Dealing with advanced threats with RSA Security Analytics & ECAT

Chezki Gil, EMED Sales Director

EMC²

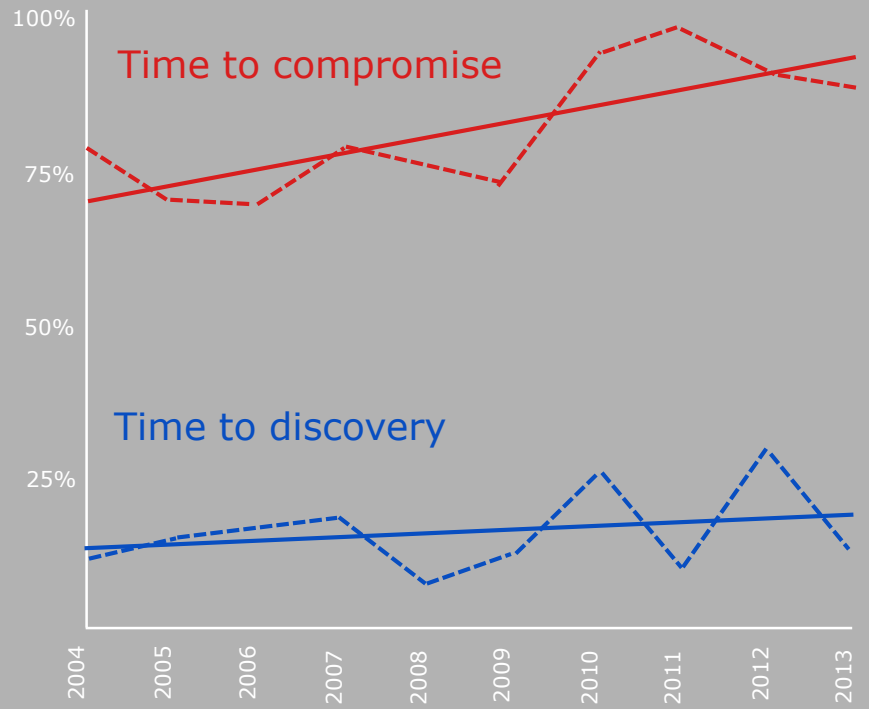
RSA

Attackers are Outpacing Defenders

Percent of breaches where time to compromise (red)/time to Discovery (blue) was days or less

Attacker Capabilities

Time to Discovery



VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

Evolution of Threat Actors & Detection Implications

Firewall

IDS/IPS

AntiVirus

Whitespace

Successful HACKS

Corporate Assets

At first, there were HACKS

Preventative controls filter known attack paths

Evolution of Threat Actors & Detection Implications

Firewall — Blocked Session

IDS/IPS — Blocked Session

AntiVirus — Blocked Session

More Logs — Alert

SIEM

Whitespace ← **Successful ATTACKS**

Corporate Assets

At first, there were HACKS

Preventative controls filter known attack paths

Then, ATTACKS

Despite increased investment in controls, including SIEM

Evolution of Threat Actors & Detection Implications

Firewall — Blocked Session

IDS/IPS — Blocked Session

AntiVirus — Blocked Session

Logs — Alert

Endpoint Visibility — Process

Network Visibility — Network Sessions

Security Analytics

Corporate Assets

Now, successful ATTACK CAMPAIGNS target any and all whitespace.

Complete visibility into **every process and network sessions** is required to eradicate the attacker opportunity.

