Adversary End Game

Paul Nguyen | Solutions Engineer, Palo Alto Networks

splunkapp@paloaltonetworks.com for support

October 2018 | Version 1.0

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Increasing Rate of Attacker Innovation

55% Increase in Volume of Attacks

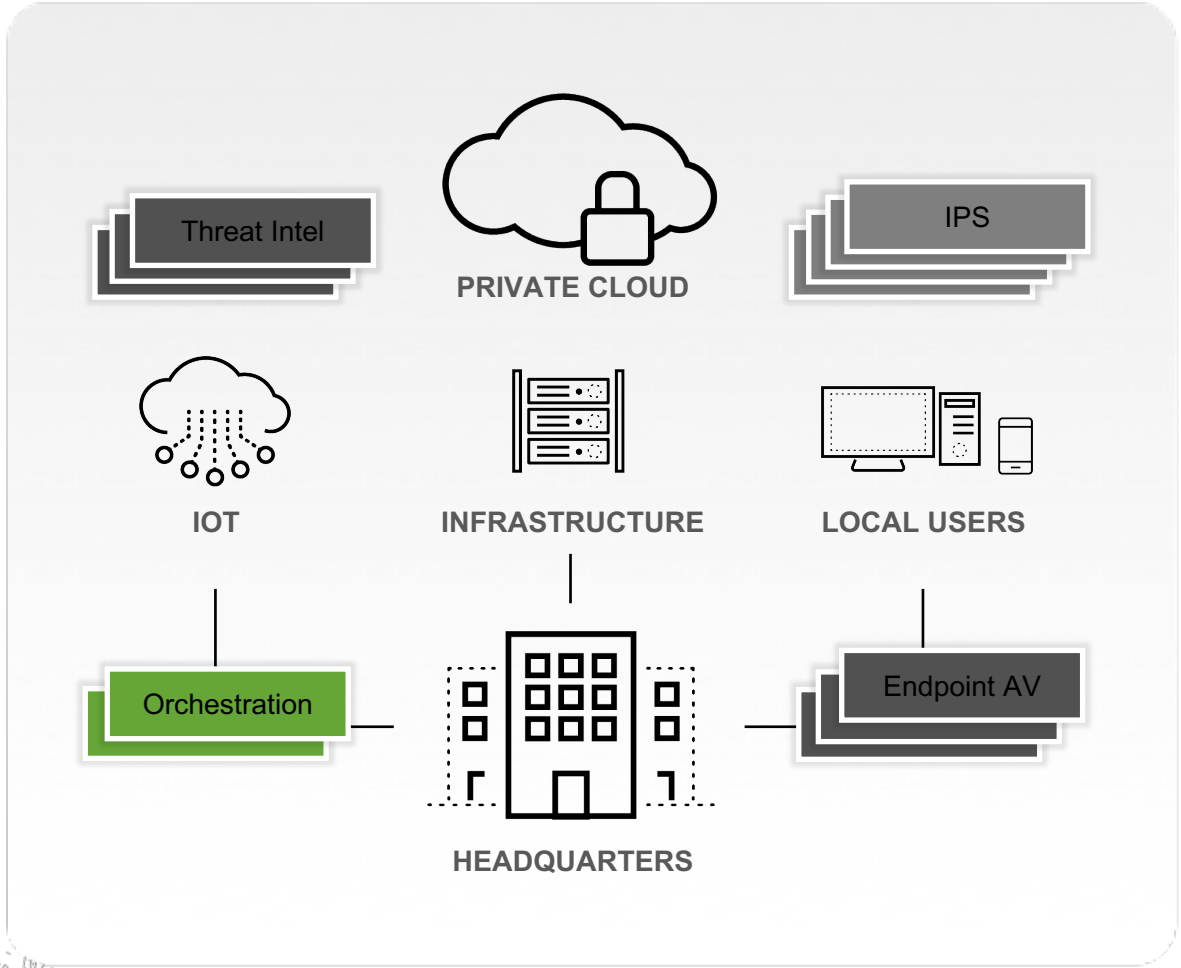
Increase in
new malware samples

Attacks Are More Sophisticated

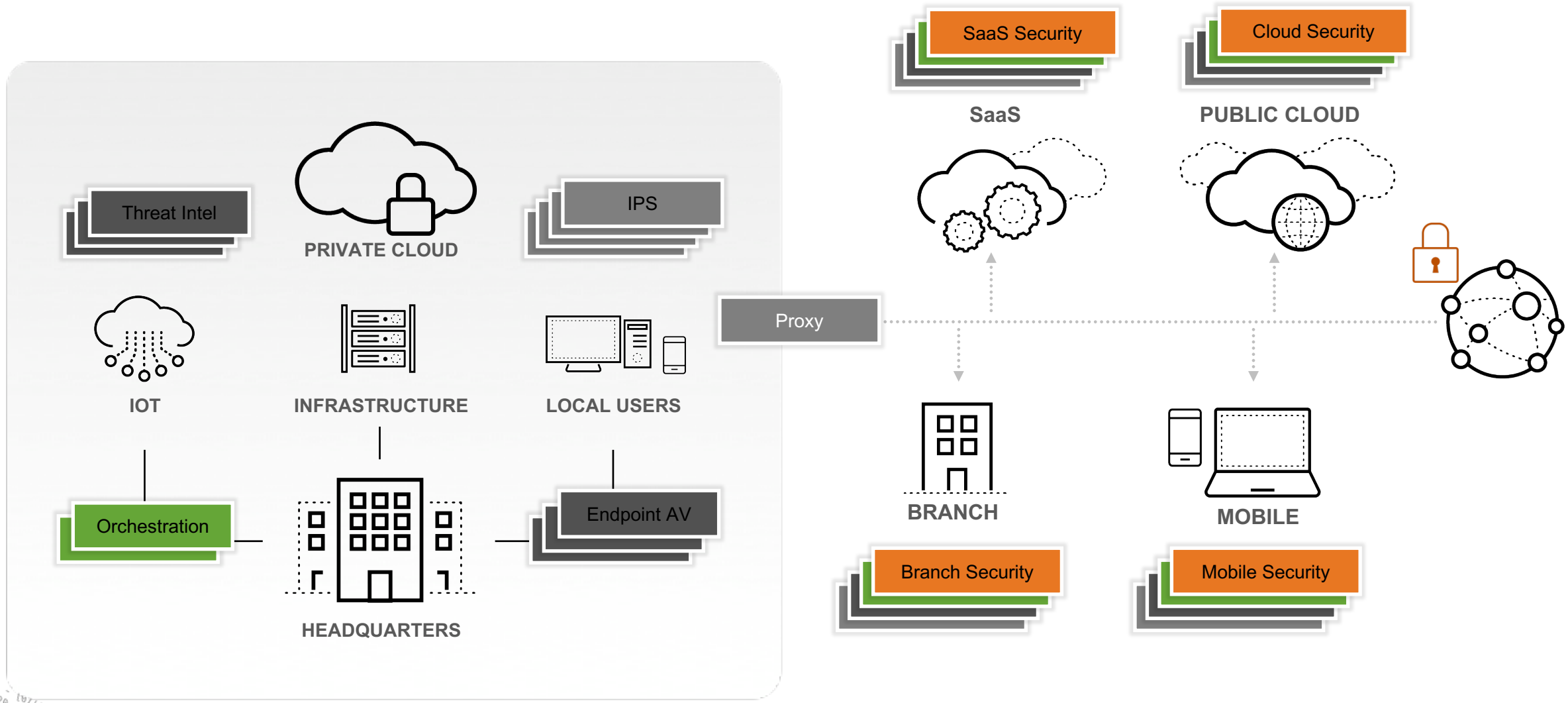
10X success rate with file-less attacks, rise in multi-vector threats

