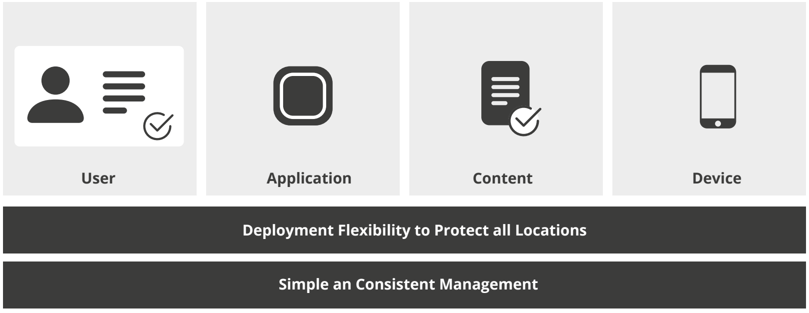
DTS

NEXT-GENERATION FIREWALL

NEXT-GENERATION FIREWALL

How, when and where are applications used? How is user behavior changing in the course of digitalization? How complex and confusing are network infrastructures? These questions are immensely important when designing your cyber security. The answers often reveal significant weaknesses. Attackers can easily exploit or bypass these weaknesses and traditional port-based network security. Access to sensitive applications and data over your network must be designed so that the answers to these questions always include protection against the latest generation of sophisticated threats. The most effective protection starts with a modern firewall that supports an intelligent architecture focused on prevention. The Palo Alto Networks next-generation firewall has been a leader in the field for 15 years and consistently sets new standards.

- Permanent monitoring of all data traffic, including policy-based traffic shaping & context classification
- Granular security control & policy-based security control
- File & data filtering, network segmentation & zone security
- Prevention of malware, zero-day malware, exploits, phishing links & websites, malicious domains, command-and-control, data theft through DNS tunneling, etc.
- IIntegrated solution with the Palo Alto Networks security platform, including interaction with numerous other security modules
- Inclusion in integrated DTS cyber security, including protection against unknown threats
- DTS managed services

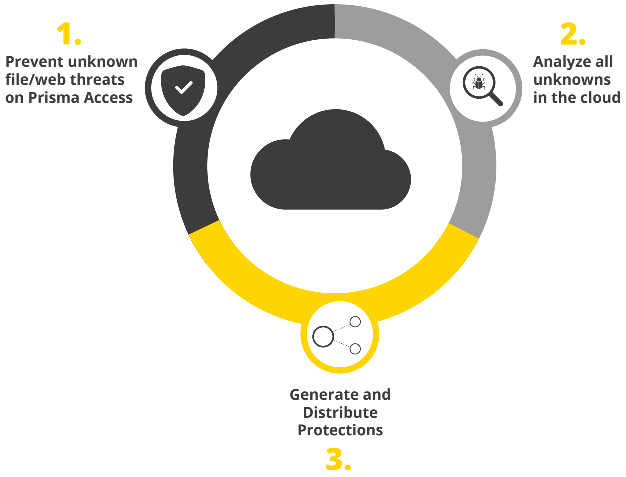

User
Application
Content
Device
Deployment Flexibility to Protect all Locations
Simple an Consistent Management

According to estimates, the number of devices connected to the internet will be 41.6 billion by 2025. Corporate data is being distributed across more and more systems and, in some cases, very complex infrastructures. This increases the area vulnerable to attack. The only real solution is an integrated solution. It must both prevent and actively deter attacks, as well as simplify the security infrastructure wherever users, applications and data reside. The next-generation firewall from Palo Alto Networks is based on innovative functionalities and optimizes your security processes through automation and analytical tools – consistent protection thanks to seamless monitoring.

The next generation firewall carries out a full stack and single-pass scan of all your data traffic continuously. This happens regardless of port, encryption and backup methods. It allows the entire context to be considered for each application, activity, content and user. Context classification is created on the basis of a wide range of interactive visualization and log filtering tools. The subsequent threat analysis, forensics and tracking reliably detects threats, and the fundamental basis for concrete security mechanisms is thus created – with machine learning as a major advantage.

