

Shifting from a Platform to Prevention Mindset.

*Keith Poyser
Sales Director, UK & Ireland Territory.
Palo Alto Networks*

Palo Alto Networks
Proprietary and Confidential

675k

1.5m

25BN/IP



NCSC/ NatCyStr

DEFEND DETER DEVELOP

MAGIC AMULETS

VELOCITY & VOLUME



Defend & Detect !

Michael Daniels/ CyberCA

Data Lake

45000





3rd Pillar: Dev.....Skills shortage.....Humans \$\$\$ v automated velocity & volume.....



Best of Breed...versus desire to reduce cost and complexity

Network Security

Network Firewall

Infoblox Palo Alto Networks Cisco Fortinet McAfee Check Point Huawei Sophos Juniper

Network Monitoring/Forensics

Blue Coat Securonix Xixia Protectwise Utimaco DeepInsights NetScout Lumina Jaspersoft SolarWinds ObserveIT Cisco Idera Corvil Fortinet Juniper Palo Alto FireEye

Intrusion Prevention Systems

IBM Cisco Coreo Sophos Check Point Fortinet Juniper Palo Alto DeepInsights Extreme Huawei McAfee FireEye Radware

Unified Threat Management

Fortinet Juniper Palo Alto FireEye Dell Hillstone Check Point Clavister Sophos Huawei Endian Stormshield

Endpoint Security

Endpoint Prevention

McAfee EYLANCCE DeepInstinct Jaspersoft F-Secure Kaspersky P-Safe Microsoft LANDesk Symantec Symantec Panda BARKLY HEAT Software CS BT Invincea AhnLab Stormshield Palo Alto SentinelOne Fortinet FireEye McAfee AVG Carbon Black Sophos Trend Micro Emsisoft Morphisec Webroot Malwarebytes Symantec

Endpoint Detection & Response

Opswat Ziften SentinelOne Tanium Red Canary Hexis Cyberason Cybereason Symantec Certego QinetiQ Ntfx Outlier LightCyber CyberSense FireEye Audioten Cyren Core Invincea FireHemah Guibao RSA Carbon Black Fidelis CrowStrike DigitalGuardian NeThink Endgame

Application Security

WAF & Application Security

Pentest Security Qualys Sucuri Alert Logic SH-PE Trustwave Anapnis Warakat Prevoty NSFOCUS ZENEDGE Certes Citrix Ergon SOHA

Vulnerability Assessment

Bugcrowd WhiteHat Security Rapid7 Trustwave Checkmarx SRCCLR McAfee Flexera Headlight Enterprise Synack BlackBuck NCCGroup Hackerone IBM Anapnis Core Veracode Digital snyk Outpost24 Qualys

Managed Security Service Provider

at&t SOLUTIONARY Verizon Clone Systems Trustwave nSPIRE OPTIV ALERT LOGIC Symantec IBM CSC SecureWorks IBM Security Services BT Cisco McAfee Wipro BAE SYSTEMS

Web Security

Blue Coat Distil Cisco Sophos StealthGen Security Wheel Cloudflare SH-PE Zscaler Zentao Forcepoint Webroot NexGuard Symantec Trend Micro GWAVA iBoss

Messaging Security

Proofpoint Forcepoint Microsoft Edgewise FireEye Cisco Trustwave PhishME Symantec McAfee Avast Avast Secure Mail Gateway McAfee Avast Avast Secure Mail Gateway McAfee Avast Avast Secure Mail Gateway

Risk & Compliance

ReView RedSeal GRX R-sam UpGuard Vocus MetricStream FICO FISMA FIRMENIA RiskSense BitSight tufin algosect Kenena Cylogic Neturix Verodin

Security Operations & Incident Response

IBM LogRhythm Sumologic RSA TIBCO Tenable EventTracker RedLock Panaseer Splunk Logpoint NetIQ Logscap Correllog Huntsman NetIQ Fortinet Netmonstry Alert Logic Fluency Logpoint

