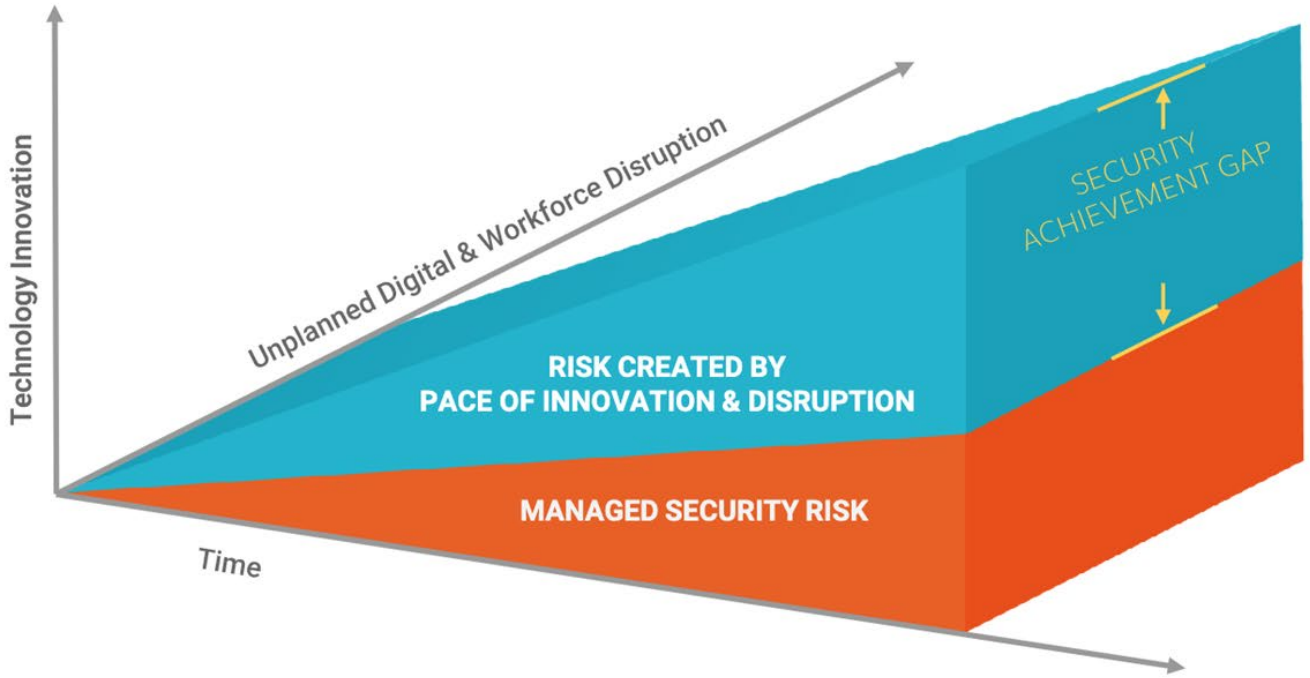
RAPID7

Bridging the Security Achievement Gap

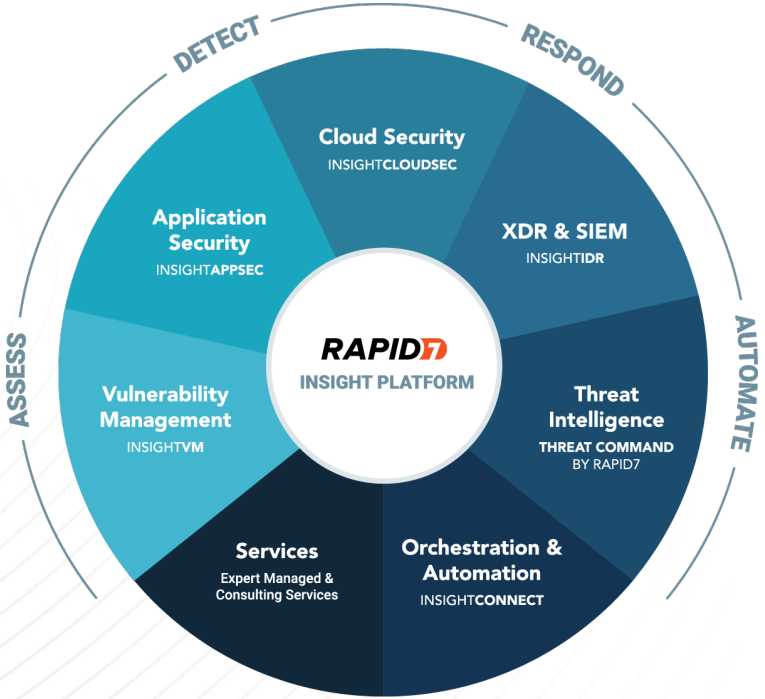
David Higgs | CISSP, CEH, CCNP

Senior Security Solution Engineer – Eastern Europe & Italy

Increasing Unmanaged Risk



Comprehensive security that powers your business.



Technology

Best-in-Class Portfolio

Unified Platform Services

