appliance e VM.	Requiere NGFW
Expedition (AKA Migration Tool)	Tool	Esta utilidade ajuda a reduzir o tempo e o esforço no processo de migração de outro vendedor para Palo Alto Networks. Inclui características para otimizar políticas e passar da filtragem L4 básica para a proteção L7 ótima, onde os aplicativos e os usuários são definidos.	Ferramienta open-source gratuita.	Adiciona um módulo de aprendizagem automática que lhe permite produzir novas políticas de segurança baseadas em registos e a ferramenta BPA para verificar se a configuração está em conformidade com as melhores práticas recomendadas pelos especialistas em segurança da PANW.

ADVANCED ENDPOINT PROTECTION

Producto/Solución	Tipo	Descripción	Licenciamiento	Requisitos / Detalles Adicionales
Cortex XDR 2.0 (Prevent in Endpoints)	Advanced Endpoint Protection	Solução de protecção do End Point. Impede a execução de ficheiros maliciosos que fazem parte de campanhas de ataque tradicionais e desconhecidas. Os administradores podem realizar análises periódicas para identificar ameaças, cumprir requisitos regulamentares, e acelerar a resposta a incidentes com contexto extraído do ponto final.	"Licenciamento por número de endpoints (mínimo 200). Incluye Wildfire"	Técnicas de prevenção múltiplas: evita malware conhecido e exploits que afectam as vulnerabilidades 0-day. Consola de gestão SaaS. Possibilidade de protecção do end point e do servidor. " Agente compatível com os sistemas operativos da família Windows 7 a W10, Linux, Android e Mac OS (não iOS). Requer Cortex Data Lake (inclui 1 TB grátis)".

