Using Machine Learning to prevent modern cyber attacks

Presenter: Domenico Stranieri | System Engineer | Palo Alto Networks

paloalto NETWORKS

SUCCESSFUL ATTACKS REQUIRE MULTIPLE STEPS

Attack Lifecycle

Vulnerability Exploit → Malware Installation → Command and Control → Lateral Movement → Data Exfiltration

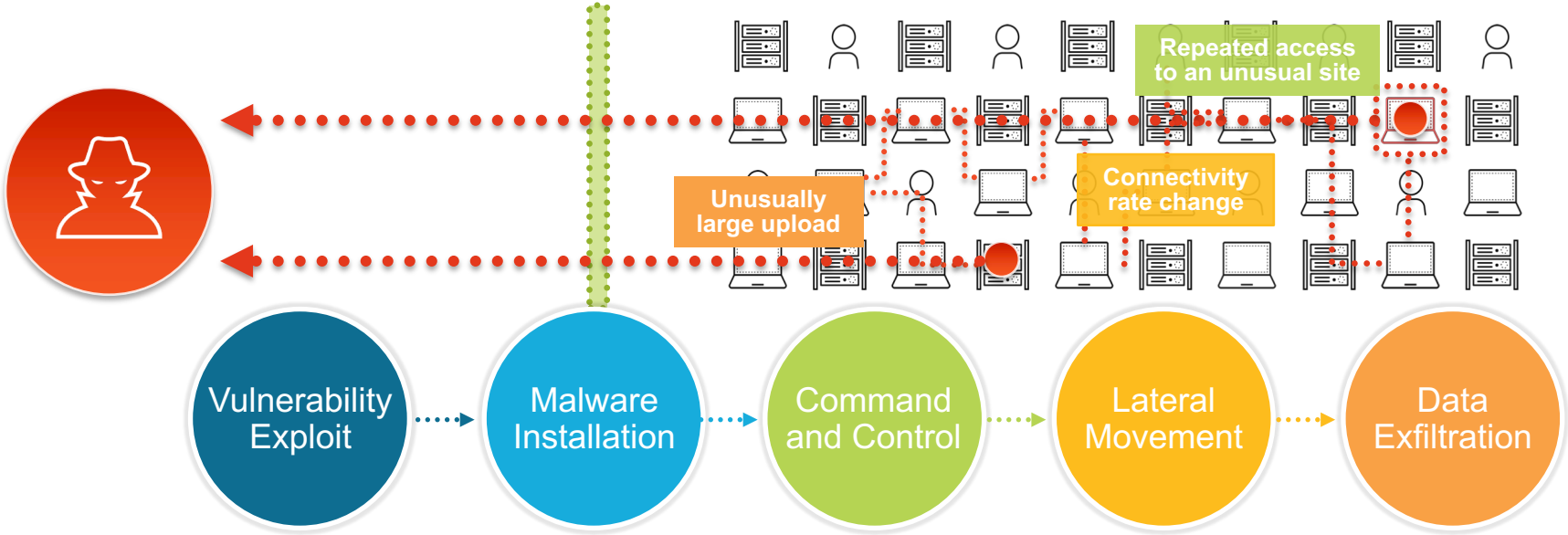
- Occurs in seconds to minutes
- Involves a small number of network actions
- Can often be identified by IoCs

- Occurs over days, weeks, or months
- Involves a large number of network actions
- Can rarely be identified by IoCs

Disrupt every step to prevent successful cyberattacks

DETECTION AND RESPONSE MUST BE DIFFERENT

- Attackers must perform thousands of actions to achieve their objective
- Each individual action may look innocent



By profiling behavior, organizations can detect the behavioral changes that attackers cannot conceal

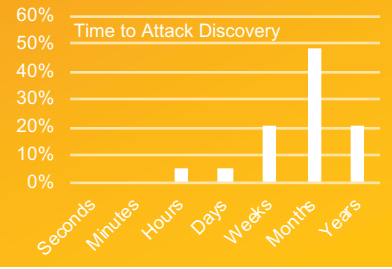
STEALTHY THREATS THAT LEAD TO DATA BREACHES

Targeted Attacks

- Multi-stage, manual attacks are the most financially devastating

$3.62 million
average cost of a breach

Malicious Insiders



25%
of breaches involve insiders

And it takes months to discover attacks

Risky Behavior

14%
data breaches caused by human error

- Risky behavior increases risk of malicious attacks

Compromised Endpoints

51%
data breaches leverage already compromised machines

$2.4 million
Average cost of malware per company

Verizon Data Breach Investigations Report, Cost of Cybercrime Study, Ponemon Institute

