



THREAT EXPOSURE MANAGEMENT

Fedon Konstantinou
Security Engineer
ITway Hellas

Agenda

- › Rapid7 Overview
- › Metasploit
- › Nexpose
- › Appspider
- › Q & A

Rapid7 Timeline



› 2000 - Founded by Alan Matthews, Tas Giakouminakis & Chad Loder

› **2004 - Nexpose Commercial Release**

› 2008 - Bain Capital Ventures invests \$10 million in Rapid7



› **2009 - Acquired the Metasploit Project**

› 2011 - Technology Crossover Ventures invests \$50 million in Rapid7



› **2012 - Acquired Mobilisafe**

› 2013 - Founded Rapid7 Labs



› **2013 - Announcement of new Products: ControlsInsight & UserInsight**

› 2014 - Bain Capital Ventures invests \$30 million in Rapid7

› **2015 - Announcement of new Acquisition: NTOBJECTives becomes Rapid7 Appspider**

› **2015 - RAPID7 IPO - NASDAQ "RPD"**

› **2015 - Acquisition of LogEntries (log search engine) to boost Rapid7's analytics platform**



RAPID7



NASDAQ: RPD

Delivering Security Data & Analytics

that revolutionize the practice of cyber security

800+

Employees

90+

Countries































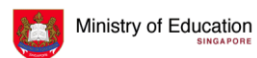









5,100+

Customers

34%

Fortune 100

5,100+ Customers in More Than 90 Countries

Technology/ Communication	Retail/ Wholesale	Energy	Financial Services	Healthcare	Manufacturing
      	      	  	   	    	    
Education	Media & Entertainment	Government Public Sector	Others		
  	  	  	  		

Addressing Threat Exposure Challenges

0101101
1000101
0101101
1000101

Data Problem

Lack of understanding
of environment and
context across
physical, virtual, cloud
and mobile



Attacker Blind Spot

Asset data, control
data & threat data
operating ineffectively
in isolation



Scan and Patch

Remediation practice
not effective or
credible & lacks
operational measures
across IT

Rapid7 Product Portfolio



- Vulnerability Verification
- Penetration Testing
- Reduce Phishing Exposure
- Password Auditing
- Test Security Controls



- Vulnerability Management
- Security Configuration Assessment
- Web Application Security
- Virtualization Security
- PCI Compliance Management



- Continuously applications monitoring
- Automated virtual patching
- Meet compliance requirements
- Quickly re-play web attacks