Plug and Play Integrations

Intelligent Automation

Expertise

Security Research

Open Source Community

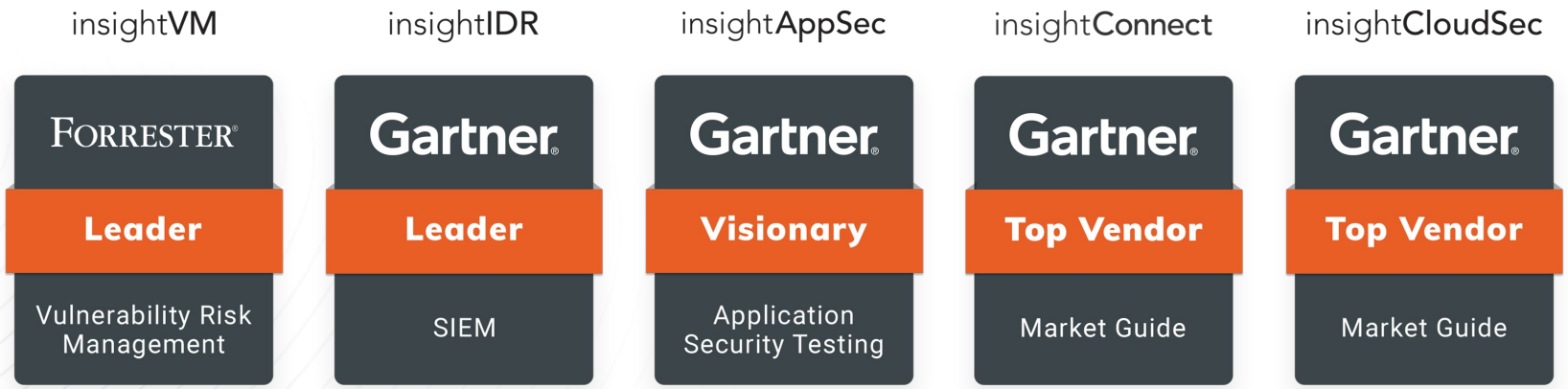
Differentiators

Flexible Product and Managed Services Mix

Time to Value

Vendor Consolidation

Best-in-class solutions all in one platform.



Our leading-edge research instantly gives customers unparalleled intelligence.

