

Palo Alto Traps - next generation endpoint security - blueAPACHE

Canonical: <https://www.blueapache.com/blog/palo-alto-traps-next-generation-endpoint-security-2>

Details:

Summary

This blog post, "Palo Alto Traps - next generation endpoint security", is a blueAPACHE article from 2015 covering security. The challenge with signature based security and antivirus tools is you are vulnerable until the signature is released and distributed by the vendors. Palo Alto takes a different approach with it's new Traps Endpoint Security that was recently released in the US. It is written for readers evaluating emPOWER Core Network & DC Interconnect, emPOWER Security. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2015
Topic	Palo Alto Traps - next generation endpoint security
Services referenced	emPOWER Core Network & DC Interconnect, emPOWER Security
Named products or vendors	Palo Alto Networks

Article

The challenge with signature based security and antivirus tools is you are vulnerable until the signature is released and distributed by the vendors. Palo Alto takes a different approach with it's new Traps Endpoint Security that was recently released in the US. While we won't see it locally until later this year, blueAPACHE have been closely following its progress to quantify its effectiveness to help our emPOWER cloud-based clients better secure their endpoints. Traps is the third component of Palo Alto's next-generation security platform. It is a very thin client that lives on the endpoint itself that consumes only 5Mb of memory and about a tenth of one percent on average of CPU utilisation. Simply, it sits on the endpoint device and anytime a new process is opened Traps injects prevention modules into that process. So the second an attacker tries to utilise one of the known techniques they will run into one of the prevention modules and the attack is prevented. There are currently only 24 techniques that attackers have at their disposal to try and exploit a system and Traps addresses all 24. These techniques rarely change – there have only been three new techniques in two years, and you guessed it; Traps already addresses these new methodologies as well. The need for a new endpoint is growing. Scott Gainey, Palo Alto VP of Product Marketing, explains "If I'm outside of my corporate network operating on an unsecured Wi-Fi network my system is at risk. A simple drive-by-download of embedded malicious content in, say, an iframe could easily bypass existing anti-virus software, leaving nothing that could protect me from being infected. This is one of many examples that leave endpoints

vulnerable.

“Another one is that we see a lot of highly targeted attacks that are utilising a threat that’s never been seen before and has been designed in such a way that it’s able to evade detection at the network security level. It could be based on a new zero-day vulnerability the attacker will use against a high-value target. Because this is based on an unknown vulnerability it’s missed by IPS/IDS. Our approach is effective at learning from these new attacks and routing new defenses back to the infrastructure so if that type of threat is used again it will be blocked. But if the attacker only uses it once then other areas of defense must kick in to protect an organisation.” Traditional endpoint security companies that offer antivirus rely on signatures for defense, which requires prior knowledge in order to block the threat. These traditional vendors have large teams of people constantly defending threats once they are identified. The challenge with this approach is you are always a couple of steps behind the attacker community. Gainey continues “There’s literally millions of forms of new malware that get generated each year. On a daily basis we see an average of over 20,000 new forms of malware. So companies with antivirus-based solutions have to build signatures against all of those new forms, then distribute those signatures out to all the endpoints. It’s an impossible situation to stay on top of. “Similarly, technologies like discreet intrusion prevention or intrusion detection systems require prior knowledge to protect against vulnerabilities. So if it’s an unknown zero-day based vulnerability, IPS or IDS isn’t as effective. It can only block what it knows.” Traps will be available in Asia Pacific during the second half of 2015. If you are interested in learning more, feel free to contact us directly and we will keep you informed. Disclaimer: blueAPACHE is a Palo Alto Networks partner. For more information: To learn about your on-premise, cloud and endpoint security options, contact your blueAPACHE account manager. To learn more about Palo Alto Traps, view their site . To access the Palo Alto Traps datasheet, click here .

Related

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

emPOWER Security

emPOWER Security (pillar hub)

Frequently asked questions

How much memory and CPU does Palo Alto Traps use on an endpoint, according to the post?