TODAY'S DETECTION & RESPONSE ARE NOT ENOUGH

Wrong Data

Inconsistent logs; mostly violations

Collecting right data requires deploying sensors and agents

Lack of Scale

Not built for big data

Cost-prohibitive to log necessary data

Slow software release cycles

Static Rules

Manually-defined correlation rules

- Hard to develop and maintain
- False positives

Slow Investigations

Repetitive processes

Manual endpoint forensics

- Days or weeks to block threats

WHAT IS NEEDED

Rich Data

Comprehensive network, endpoint and cloud data collected by existing infrastructure

Cloud Scale & Agility

Cloud elasticity for data storage

Rapid innovation

Machine Learning

Machine learning to profile behavior and automatically detect attacks

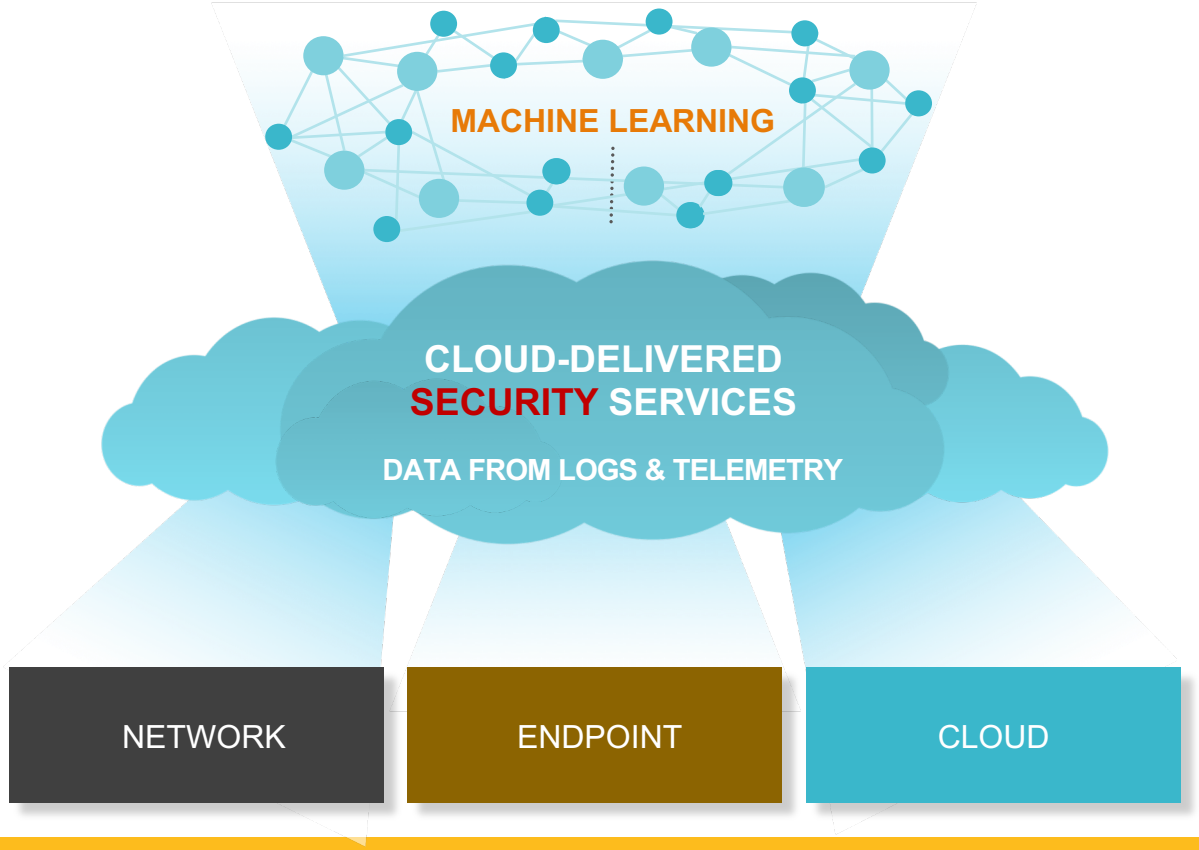
Rapid Response

Small number of actionable alerts

Threat intelligence and endpoint analysis

Firewall remediation

HOW BEHAVIORAL ANALYTICS CAN HELP

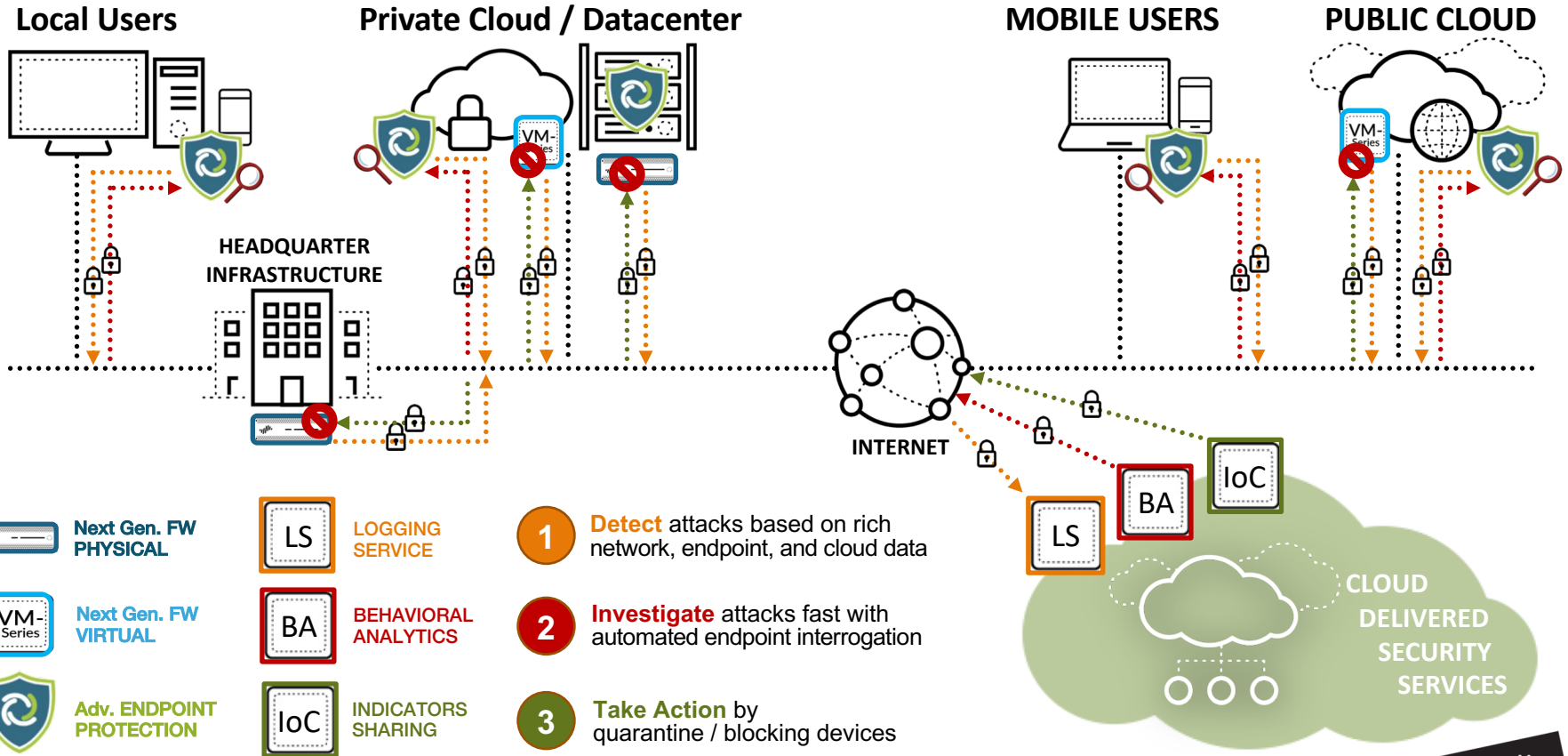


Analyze rich network, endpoint and cloud data with machine learning

Accelerate investigations with endpoint analysis

Gain scalability, agility and ease of deployment as a cloud-delivered app

HOW BEHAVIORAL ANALYTICS CAN HELP



HOW B. ANALYTICS CAN STOP STEALTHY THREATS

	Automatic Detection	Streamlined Investigation	Rapid Response
Targeted Attacks	Command and Control, Internal Reconnaissance, Remote Command Execution	 Actionable alerts with context of: • User • Endpoint • Process	 Firewall remediation: • Block attack sources • Block malicious destinations
Malicious Insiders	New Administrative Behavior, Exfiltration		
Risky Behavior	Large File Uploads, Remote Desktop Services		
Compromised Endpoints	Spambot Behavior, Command and Control , Malware Behavior		

Questions & Answers

Thank You!

Domenico Stranieri

Pre-Sales System Engineer

Palo Alto Networks | EMEA Italy

e: dstranieri@paloaltonetworks.com

m: +39 338 6986710