Metasploit

The most used penetration testing tool

Project Sonar

Internet-wide scans

Attacker KB

Vulnerability database

Project Heisenberg

Global honeypot network

Velociraptor

Digital forensic endpoint detection and response

Vulnerability Disclosures

Publicly released security flaw data

Rapid7 Knowledge and Threat Intelligence

Rapid7 Customers

Vulnerability Disclosure

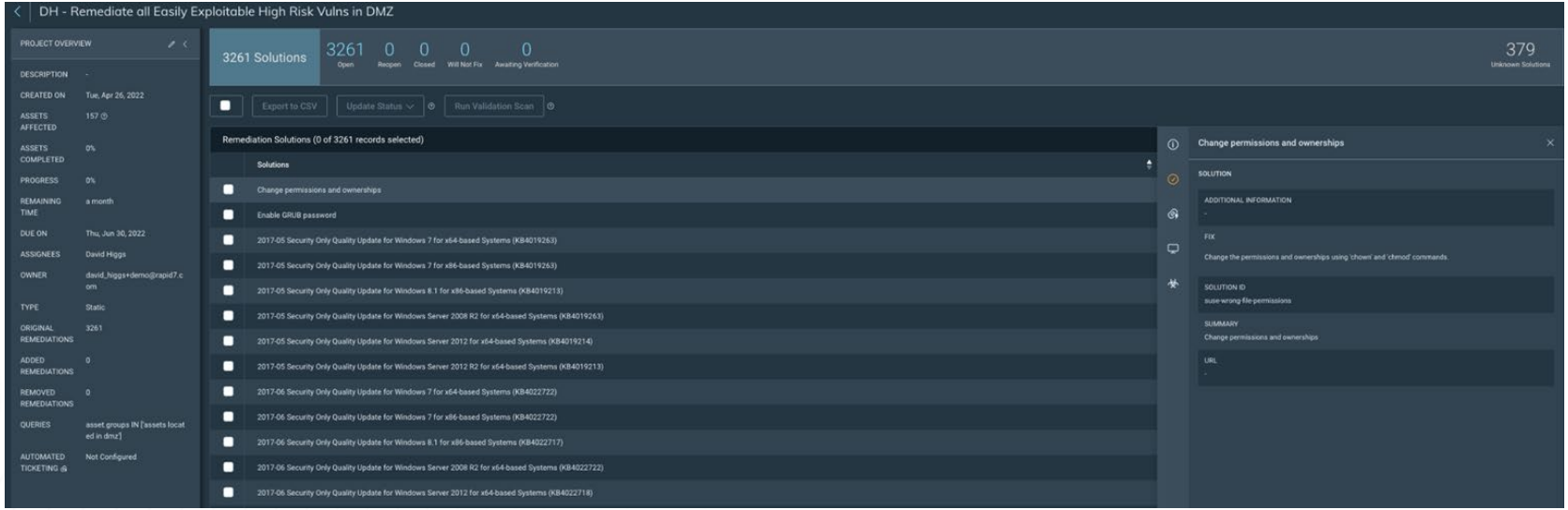
Intelligence Sharing

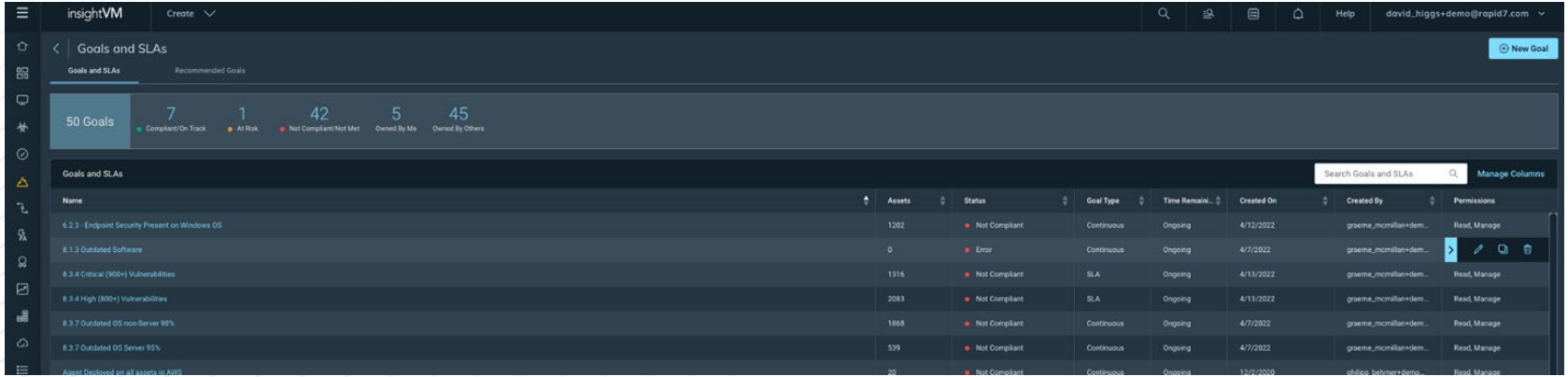
Threat Hunters

Metasploit Community

Project Heisenberg

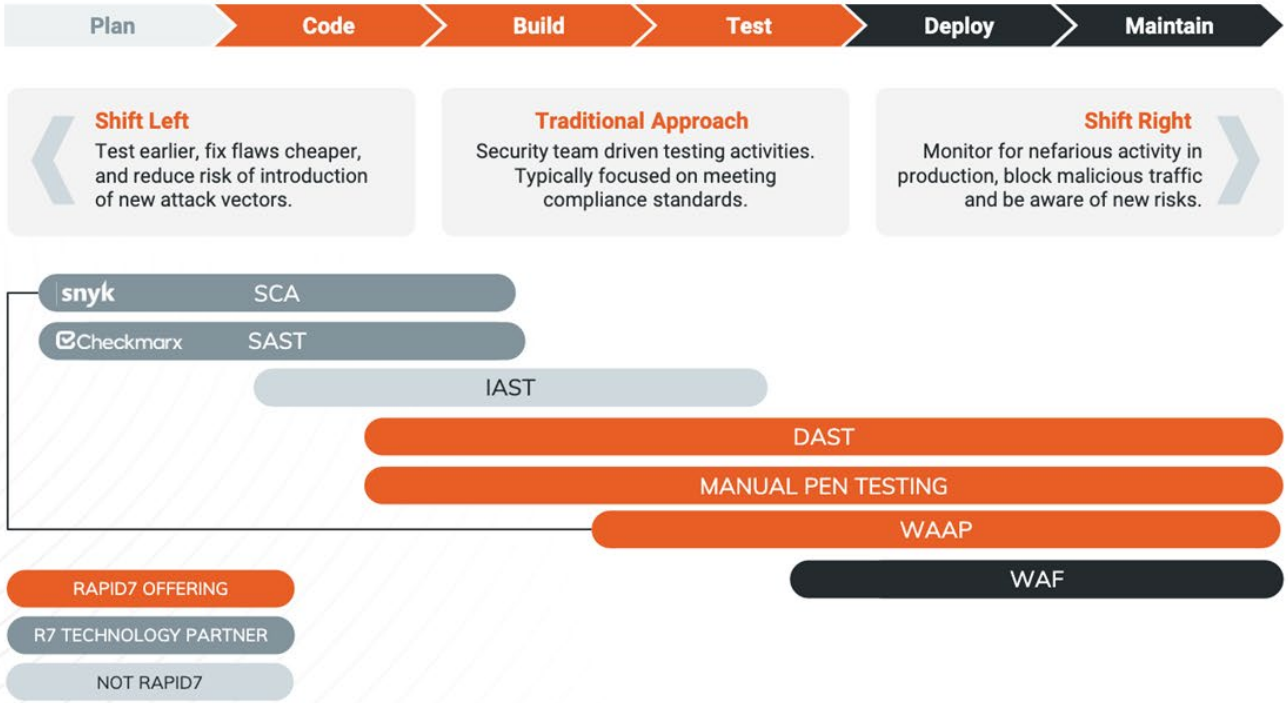
Project Sonar


DH - Remediate all Easily Exploitable High Risk Vulns in DMZ
PROJECT OVERVIEW
DESCRIPTION
CREATED ON Tue, Apr 26, 2022
ASSETS AFFECTED 157
ASSETS COMPLETED 0%
PROGRESS 0%
REMAINING TIME a month
DUE ON Thu, Jun 30, 2022
ASSIGNEES David Higgs
OWNER david_higgs+demo@rapid7.com
TYPE Static
ORIGINAL REMEDIATIONS 3261
ADDED REMEDIATIONS 0
REMOVED REMEDIATIONS 0
QUERIES asset groups IN ['assets located in dmz']
AUTOMATED TICKETING Not Configured
3261 Solutions
3261 Open
0 Reopen
0 Closed
0 Will Not Fix
0 Awaiting Verification
379 Unknown Solutions
Export to CSV
Update Status
Run Validation Scan
Remediation Solutions (0 of 3261 records selected)
Solutions
Change permissions and ownerships
Enable GRUB password
2017-05 Security Only Quality Update for Windows 7 for x64-based Systems (KB4019263)
2017-05 Security Only Quality Update for Windows 7 for x86-based Systems (KB4019263)
2017-05 Security Only Quality Update for Windows 8.1 for x86-based Systems (KB4019213)
2017-05 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4019263)
2017-05 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB4019214)
2017-05 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4019213)
2017-06 Security Only Quality Update for Windows 7 for x64-based Systems (KB4022722)
2017-06 Security Only Quality Update for Windows 7 for x86-based Systems (KB4022722)
2017-06 Security Only Quality Update for Windows 8.1 for x86-based Systems (KB4022717)
2017-06 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4022722)
2017-06 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB4022718)
Change permissions and ownerships
SOLUTION
ADDITIONAL INFORMATION
FIX
Change the permissions and ownerships using 'chown' and 'chmod' commands.
SOLUTION ID
suse-wrong-file-permissions
SUMMARY
Change permissions and ownerships
URL

