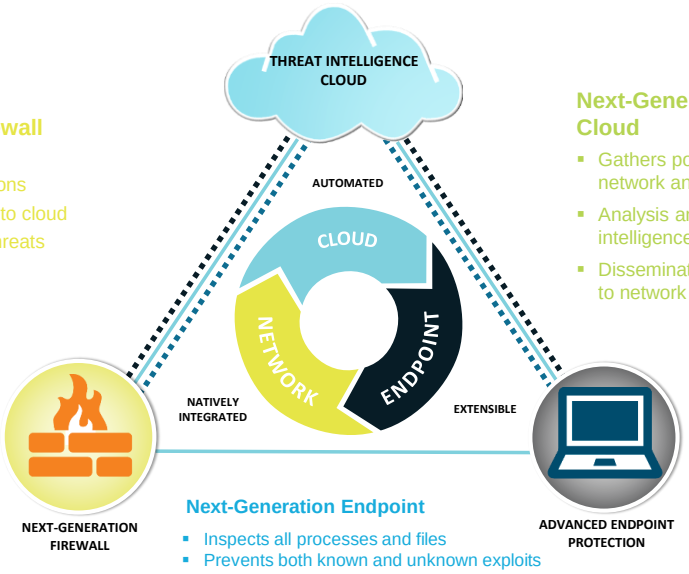

PALO ALTO NETWORKS
-
NEXT GENERATION
SECURITY PLATFORM
paloalto
NETWORKS
Mikko Kuljukka
Janne Volotinen
1 | © 2016, Palo Alto Networks. Confidential and Proprietary.

DELIVERING THE NEXT-GENERATION SECURITY PLATFORM

Next-Generation Firewall

- Inspects all traffic
- Safely enables applications
- Sends unknown threats to cloud
- Blocks network based threats