Security Landscape

Opswat Spiron Vera Nuro Thinair StorageCall Harvest.ai Wicr Idera GlobalVector Virtru Yphre PKWare Druuo CyberCloud Somansa Code42 CyberArk Somansa Code42 CyberArk

Mobile Security

Lookout MobileIron Skyeye Wandera Nuro Bitglass MOCANA TrustLock Airwatch TigerSec Apphority Moxiplex LaunchKey Vikei Wicr Ophidias CyberAPT Vikei Airlight NetScout Pindrop Goldpan Saldina

Security Incident Response

Hexadite Uplevel Ayeahu Flux Resilient Invotas Radar Demisto Skybox CyberCrash Security Hexis

Threat Intelligence

ISIGHTPARTNERS ThreatMetrix RiskIQ 472 DomainTools ThreatQuotient CyberScyramal digital shadows bandprotect serviceNow ThreatConnect Blueiv. electric IQ Diginis Flashpoint Farsight

Identity & Access Management

Coisvent Wheel Nok Nok Oracle PingIdentity Linken Cloudway WISKey GIGA Bitium Core CLEF UnboundID SaaSas okta Virgil Identity UnboundID SaaSas okta Virgil Identity

Cloud Security

Swamynt CloudPassage Humint RedLock Evidentio Zscaler Avanan ManageMethods SOHA Whielst Vaulite VERA CODE42 Cloudway Harvest.ai Covata Threat Stack HyTrust Oracle Palerra Microsoft CloudGuard Cato FORTYFOUR DOMEQ GuardTime Cato Fortify CloudIQ Clean DATA

Fraud Prevention / Transaction Security

FICO Linken Feedzai Iovation Ethoca Forter Guardian Analytics ThreatMetrix BDOcatch Early Warning IdenTrust AUXTIX SIGNIFYD sift science NUS Daily Security Secure Riskified Brighterion GordianMind MaxMind Acculynk Kount

Specialized Threat Analysis & Protection

FortScale Cenzar Bay Dynamics Invincea TRAPX exasim ZEROFox Interset GuardOne Sec3 observable JASK LightCyber SSB Mobile System Transperd Cymetria Area 1 Vectra Palantir Acalvio Cymetria Area 1 Protectwise Fireglass Sqrll Lastline Dataphy Avecto DeepInstinct Securonix Kildow Seculet Prelet Darktrace Novetta

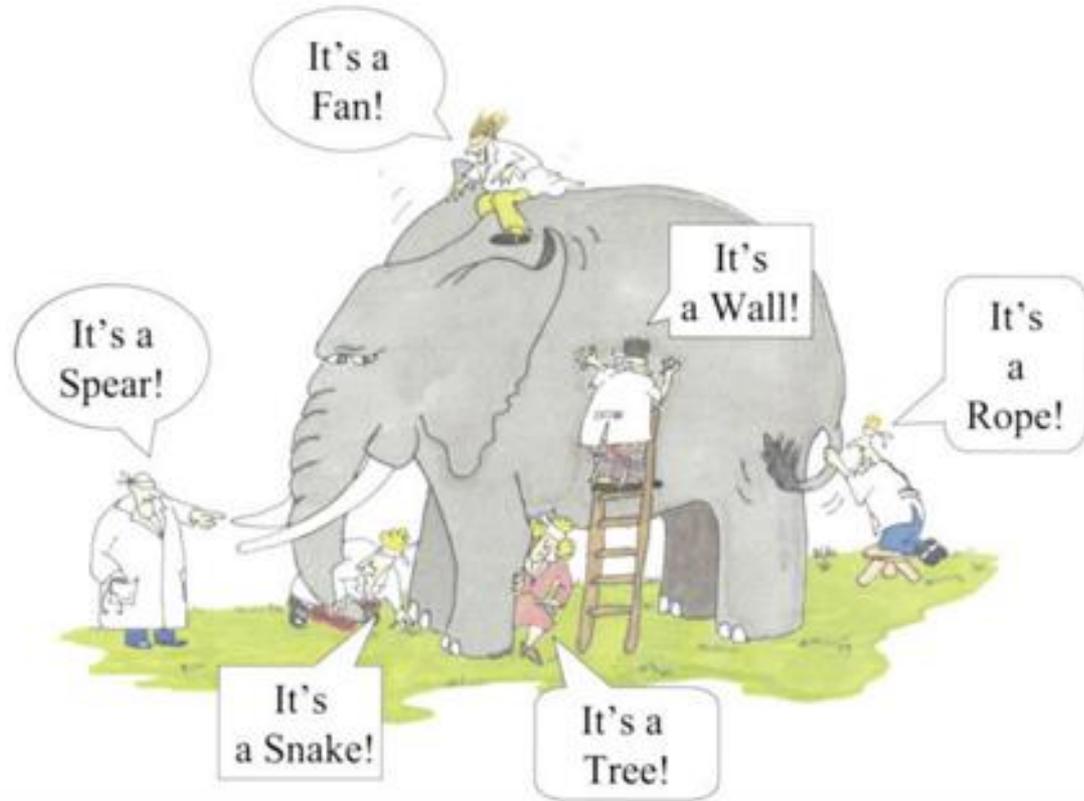
TOO MANY TOOLS, TOO MANY PEOPLE, TOO MANY ALERTS, TOO MANY CONSOLES, TOO MANY LOGS, TOO MANY GAPS, TOO COSTLY...OLD SCHOOL APPROACH...DETECT AND REMEDIATE...V AUTOMATED V&V.