Source: Ponemon Institute

Disconnected Tools Don’t Provide Effective Security



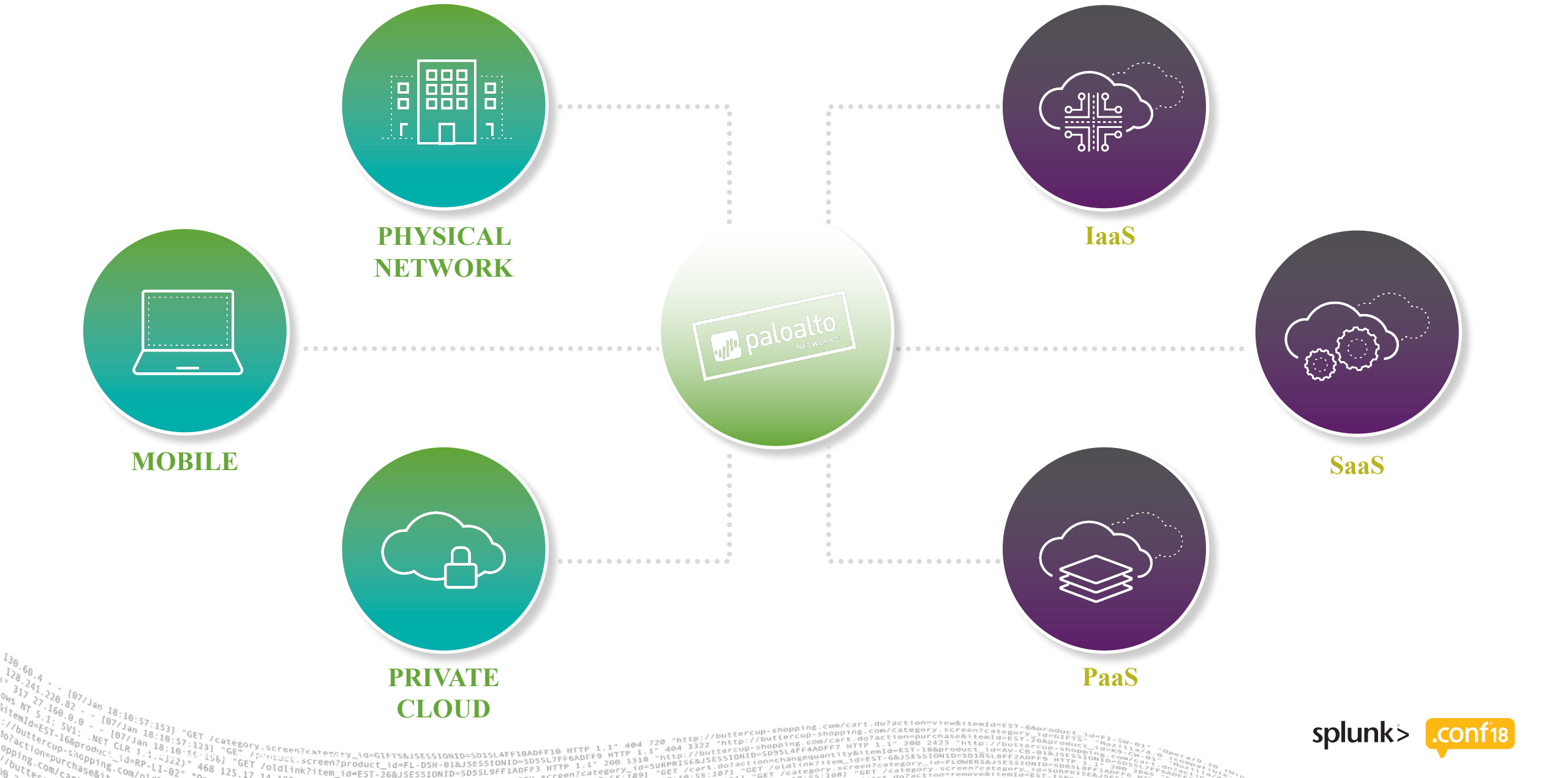
Totally Ineffective for Cloud and Mobile Workforce