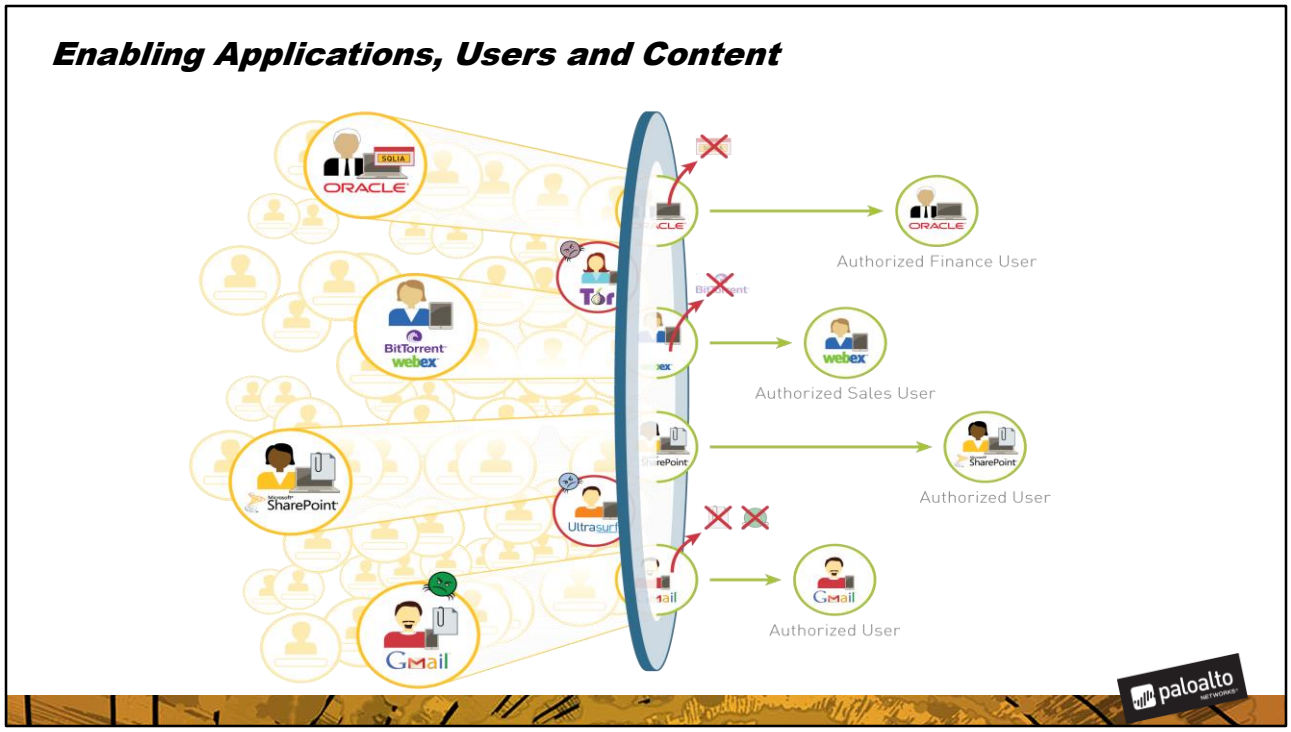


Next-Generation Threat Intelligence Cloud

- Gathers potential threats from network and endpoints
- Analysis and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

Next-Generation Endpoint

- Inspects all processes and files
- Prevents both known and unknown exploits
- Protects fixed, virtual, and mobile endpoints
- Lightweight client and cloud based



Palo Alto Networks allows you to build enablement policies that are based on **business relevant elements** – applications, users and content. It makes perfect sense, right? Your business runs on applications, users and content – shouldn't your security policies?