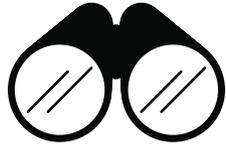


LOGS !!

Partial visibility without broader context = flawed conclusions



The four requirements for preventing successful attacks



Complete visibility

- All applications
- All users
- All content
- All endpoints
- Encrypted traffic
- SaaS & Cloud
- Mobile



Reduce attack surface area

- Block “bad” apps
- Limit app functions
- Limit file types
- Block high risk websites
- Verify users
- Limit devices
- Control sharing



Prevent all known threats

- Exploits
- Malware
- Command & control
- Malicious websites
- Bad domains
- Stolen credentials



Prevent new threats

- Dynamic analysis
- Exploit techniques
- Malware techniques
- Machine learning
- Static analysis
- Anomaly detection
- Analytics

Legislation isn't decreasing....GDPR....and Brexit wont help !

How do you define “state of the art” ?



Legislation isn't decreasing contd....NIS: Network and Information Security Directive...(U.K Gov)



[Departments](#) [Worldwide](#) [How government works](#) [Get involved](#)
[Policies](#) [Publications](#) [Consultations](#) [Statistics](#) [Announcements](#)

[Home](#)

Open consultation

Consultation on the Security of Network and Information Systems Directive

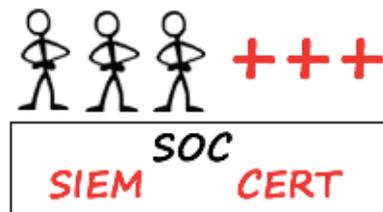
From: [Department for Digital, Culture, Media & Sport](#) and [The Rt Hon Matt Hancock MP](#)
Part of: [Cyber security](#)
Published: 8 August 2017



675 000 (THREATS/APPS)