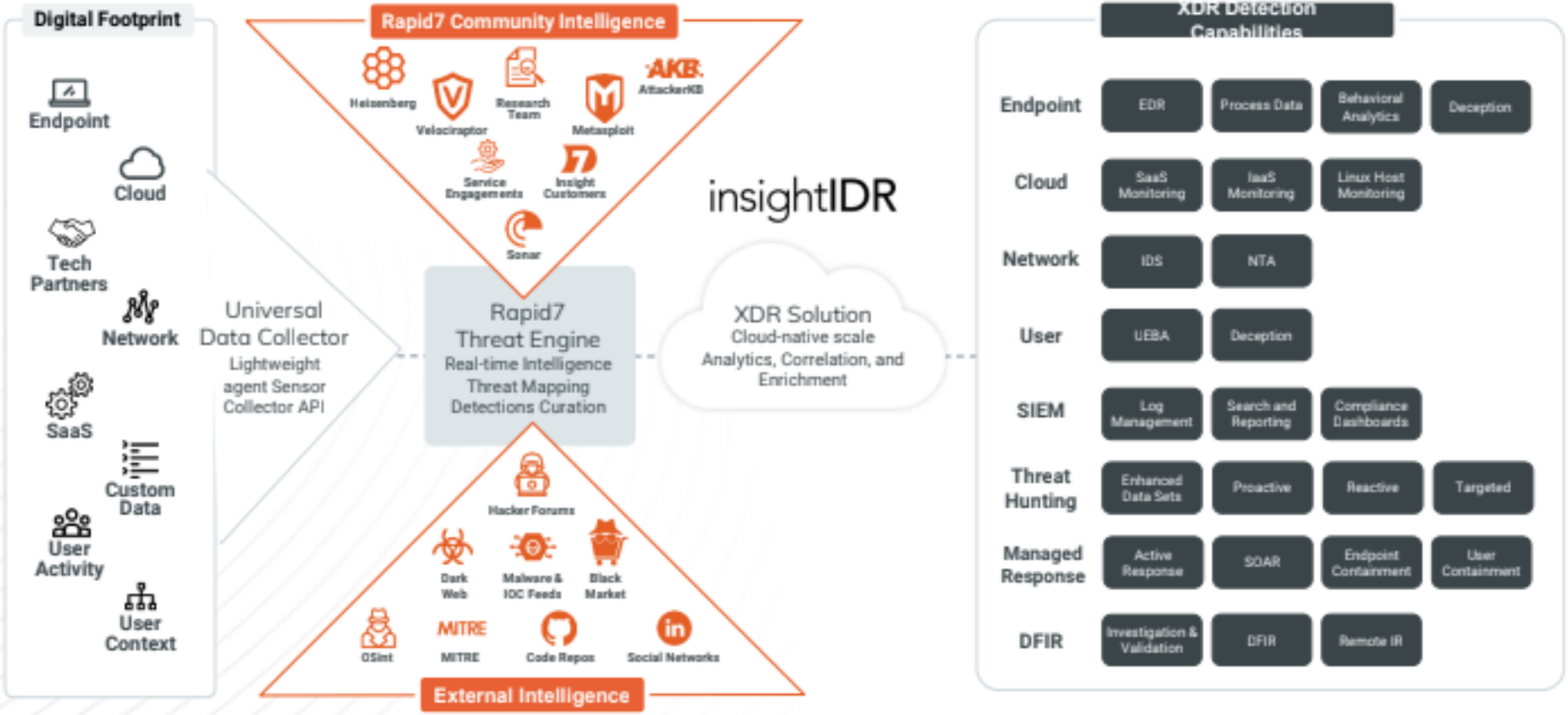

insightVM
Create
Help
david_higgs+demo@rapid7.com
Goals and SLAs
New Goal
Goals and SLAs
Recommended Goals
50 Goals
7 Compliant/On Track
1 At Risk
42 Not Compliant/Not Met
5 Owned By Me
45 Owned By Others
Goals and SLAs
Search Goals and SLAs
Manage Columns
Name
Assets
Status
Goal Type
Time Remaini...
Created On
Created By
Permissions
6.2.3 - Endpoint Security Present on Windows OS 1202 Not Compliant Continuous Ongoing 4/12/2022 graeme_mcmillan+dem... Read, Manage
8.1.3 Outdated Software 0 Error Continuous Ongoing 4/7/2022 graeme_mcmillan+dem... Read, Manage
8.3.4 Critical (900+) Vulnerabilities 1316 Not Compliant SLA Ongoing 4/13/2022 graeme_mcmillan+dem... Read, Manage