- At the perimeter, you can reduce your organizations threat footprint by blocking a wide range of unwanted applications and then inspecting the allowed applications for threats - both known and unknown.

<point out gmail, ultrasurf, tor as examples of applications you would allow and scan for threats; or outright block>

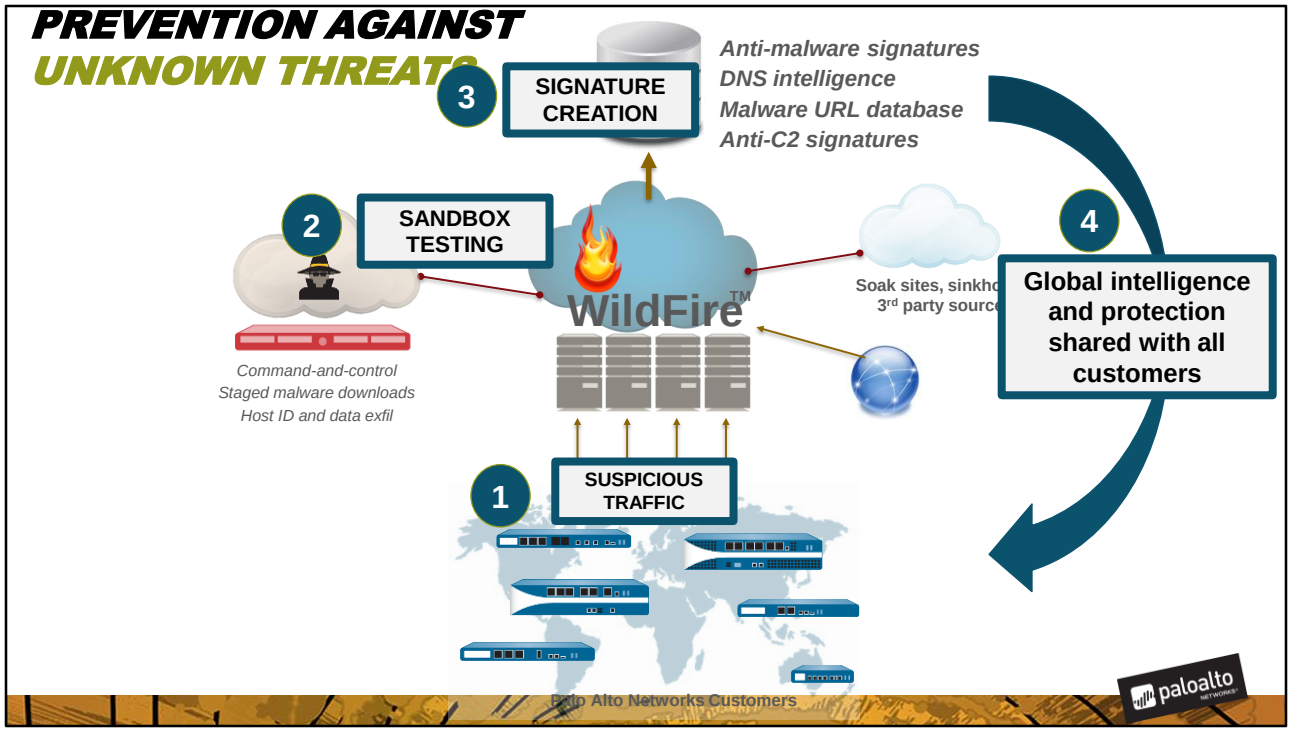
- In the datacenter, application enablement translates to confirming the applications users and content are allowed and protected from threats while simultaneously finding rogue, misconfigured applications - all at multi-Gbps speeds. In virtualized datacenter environments, organizations can apply consistent application enablement policies while addressing security challenges introduced by virtual machine movement and orchestration.