1.5 M SHORTFALL (F & S)

25 BN/IP



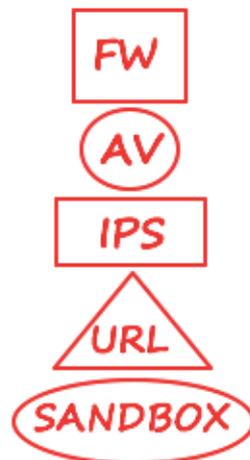
RECY
EXP
MAL
CC
EXFIL



PREVENT



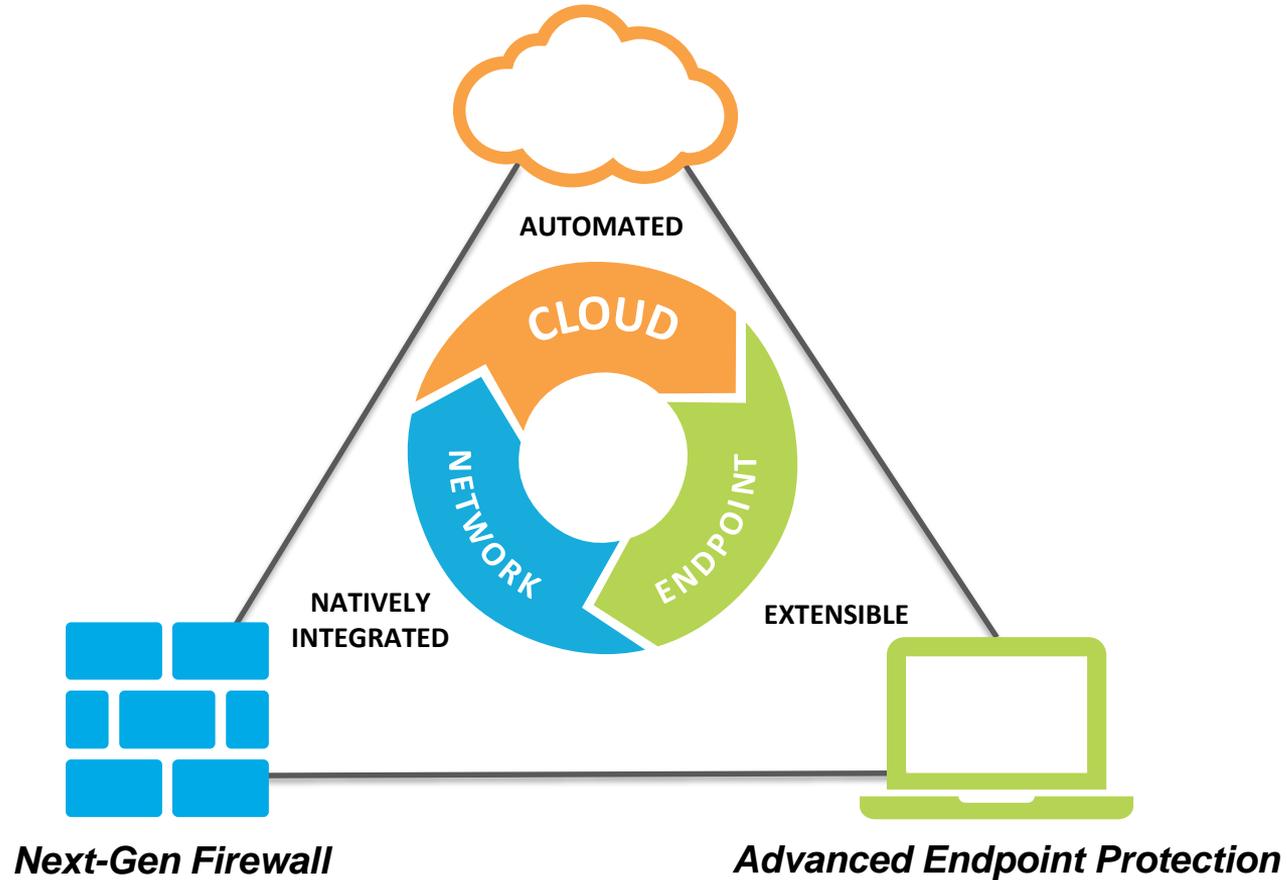
SELF LEARN



!!!!!!!
↑ MANUAL COSTS



Threat Intelligence Cloud





Thank you...

<https://youtu.be/Rs17MirSa8Q>

***if you ant to really understand what we do.....
Or come to talk to us.***

kpoyser@paloaltonetworks.com

+447711773878