Unified platform for advanced threat detection & investigations

A Logs-Only Approach to Detection Isn't Working

99%

Percent of successful attacks went **undiscovered by logs**

Percent of incidents that took **weeks or more** to discover

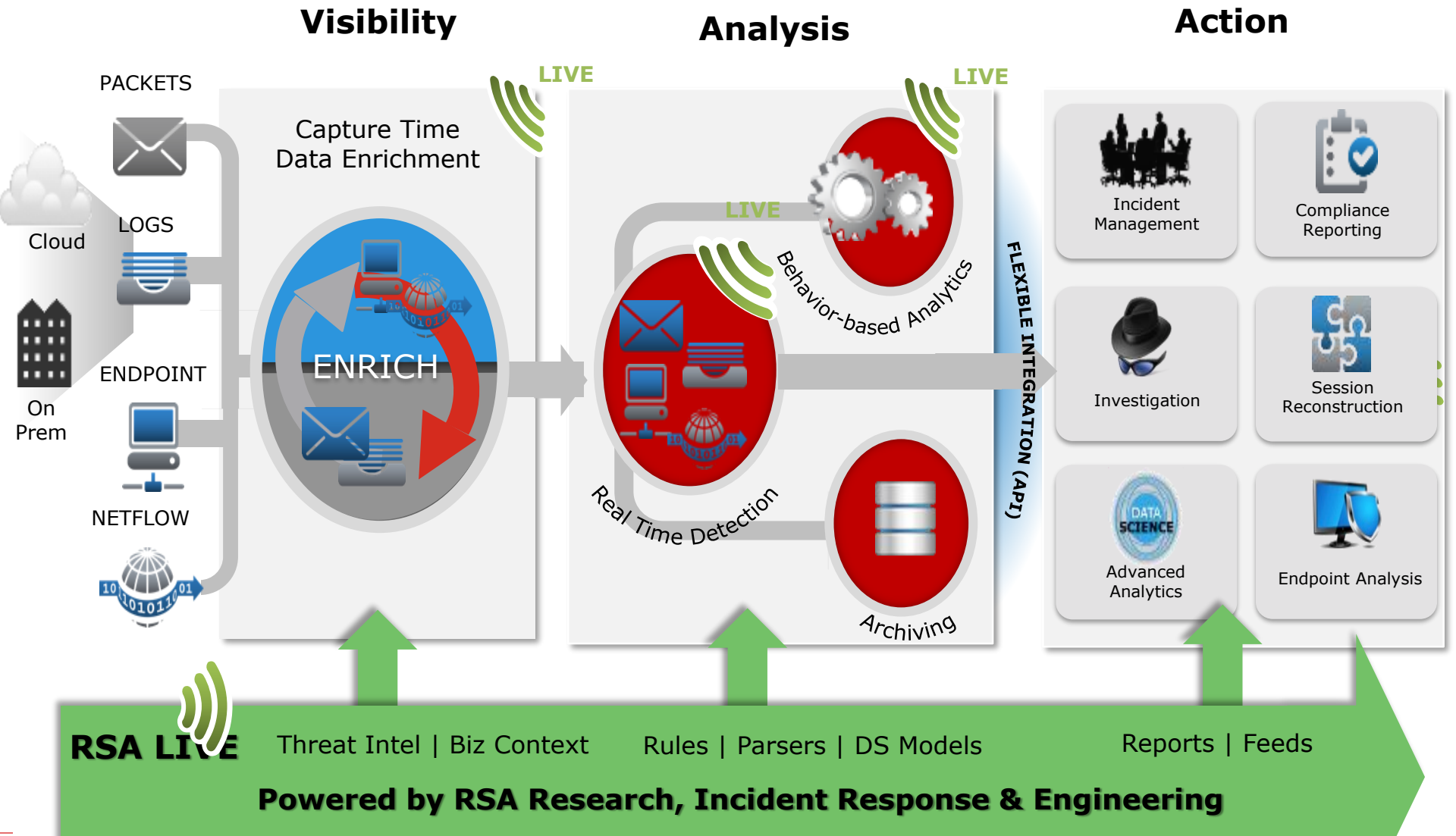
83%

- VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

RSA Strategy

RSA Security Analytics Platform

Capture, enrich and analyze data from across your network



Proven and Widely Deployed Solution

1,600+ Customers worldwide

Top 20 U.S. Financials

90+ Countries worldwide

70+ U.S. Federal/Govt. Agencies

RSA