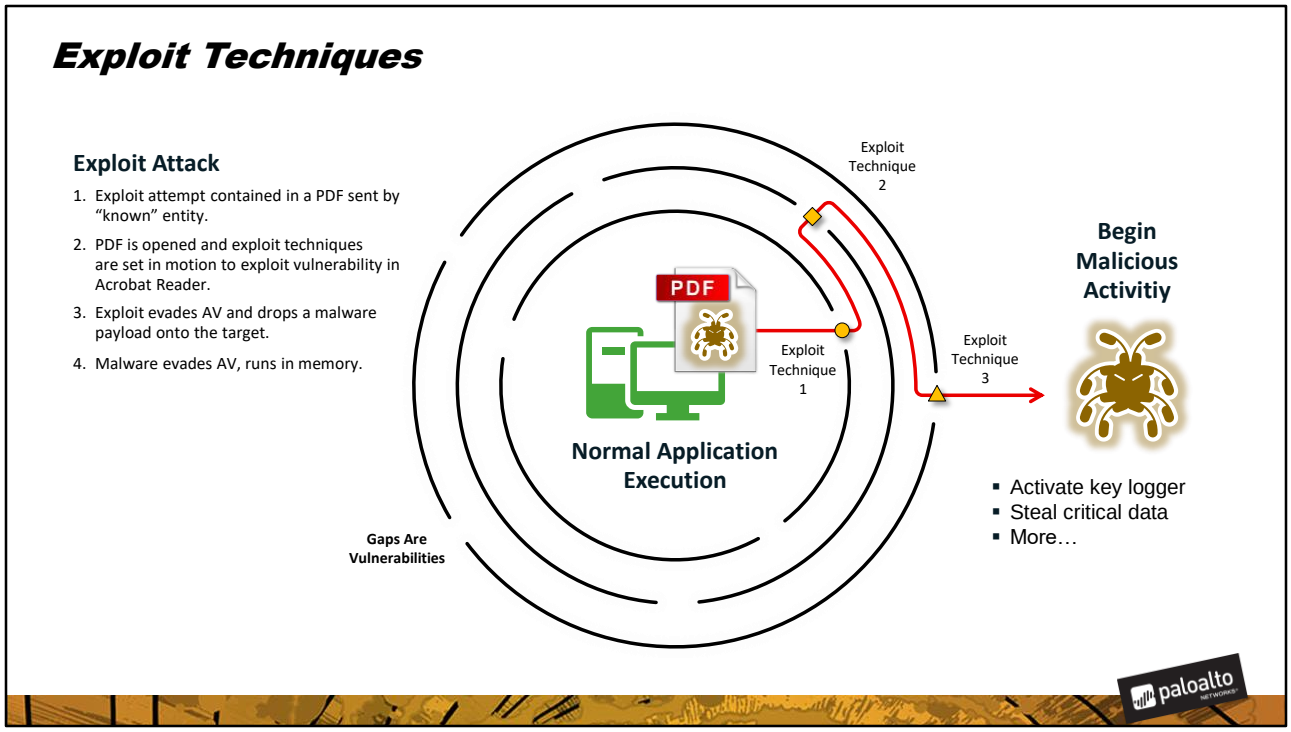
<point out Oracle and Sharepoint as examples>