Rapid7 Workflow

Know your
weak points



Prioritize what
matters most



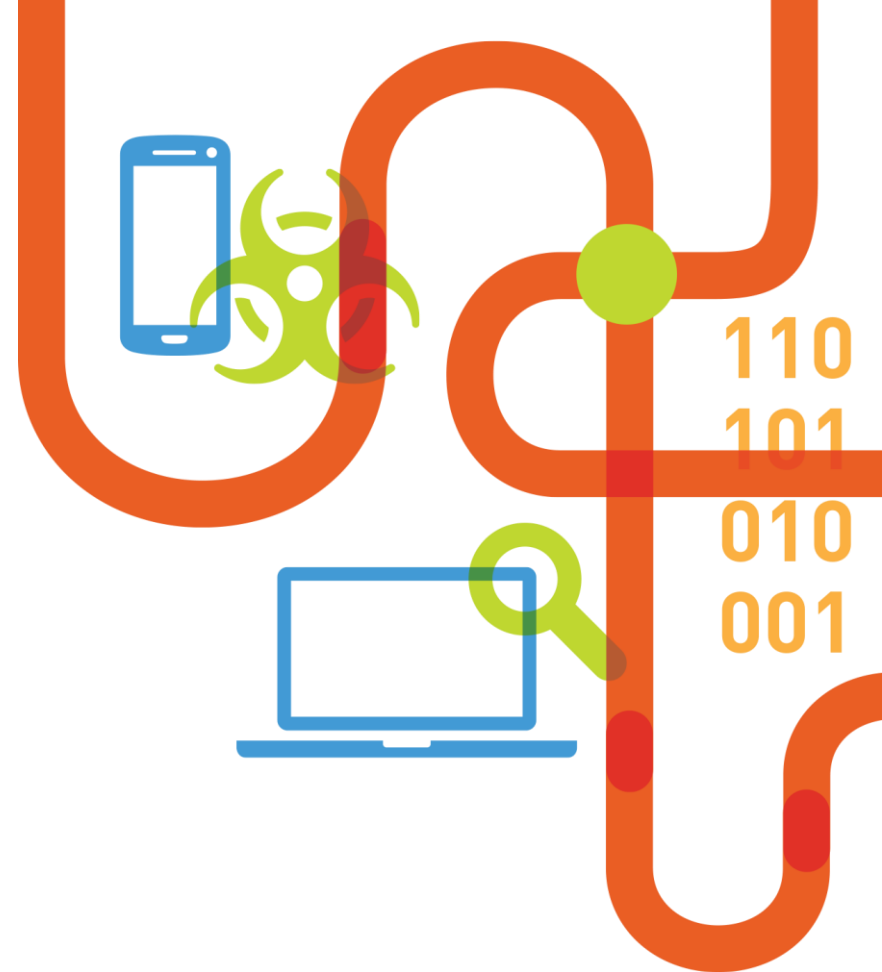
Improve Your
Outcomes



RAPID7

metasploit[®]

Reduce Your Risk of a Breach



metasploit[®]

Utilize world's largest code-reviewed exploit database



Community
Members



Exploit Modules



MetaModules

Simulate real-world attacks
against your defenses



Evade Anti-Virus,
Firewall, and IPS



200 Post-exploitation
modules



VPN Pivoting

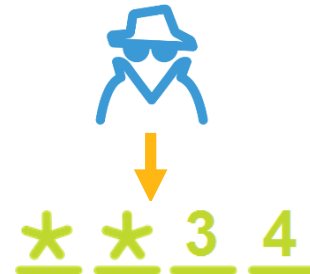
Uncover weak and reused
credentials



Threat Action
(Verizon DBIR 2015)



Brute-force



Password Auditing

metasploit[®]