8.3.4 High (800+) Vulnerabilities 2083 Not Compliant SLA Ongoing 4/13/2022 graeme_mcmillan+dem... Read, Manage
8.3.7 Outdated OS non-Server 98% 1868 Not Compliant Continuous Ongoing 4/7/2022 graeme_mcmillan+dem... Read, Manage
8.3.7 Outdated OS Server 95% 539 Not Compliant Continuous Ongoing 4/7/2022 graeme_mcmillan+dem... Read, Manage
Agent Deployed on all assets in AWS 20 Not Compliant Continuous Ongoing 12/2/2020 philipp_behmer+demo... Read, Manage

We disrupt attackers, not your tech stack.

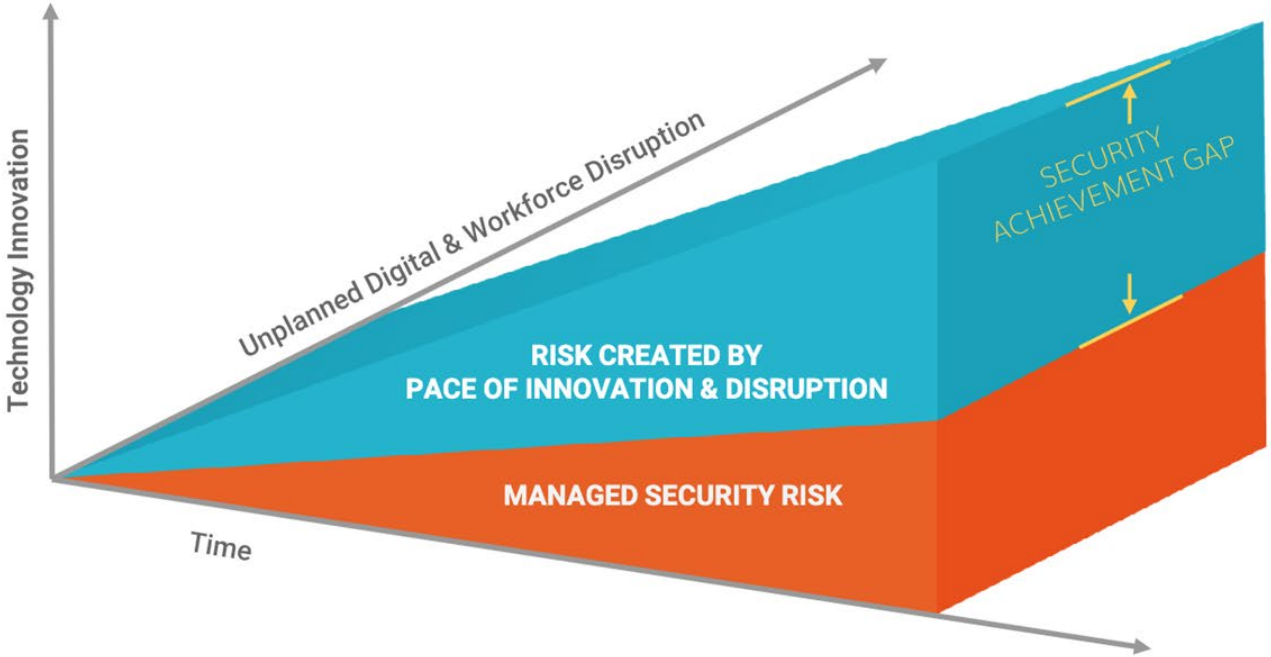
Where does Rapid7 fit in?



We use XDR to detect the threats others miss



Increasing Unmanaged Risk



Thank you!

Please stop by the stand for demos or just a chat!