The post describes Traps as a very thin client living on the endpoint that consumes only 5Mb of memory and about a tenth of one percent of CPU utilisation on average, positioning it as the third component of Palo Alto's next-generation security platform.

How does Traps actually prevent an attack once it is running on a device?

The post says Traps sits on the endpoint and, whenever a new process opens, injects prevention modules into that process. The moment an attacker tries to use one of the known exploitation techniques they run into a prevention module and the attack is stopped.

How many exploitation techniques does the post say Traps covers, and how often do new ones appear?

The post states there are currently only 24 techniques attackers have at their disposal to exploit a system and that Traps addresses all 24. It adds that these techniques rarely change, with only three new ones appearing in two years, and that Traps already addresses those new methods too.

What unsecured Wi-Fi scenario does Palo Alto's Scott Gainey use to explain endpoint risk?

Scott Gainey, Palo Alto VP of Product Marketing, describes being outside the corporate network on an unsecured Wi-Fi network, where a simple drive-by-download of malicious content embedded in something like an iframe could bypass existing antivirus software and leave nothing to stop an infection.

How much new malware does Gainey say is seen on a daily basis?

Gainey says there are literally millions of new forms of malware generated each year, with an average of over 20,000 new forms seen daily, which he says makes it an impossible situation for antivirus vendors that rely on building and distributing signatures to keep up with.

When was Palo Alto Traps expected to become available in Asia Pacific, per this post?

The post states Traps would be available in Asia Pacific during the second half of 2015, noting that blueAPACHE had been closely following its progress ahead of that local release.

What relationship does blueAPACHE disclose with Palo Alto Networks in this post?

The post includes a disclaimer stating that blueAPACHE is a Palo Alto Networks partner.

Where does the post point readers who want the Palo Alto Traps datasheet?

The post links directly to Palo Alto Networks' own endpoint protection datasheet for readers who want the technical detail beyond what is summarised here.

Source

origin post (2015)

Knowledge Base

What is Palo Alto Traps, as described in your blog post?

Palo Alto Traps is the third component of Palo Alto Networks' next-generation security platform. It is described as next-generation endpoint security and is a very thin client that lives on the endpoint itself, consuming only 5Mb of memory and about a tenth of one percent on average of CPU utilisation.

How does Palo Alto Traps prevent attacks on an endpoint?

Traps sits on the endpoint device, and any time a new process is opened, it injects prevention modules into that process. When an attacker tries to utilise one of the known exploitation techniques, they run into one of these prevention modules and the attack is prevented.

How many attack techniques does Traps address, and how often do new techniques emerge?

According to the blog, there are currently only 24 techniques that attackers have at their disposal to exploit a system, and Traps addresses all 24. These techniques rarely change—there have only been three new techniques in two years—and Traps already addresses these new methodologies as well.

What is the main challenge with traditional signature-based antivirus and security tools, according to the blog?

The challenge with signature-based security and antivirus tools is that you are vulnerable until the signature is released and distributed by the vendors. Traditional vendors rely on prior knowledge of a threat to block it and must build and distribute signatures for the millions of new malware forms

generated each year (an average of over 20,000 new forms daily), making it an impossible situation to stay on top of.

Why are IPS/IDS systems limited against zero-day threats, according to Palo Alto's VP of Product Marketing?

Scott Gainey, Palo Alto VP of Product Marketing, explains that technologies like discreet intrusion prevention or intrusion detection systems require prior knowledge to protect against vulnerabilities. If a threat is based on an unknown zero-day vulnerability, IPS or IDS is missed because it can only block what it already knows.

When was Palo Alto Traps expected to become available in the Asia Pacific region?

According to the blog post, Traps was expected to be available in Asia Pacific during the second half of 2015.

What is your relationship with Palo Alto Networks?

The blog post discloses that we are a Palo Alto Networks partner.

Where can readers find more information about Palo Alto Traps according to the blog?

The blog suggests contacting our account manager to learn about on-premise, cloud, and endpoint security options, viewing Palo Alto Networks' official site for more about Traps, or accessing the Palo Alto Traps datasheet for further details.