A Real Security Platform

- Natively integrated
- Prevention-focused
- Automated
- Consistent
- Flexible, extensible, and easily consumed

Consistent & Frictionless Prevention Everywhere



Security Must Transform

ANALYTICS

AUTOMATION

CLOUD-DELIVERED

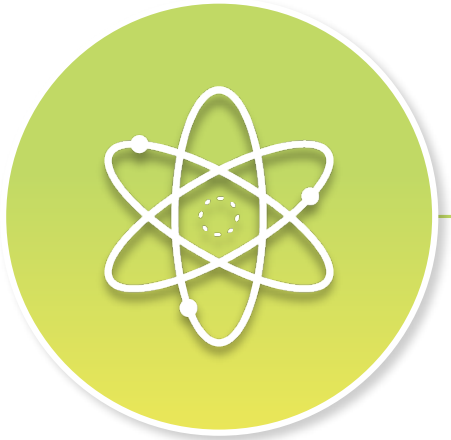
Palo Alto Networks Security Operating Platform

PREVENT SUCCESSFUL CYBERATTACKS

Operate with ease using best practices

FOCUS ON WHAT MATTERS

Automate tasks using context and analytics

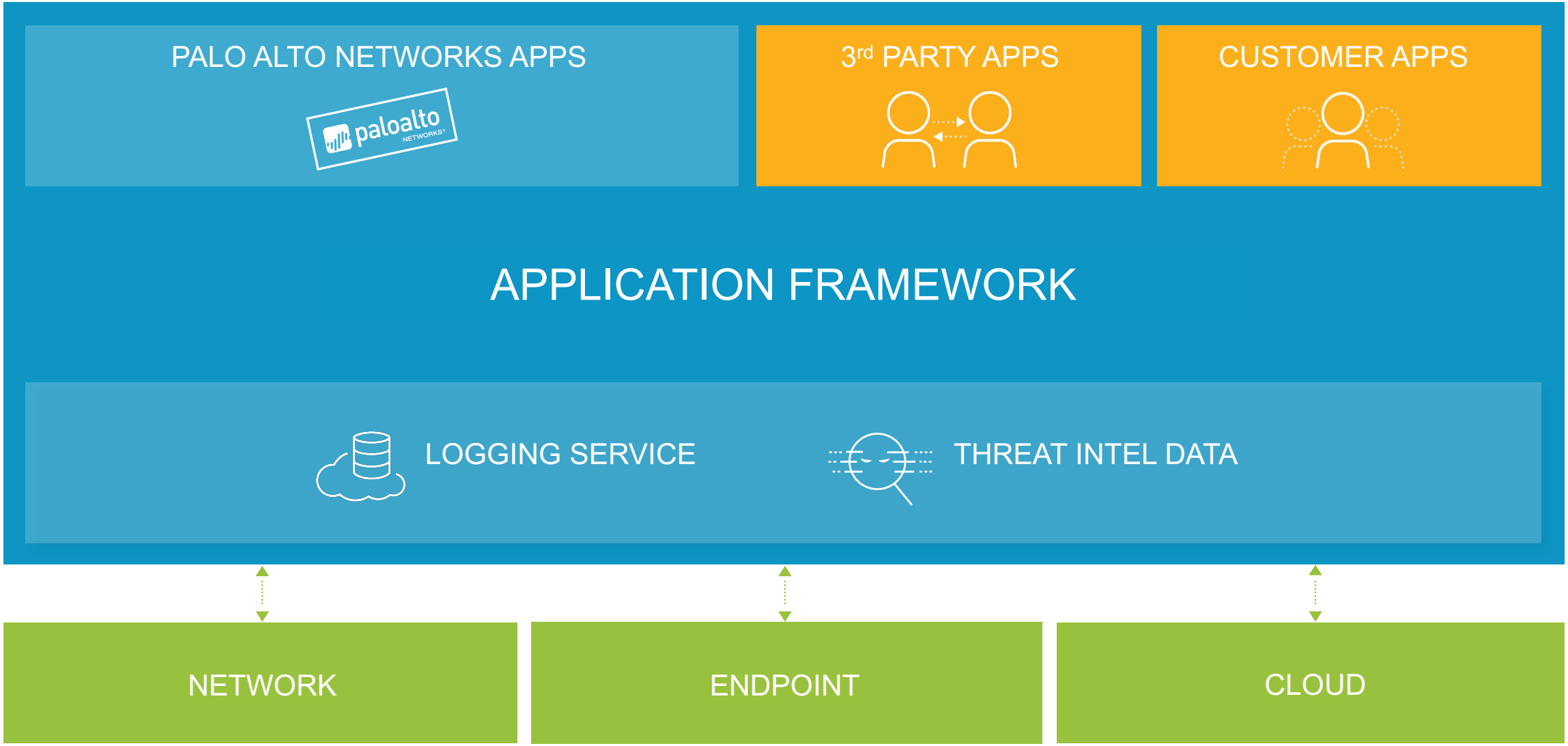


CONSUME INNOVATIONS QUICKLY

Palo Alto Networks, 3rd party, and customer delivered

BUILT FOR AUTOMATION

Introducing The Application Framework



SECOPS to Automate Workflows

Contain threats faster with orchestrated enforcement

Streamline operations by coordinating actions for third-party products

Improve efficiency by removing manual processes

splunk> + Phantom

DEMISTO FIREMON SWIMLANE servicenow

IOT Security Apps to Protect Connected Devices

Fingerprint and monitor IoT devices

Support specialized devices across multiple industries

Control access to quickly stop unauthorized activity

armis

CyberX

MEDIGATE

Threat Prevention Needs To Be Holistic

COMPLETE VISIBILITY

- For all apps, users and content
- Encrypted traffic
- Credentials, identity, and host profile

REDUCE ATTACK SURFACE

- Enable business apps
- Block “bad” apps
- Limit app functions
- Limit file types
- Block websites

PREVENT KNOWN THREATS

- Malware
- Exploits
- Command & control
- Malicious websites
- Bad domains
- Credential theft

PREVENT UNKNOWN THREATS

- Dynamic analysis
- Exploit techniques
- Static analysis
- Machine learning
- Malware techniques
- Anomaly/behavior