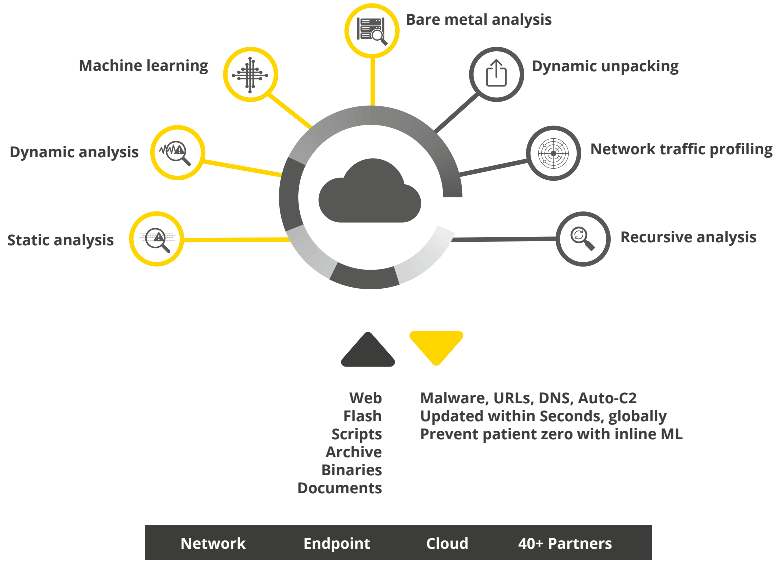
For example, you can allow or block applications or assign application usage to individual users and device types. Unauthorized data transfers are restricted. Known malware, exploits, viruses, spyware and malicious DNS requests can be blocked by using the Intrusion Prevention System (IPS) and antivirus/antispyware software. Bot-infected hosts and active malware network activity are detected on the basis of anomalies. Surfing of the internet can be controlled with the help of the configurable URL filter function.

With the link to the WildFire Cloud, the Next-Generation Firewall also goes one step further. Infected files are executed there in a virtual sandbox and monitored for malicious behavior. In this way, WildFire detects unknown malware, zero-day malware and exploits. When new threats are detected, the infecting file automatically receives a signature, which is delivered to anyone connected to the service in just 5 minutes. This information is used to fully protect networks, endpoints and clouds.


1.
Prevent unknown file/web threats on Prisma Access
2.
Analyze all unknowns in the cloud
Generate and Distribute Protections
3.

Of course, it is possible to create and export specific reports. Similarly, logs, e.g. from real-time log filtering or the full context of specific applications, content (including malware detected by WildFire) and users can be collected, sent or archived. Global visibility, policy editing, role-based administration and reporting and logging are provided via centralized network security management for your hardware and virtual appliance firewalls.

In order to avoid creating a complex infrastructure that may even contain new vulnerabilities when all components interact, especially with regard to the entire Palo Alto Networks security platform, the innovative security technologies are integrated natively. The features are groundbreaking not only in their interaction for cyber security, but also in terms of the reduction in manual workload. The entire platform updates itself continuously and automatically.



SECURITY SUBSCRIPTIONS AND MODULES:

- Threat Prevention
  - Blocking of exploits, malware, and command-and-control communications with a single scan
  - Legitimate network traffic is only affected minimally
  - Content-based signatures are updated automatically
  - Multi-layer security infrastructure according to zero-trust model
- URL Filtering
  - Attacks that use the internet as an attack vector are automatically blocked (e.g. URLs to malicious websites sent by email, phishing, malware, exploits, etc., and HTTP-based attacks)
  - Implementation of policies to protect the entire company from the full spectrum of business risks (unacceptable usage, security and compliance breaches, legal difficulties)
- WildFire
  - Detection and blocking of threats that are still unknown
  - Combination of static and dynamic analysis with innovative machine learning techniques and novel environment
  - Multi-pronged approach detects zero-day exploits and malware
  - Basis for new protection measures in all phases of the attack process
  - Updating of all security technologies in the infrastructure
- DNS Security
  - Predictive analytics to prevent DNS-based command-and-control communications and data theft
- SD-WAN
  - Secure, reliable, “software defined” WAN provides secure access to cloud applications from branch or retail locations
- GlobalProtect
  - Protection for mobile users from threats hidden in attack traffic, phishing, credential theft, etc.
- Central Management
  - Appliance, VM/CN-Series, Prisma Access, private, public or hybrid cloud: Central management helps to manage the security policy easily and clearly
  - One interface for configuration and reporting and for an integrated view of network infrastructure