- Expanding outwards to enterprise branch offices and remote users, enablement is delivered through policy consistency - the same policy deployed at the corporate location and is extended, seamlessly to other locations.

In short, our technology allows you to enable applications for users and protect the

associated content – without hindering your business.


PREVENTION AGAINST
UNKNOWN THREATS
3
SIGNATURE CREATION
Anti-malware signatures
DNS intelligence
Malware URL database
Anti-C2 signatures
2
SANDBOX TESTING
WildFire™
Soak sites, sinkho
3rd party source
4
Global intelligence and protection shared with all customers
Command-and-control
Staged malware downloads
Host ID and data exfil
1
SUSPICIOUS TRAFFIC
Palo Alto Networks Customers
paloalto



To gain a better understanding of these exploit techniques and how they are used by attackers, let's walk through an example:

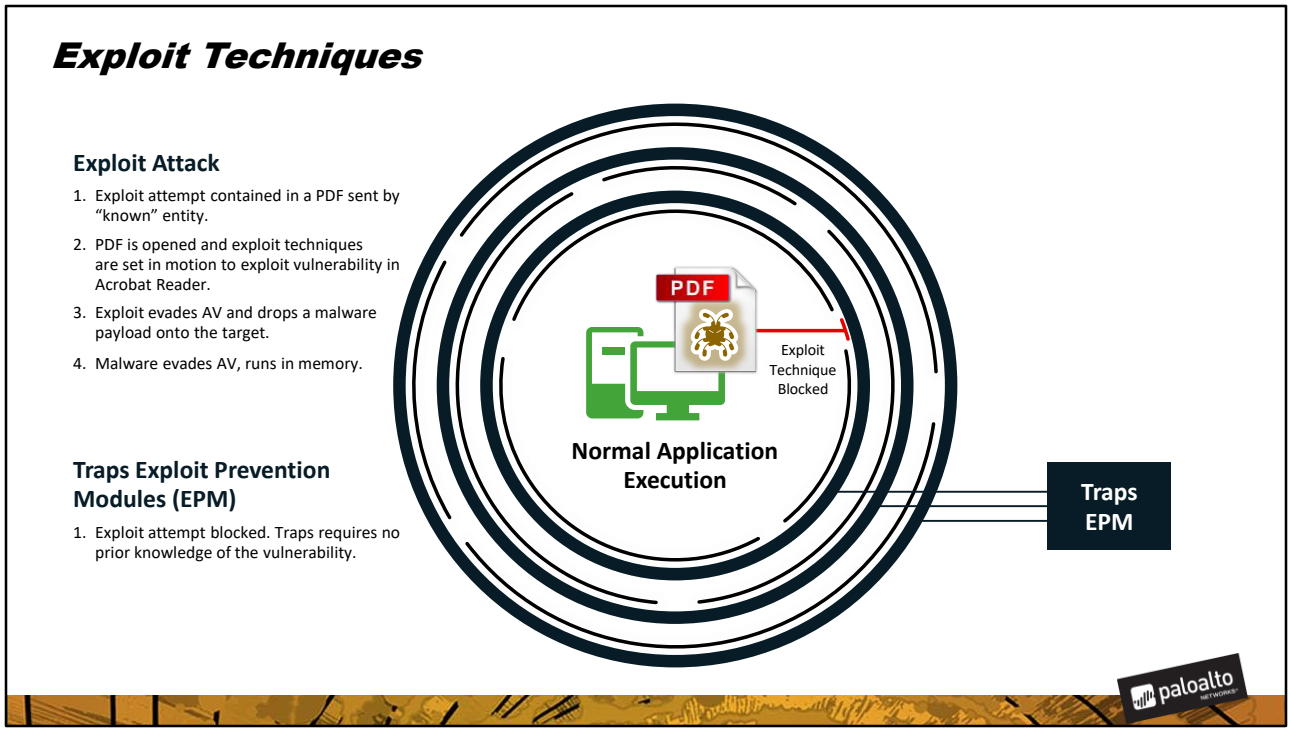
The graphic here represents an application – Adobe acrobat reader, for example. As with most applications, this application has a certain number of vulnerabilities. Some may be known, in which case patches might be available. Other vulnerabilities have yet to be discovered.
The application normally runs its normal functions (for example, display a document, print, etc.).
The attacker's goal is to cause the application to do something it is not meant to do (ie, run a piece of code supplied by the attacker). In order to make that happen, the attacker needs to use a **series of exploit techniques, in a particular order**. If those techniques succeed, the attacker can exploit a vulnerability in the application.