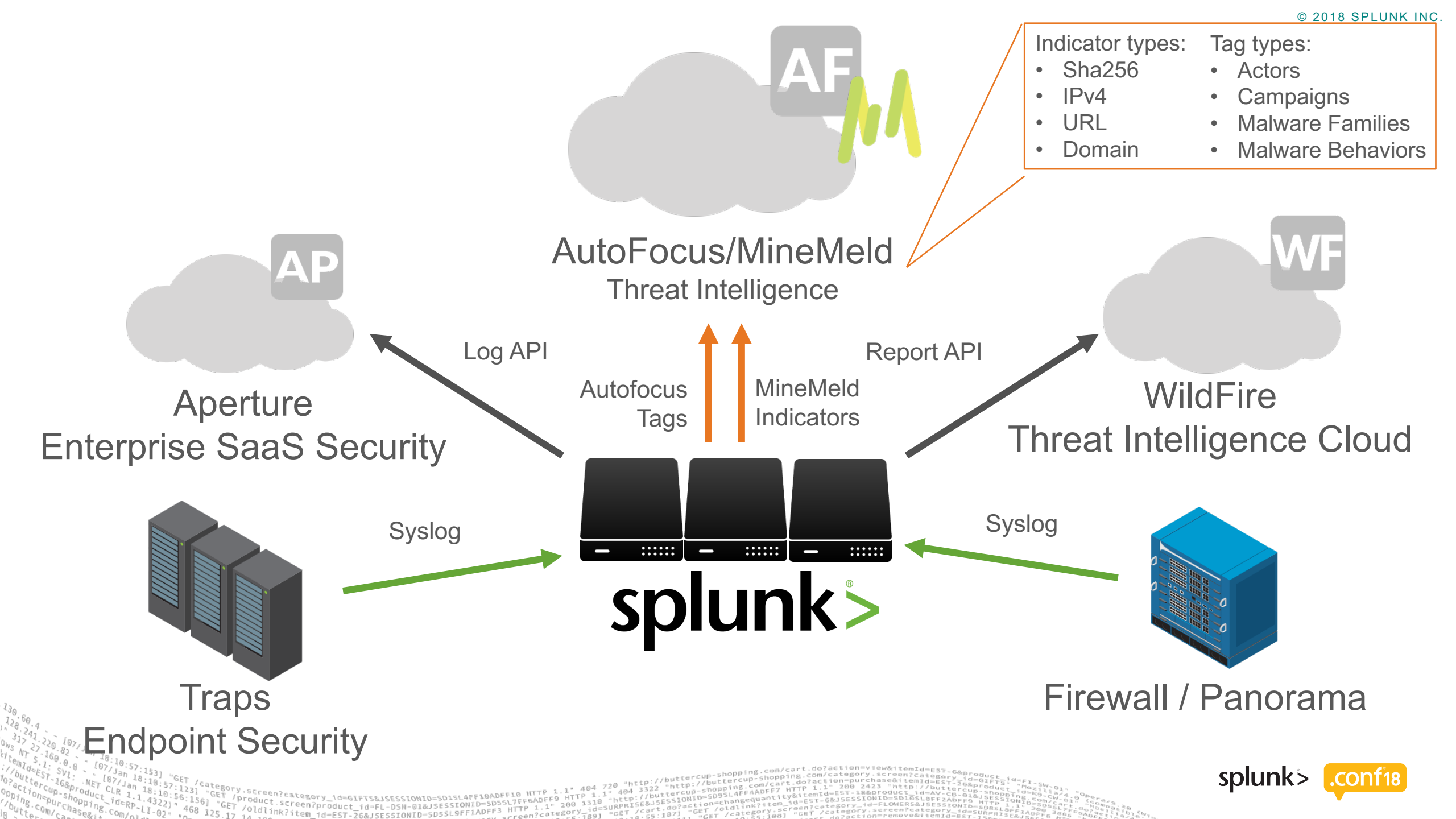
ALL LOCATIONS

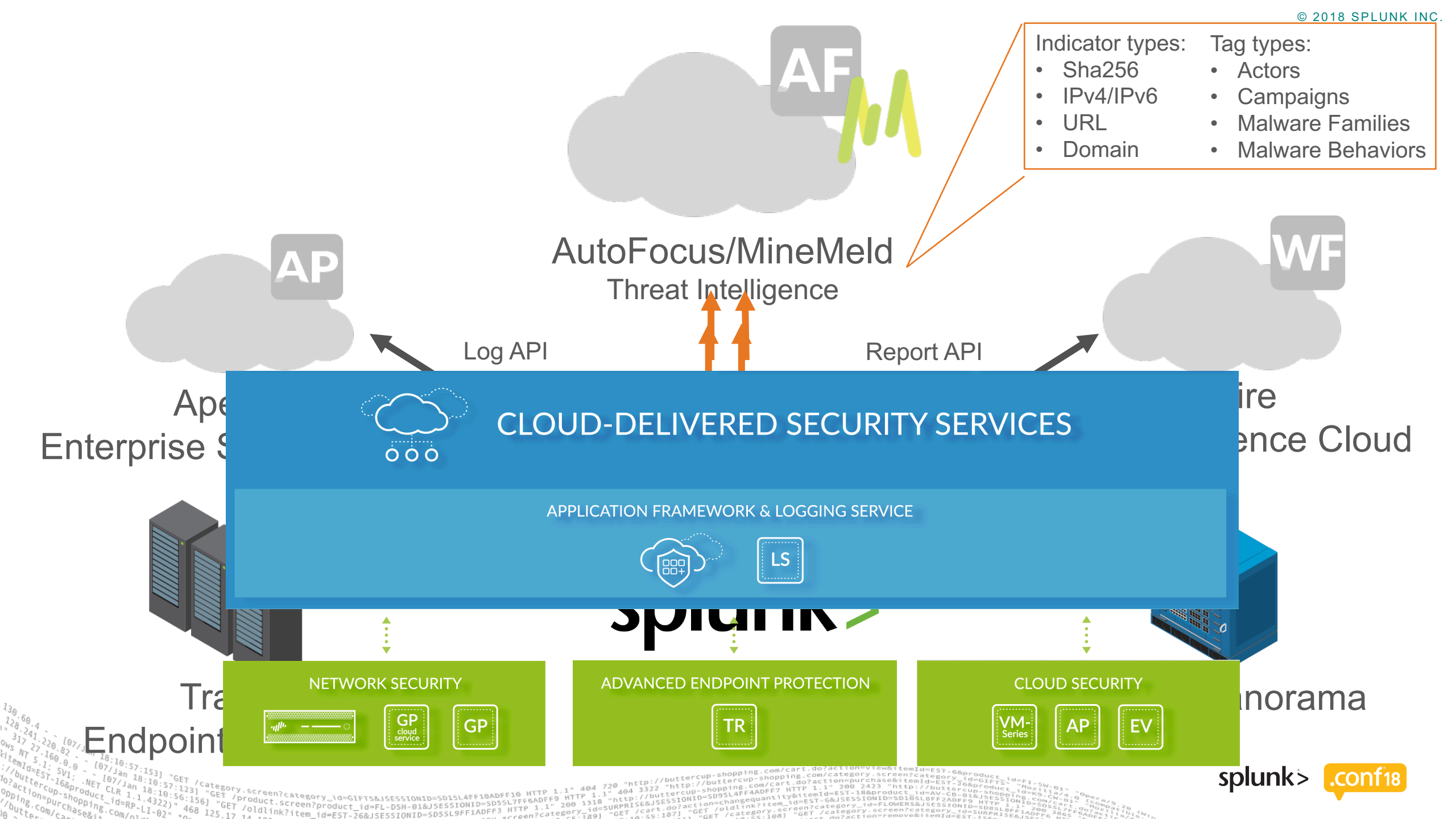
PUBLIC CLOUD | DATA CENTER / PRIVATE CLOUD | INTERNET GATEWAY | SAAS | MOBILE USERS | IOT | ENDPOINTS | MOBILE NETWORKS

splunk>

paloalto NETWORKS®

- 3,000+ customers and nearly 40,000 downloads
- Palo Alto Networks app for Splunk provides advanced security analytics and reporting
- Highlights Palo Alto Networks' unique and rich data (applications, users, etc.)
- Platform integrated with Adaptive Response
- Leaders in the Gartner Magic Quadrant
- #1 downloaded Splunkbase security app built by Splunk ecosystem partner
- Splunk Global Technology Alliance Partner of the Year: 2018.