CLOUD SECURITY

Virtualized Next-Generation Firewall	VM-Series	Proporciona as características do NGFW numa plataforma virtual para utilização em ambientes de Private Clour ou Public Cloud.	Plataforma base em formato virtual. Nas arquitecturas HA, cada equipa deve ser licenciada por separado. Disponível em 3 bundles: • Basic: Inclui VM+soporte • Bundle 1: Inclui VM+Licencia TP+Soporte • Bundle 2: Inclui VM+Licencias TP+URLF+WF+GP+DNS +soport	Pode ser implantado em ambientes Cloud públicos AWS, Azure, GCP, Alibaba, Oracle Cloud y en clouds privados , VMWare ESX, NSX, KVM, OpenStack, Hyper-V, Nutanix o Cisco ACI. Existe uma opção para consumir em formato Enterprise License Agreement (ELA).
Prisma SaaS	SaaS Security/ Compliance	Estabelece uma ligação directa a aplicações SaaS para proporcionar classificação de dados, prevenção de fugas de dados e detecção de ameaças, para que os clientes possam assegurar suas aplicações SaaS corporativas.	Licenciamento por número de usuários. A licença actual cobre todos os aplicativos que se deseja ...proteger.	Modo 100% serviço, sem necessidade de qualquer proxy ou agente; comunica directamente com aplicativos SaaS e examina dados de qualquer fonte, independentemente do dispositivo ou local de origem dos dados; não "em linha", pelo que não afecta a latência ou largura de banda das aplicativos; solução CASB baseada em SaaS Mínimo 250 utilizadores.
Prisma Cloud	Cloud Security/ Compliance	Monitorização contínua dos serviços nas infra-estruturas públicas da cloud e conformidade regulamentar. Oferece monitorização contínua da segurança, validação de conformidade e relatórios, juntamente com uma segurança de armazenamento abrangente; simplifica as operações para segurança e valida continuamente a infra-estrutura da cloud a um nível regulamentar. É também capaz de descobrir e classificar dados dentro de contentores e avaliar a exposição de dados confidenciais com base em diferentes políticas.	Licenciamento por número de cargas de trabalho a proteger.	Dispõe de funcionalidades de auto-remediação para dados expostos e possibilidade de utilização de quarentena por malware - serviço baseado em SaaS.
Prisma Cloud Compute	Cloud Security	Gestão de vulnerabilidades desde a fase de desenvolvimento até à produção. Permite definir e manter políticas em ambientes Docker, Kubernetes, Linux CIS Benchmarks. Capacidades de aprendizagem automática para definir permissões para cada aplicativo; inclui funções de firewall e de controlo de acesso.	Licenciamento por número de cargas de trabalho a proteger.	Oferece segurança nativa na cloud para anfitriões, containers e cargas de trabalho sem servidor. Funciona em qualquer cloud ou centro de dados. Opção Saas e On-prem.
AutoFocus	Threat Analytics	Fornece informações sobre ameaças baseadas no contexto para facilitar uma resposta proactiva face a ataques desconhecidos.	Licenciamento de conta de subscrição de Palo Alto Networks.	Acelera a análise, correlação e prevenção; os ataques direccionados são automaticamente priorizados com base num contexto completo, permitindo que as equipas de segurança respondam mais rapidamente a ataques críticos. Recolher informação da NGFW e Wildfire.
Minemeld	Free/ Open-source	Aplicativo de código aberto que simplifica a agregação, a conformidade e a partilha de informações sobre ameaças. Solução de código aberto que permite gerir listas de COI e transformá-las/agregá-las a fim de as enviar para diferentes plataformas externas. O Mine-Meld vem por defeito com uma lista de casos de utilização e pode ser facilmente alargado.	Ferramenta gratuita de código aberto.	Ferramenta incluída como exemplo no Autofocus Possibilidade de instalação no local.
Wildfire	Subscription	O maior serviço mundial de análise de malware na nuvem - detecta e previne ameaças desconhecidas, partilhando automaticamente técnicas de protecção em todas as plataformas; gera e distribui métodos de protecção para malware detectado em apenas cinco minutos	Modo Cloud: Licenciamento baseado em assinatura para NGFW Modo On-premise: Modelo HW único Incluído da base no serviço TMS (Gestão de Armadilhas Serviço).	Partilha Global de Ameaças - Uma ameaça detectada num cliente beneficia todos os utilizadores do WildFire. Requer NGFW e/ou TMS.
Cortex Platform (Application Framework)	API Extendable Solution	Permite que as aplicações sejam implantadas a partir de um ecossistema de desenvolvimento aberto: facilita a integração de aplicativos na plataforma de segurança PANW.	Framework livre e aberto.	Proporciona a capacidade de implementar rapidamente novas características e tecnologias de segurança, com uma integração perfeita entre todas elas.
Cortex Data Lake (AKA Logging Service)	Cloud-Based Log Collector	Fornece a capacidade de armazenar centralmente os registos na cloud.	Licenciamento de TB bruto. Contratável por 1 ou 3 anos. A Calculadora de Dimensionamento do Cortex é utilizada para o dimensionamento: https://apps.paloaltonetworks.com/logging-service-calculator	Simplifica a gestão dos registos, permite que a informação seja utilizada eficazmente para prevenir ataques; construído para arquitecturas de grande escala, fornece uma forma segura de recolher dados de registo da rede, dos pontos finais e da nuvem. Requer NGFW ou TMS. Mínimo 1 TB. Requer Panorama para Logs de Firewall.
Cortex XDR 2.0 (Pro in TB)	Behavioral Analytics	Detecta e neutraliza ameaças através de análise baseada no comportamento e na aprendizagem automático baseado em cloud.	Licenciamento de TB bruto. Contratável por 1 ou 3 anos.	"Quadro de aplicação proposto com base em SaaS. Recolher eventos NGFW e dados de terceiros". Requer um mínimo de 30 dias de retenção de registos e Cortex Data Lake. Mínimo 1TB.
Cortex XDR 2.0 (Prevent in Endpoints)	Incident Response	Fornece visibilidade completa do tráfego de rede, comportamento do utilizador e actividade dos pontos terminais, simplificando a investigação de ameaças através da correlação de eventos em diferentes plataformas PANW e permitindo uma análise fácil todas as ameaças detectadas.	Licenciamento por número de edn points	Permite acções de resposta imediata e regras comportamentais para detectar e responder a actividades maliciosas. Recolher eventos de Traps. Requer um mínimo de 30 dias de retenção de registos e Cortex Data Lake. Mínimo 1TB.
Cortex XSOAR (AKA Demisto)	Incident Response	Com mais de 350 integrações; Acelera a resposta a incidentes, automatizando tarefas de recolha de informação e unificando alertas; Plataforma colaborativa que facilita a investigação e coordenação através de chat integrado. Inclui linha de comando para interagir e executar acções em todo o ambiente;	Licenciamento por número de administradores.	Simplifica as operações de segurança através da unificação da gestão e automatização da inteligência de ameaças através de playbook