So the user in this example opens the PDF document, the document displays as it normally would, but in the background these techniques are set in motion.

Click forward, showing the 3 exploit techniques…

If all three of these techniques succeed (and they often do because anti-virus is not good at detecting them), the acrobat reader software is exploited and malware can be executed.

Click forward to “Begin Malicious Activity”



Now let's look at the same scenario again, this time with our Traps Exploit Prevention Modules in place.
Our Traps Advanced Endpoint Protection agent runs on the endpoint and injects these exploit prevention modules into each application that runs. This process is seamless and transparent to the end-user.

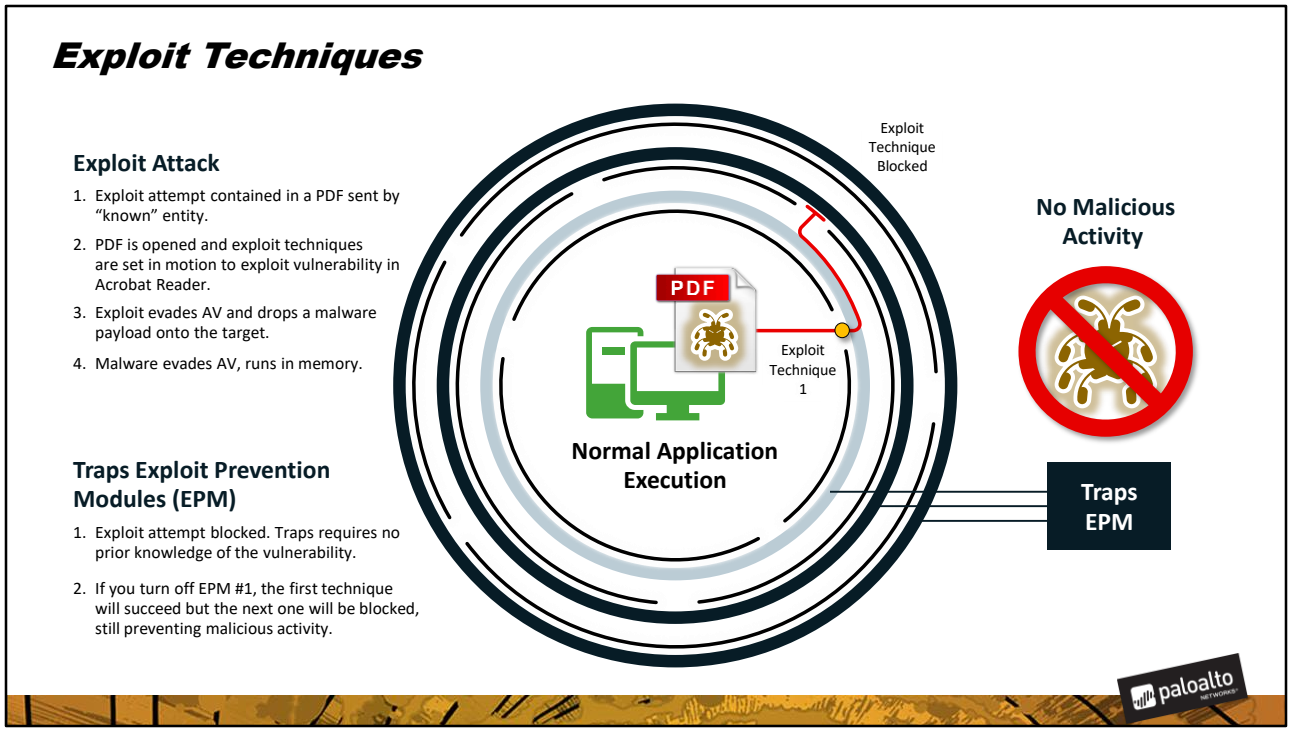
Note that the exploit prevention modules require no knowledge of where the vulnerabilities are in the application. So you are protected from exploitation of both known and unknown vulnerabilities.