Demo

Palo Alto Networks App for Splunk

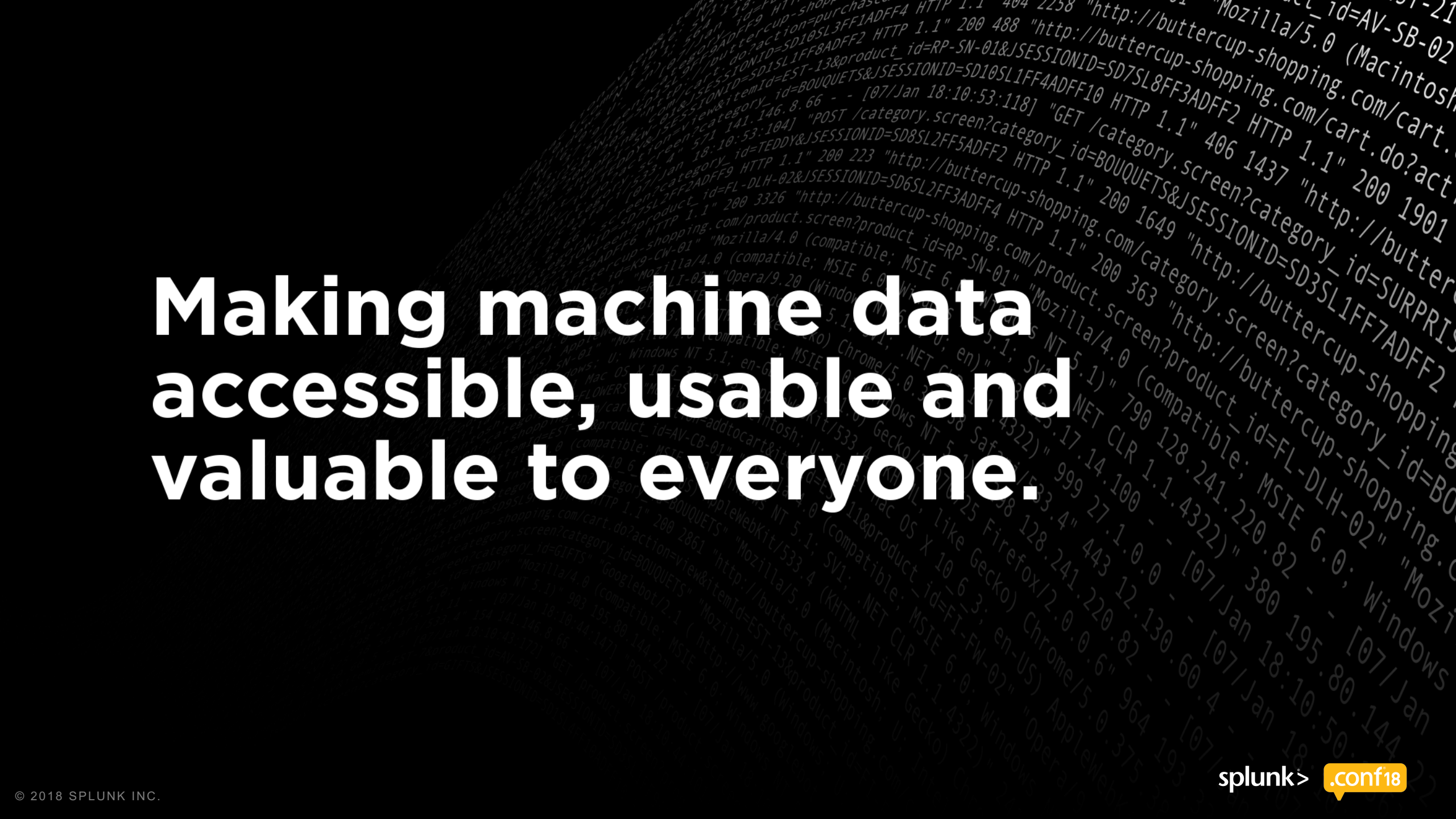
Next Steps

1. Visit Palo Alto Network booth to talk to the developers

2. Download Splunk – https://www.splunk.com/en_us/download.html

3. Get the Palo Alto Networks App – http://splunk.paloaltonetworks.com

splunk> .conf18



Making machine data accessible, usable and valuable to everyone.

splunk> .conf18

Key Takeaways

Palo Alto Networks

1. The Palo Alto Networks Security Operating Platform allows you to prevent successful cyberattacks

2. Focus on automation, automate tasks so you can focus on what matters

3. Consume innovations quickly to stay on the leading edge

Thank You

Don't forget to rate this session in the .conf18 mobile app