Run penetration testing
programs at scale



Multiple Projects



Multiple Users

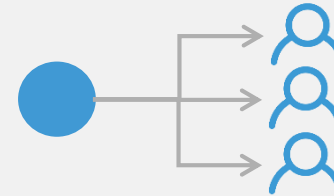


Task Chaining

Reduce user risk using
phishing campaigns and
education



Clone Webpages



Send, track, and
target education



Measure User
Risk

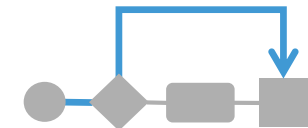
Complete compliance
programs faster



Customizable Audit
Reporting



Compliance Reports

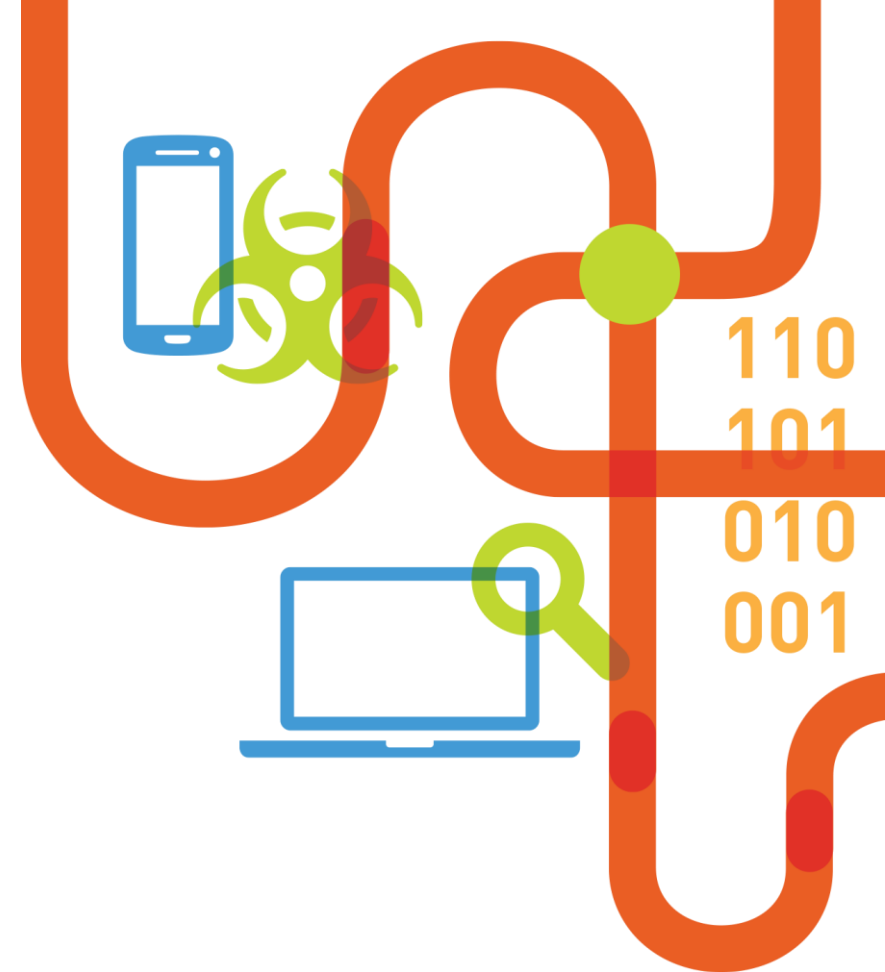


Validate Vulnerabilities,
Identify Exceptions

RAPID7

nexpose®

Reduce Your Risk of a Breach



Nexpose Awards

Uncover your hidden
attack surface



Physical



Virtual

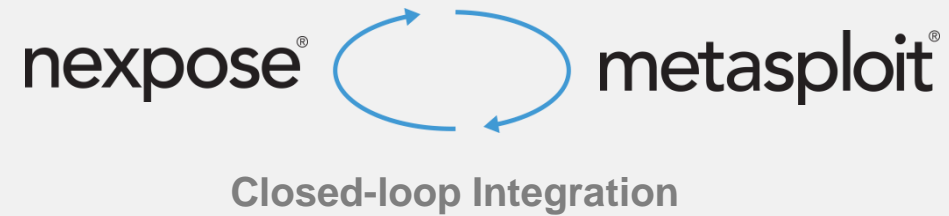


Cloud



Mobile

Validate Vulnerabilities
with Metasploit[®]



Contextualize assets using
RealContext[™]



Asset Owner



Asset Location



Asset Importance

Focus on the highest risks with RealRisk™



Granular Scoring
(0-1000)



Exploit & Malware Kit
(Increases risk)



Weighted Scoring
(using RealContext™)

Deliver impactful,
actionable remediation
plans



Owner Assignment
(using RealContext™)



Top remediation
reports



Clear steps
to follow

Implement best practice
security controls



Visualize deployment
of controls



Measure effectiveness
of controls



Prioritizes controls for
implementation

RAPID7

appspider

Application Assessment for the Modern World



Web applications are a primary target...