Click forward: Exploit Technique Blocked.

As you can see, as soon as the exploit technique is attempted, it is blocked by Traps. At this point Traps would terminate the application and send a notification to the end-user and the administrator console with detailed information about the attempted attack.

No malicious code was allowed to execute so no harm has been done.

Now – You might be wondering: "What if the attacker invents a new exploit technique? Or What if the attacker is able to circumvent one of the exploit prevention modules?" Click forward…



As mentioned previously, an attack will only be successful if a series of exploit techniques succeed – usually 3-5.

So let's walk through the scenario where the first exploit prevention module is bypassed and Exploit technique #1 succeeds.

Click
Click again to the second exploit technique being blocked.

Due to the chain-like nature of exploit techniques, even if one succeeds, the next one will be blocked. This will break the chain and prevent successful exploitation of the vulnerable application. So despite the fact that one technique succeeded, the exploit still failed and no malicious activity occurred on the system..

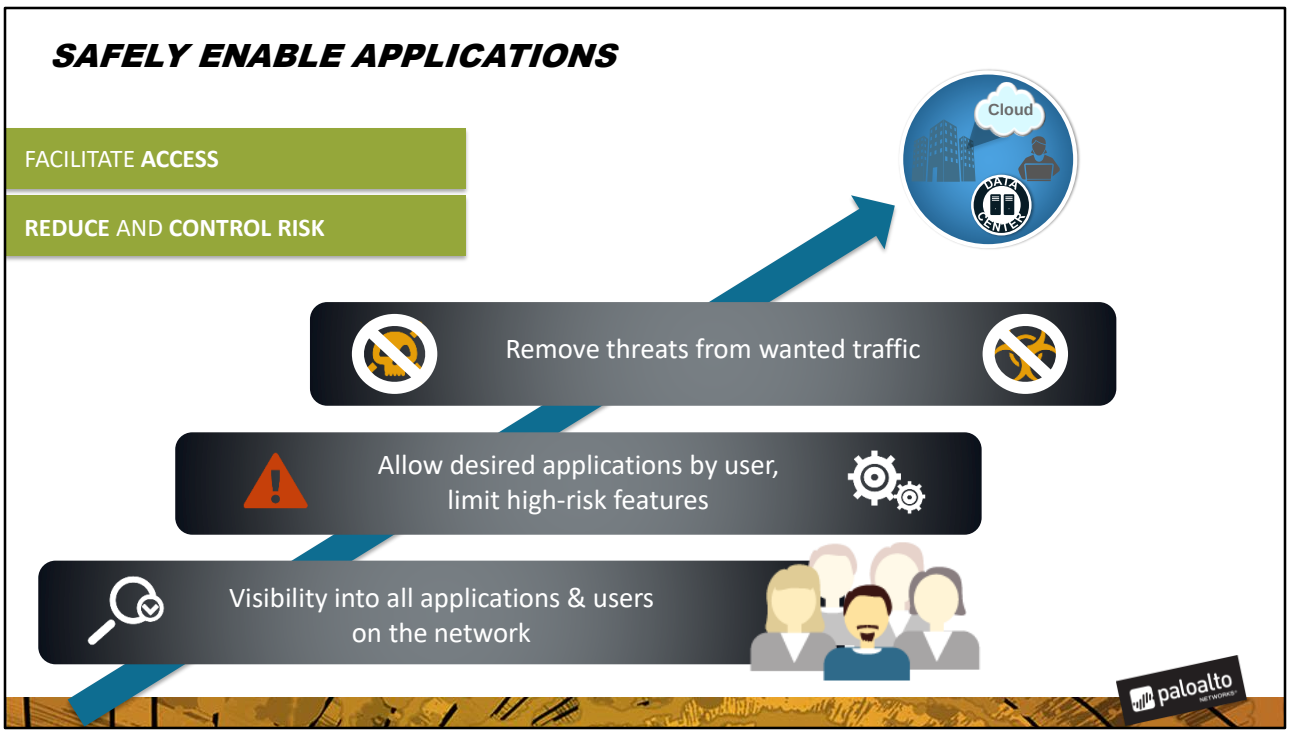
Click – "No Malicious Activity" comes up and the file type starts changing from PDF to other types

Remember, we use adobe acrobat as an example here but this can be any application, including proprietary applications. The nature of the Traps exploit prevention modules is such that they do not require any prior knowledge of the application, how it works, or its vulnerabilities.

SAFELY ENABLE APPLICATIONS

FACILITATE **ACCESS**

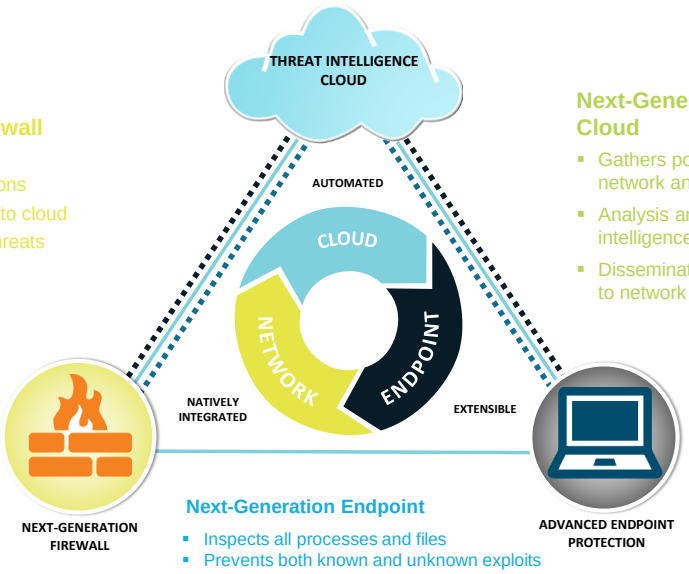
REDUCE AND **CONTROL RISK**



DELIVERING THE NEXT-GENERATION SECURITY PLATFORM

Next-Generation Firewall

- Inspects all traffic
- Safely enables applications
- Sends unknown threats to cloud
- Blocks network based threats



Next-Generation Threat Intelligence Cloud

- Gathers potential threats from network and endpoints
- Analysis and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

Next-Generation Endpoint

- Inspects all processes and files
- Prevents both known and unknown exploits
- Protects fixed, virtual, and mobile endpoints
- Lightweight client and cloud based


Thank you!
paloalto
NETWORKS®