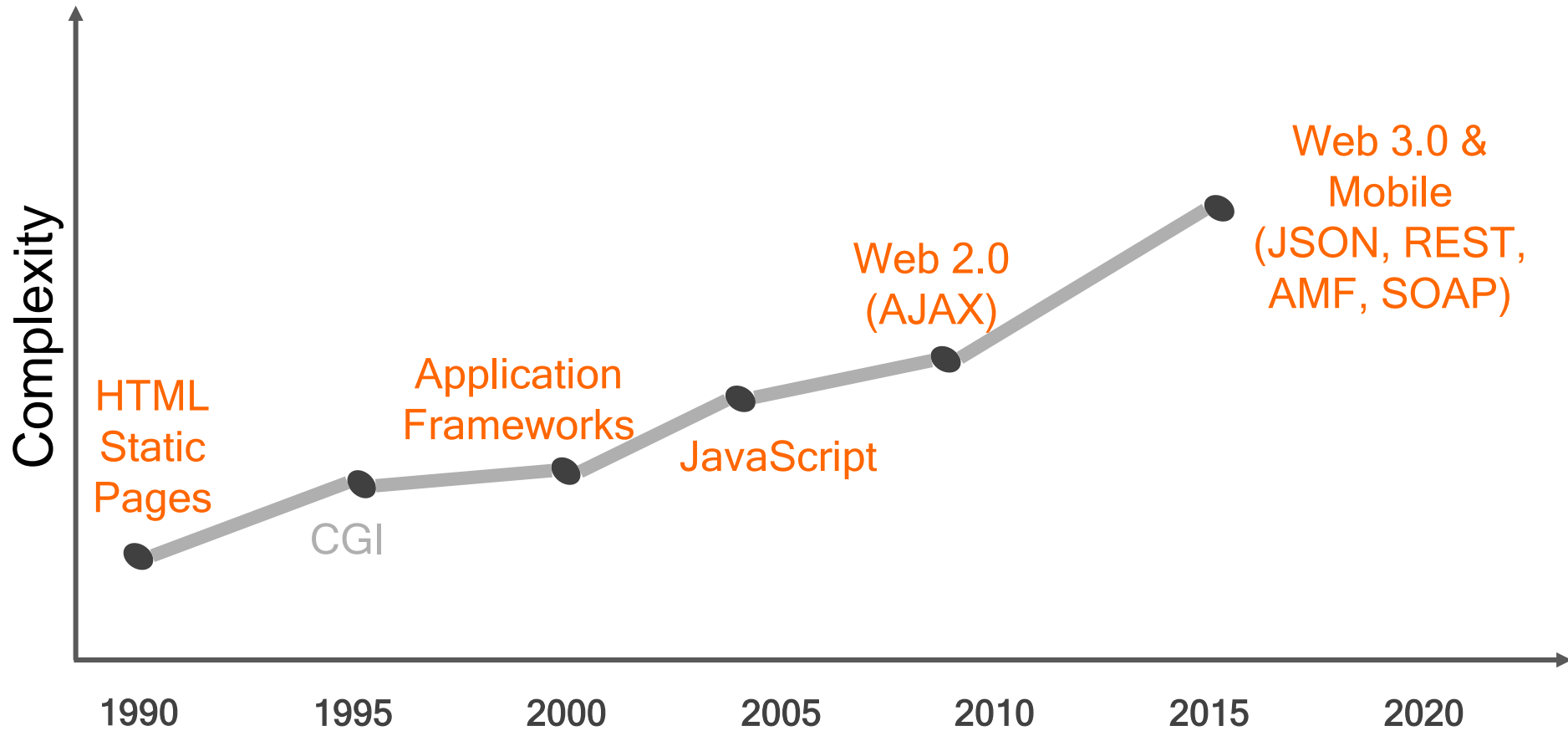
Web application attacks remain the most frequent incident pattern in confirmed breaches and accounted for up to 35% of breaches in some industries.

The 2015 Verizon Data Breach Investigation Report



35%

So, why is application security still so hard?



appspider

Application Assessment for the Modern World



Maximum application testing and breadth of coverage



Deep analysis with interactive reports



Automated WAF and IPS virtual patching

SIEM



RSA

solarwinds



splunk

ArcSight
An HP Company

LogRhythm



RAPID7 Technology Partner Ecosystem

Ticketing

servicenow



Credentials



IT GRC

RSA



Agilance



eGestalt

Virtualization

vmware



Topology Risk



FIREMON



SaaS



Google Apps



NGFW - IPS

SOURCEfire

IBM



Patch



Windows Server

IBM

vmware

NAC



ForeScout

WAF

IMPERVA



THANK YOU