AGCPARTNERS

April 2017
INSIGHTS

Security Orchestration & Automation

Bridging the Gap Between Alert Overload and Analyst Capacity

Eric Davis, *Partner*
Maria Lewis Kussmaul, *Co-Founder, Partner*
Ben Howe, *Co-Founder, CEO*
Russ Workman, *Partner*

The Cybersecurity Capacity Problem

Evolving threats impact increasing breadth of attack surface

- Threat environment is evolving rapidly as organizations move their sensitive data and applications to the cloud, workforces become more mobile, and IoT is everywhere
- Attacks have become more powerful (e.g. DDoS via IoT devices vs. PCs) and destructive
- Nation-state involvement as well as ready consumerization of sophisticated attack tools fuels attacker advantage

Security Analysts are Bedeviled by Scale

- SYMC discovered over **430 million** new and unique examples of malware in 2015, **36%+ YoY**
- 451 Research counts over **1,300 security vendors** on top of an ever-expanding attack surface
- Mandiant's M-Trends report shows an average pre-discovery **dwell time of 5 months**

Emergence of new technologies built to tackle the growing attack surface, resulting in many organizations managing their security in silos and lacking a holistic, integrated approach

- Enterprises currently deploying tens to hundreds of "best-of-breed" point products, lacking the necessary context

Growing need to bridge the gap between alert overload and analyst capacity

- Critical shortage of skilled cybersecurity professionals – as many as 1 million unfilled cybersecurity jobs globally
- 92% of companies get more than 500 alerts per day, with some getting as many as 5x that amount; a single cyber analyst can handle roughly 10 alerts per day, illustrating the capacity gap

This mismatch between alerts and capacity causes many attacks to go undetected and lengthens attacker dwell time, increasingly leading to mega-breaches that destroy reputations and shareholder value

- Analysts investigate only 4% of alerts, suggesting that human resources alone are woefully insufficient to keep organizations safe

Sources: Enterprise Strategy Group, Ponemon Institute, Enterprise Management Associates, 451 Research, Symantec, FireEye

Defining Security Orchestration & Automation

Security orchestration and automation tools seek to bridge the gap between alert overload and analyst capacity by automating the detection, investigation, and remediation workflow, freeing skilled cyber professionals to focus on higher-value work

What is Security Orchestration & Automation?

- Orchestration platforms connect existing security tools together with the goal of bringing simplicity, context, and efficiencies to complex customer security product environments
- Automation refers to the process of injecting efficiencies into the IR workflow and can range from tools that accomplish this by codifying workflows or performing actions based on scripts to full machine-based automation
- Orchestration and automation platforms are increasingly converging in functionality in an attempt to optimize value and uptake as an end-to-end efficiency platform

Gartner and 451 Research coined the following concepts, which dovetail with the emergence of security orchestration:

Security Operations, Analytics, and Reporting (SOAR)

- Support workflow management and automation, analytics, and reporting
- Enables security operations teams to automate and prioritize security operational activities and report data to inform better business decision-making

Actionable Situational Awareness Platform (ASAP) – Better integration, fewer silos, reaping the advantages of automation

- Intake of internal monitoring and assessment data
- Correlation with threat intelligence
- Synthesis and (where human interaction plays a role) visualization of findings through the application of analytic techniques
- Automation of response: emphasis on integrated automation to translate insight directly into action

Sources: Gartner, 451 Research, Zion Market Research

Orchestration and Automation Functionality in ASAP & SOAR

The Actionable Situational Awareness Platform

Gathering

- Internal assessment, monitoring & investigation

- External intelligence shared across organizations

CORE ORCHESTRATION AND AUTOMATION FUNCTIONALITY

Synthesis

- Integration across data silos to improve data quality and enhance context to optimize response

- Eliminate information overload and alert fatigue
- Leveraging machines and human superiority where each can be most effective

Action

- Coupling insight with consistent, effective response

- Emphasis on automation integrated with the outcomes of synthesis
- Alignment with broader automation initiatives defining "new IT"

Security Operations, Analytics and Reporting Stack

Detection

Assessment

Impact and Risk Analysis / Modelling, Threat Intelligence Fusion

Response

Policies, Processes, Playbooks, Triage

Mitigation

Configuration / System Change, Application Patching / Rule / Signature Creation

Sources: 451 Research, Gartner

Orchestration and Automation in Incident Response

Orchestration and Automation are often used interchangeably in Incident Response contexts. Both are core components of an efficient security platform, but in fact address two distinct challenges

- Orchestration platforms connect existing security tools together, integrating with hundreds of leading point products out of the box and providing functionality to integrate with new products in the future. Orchestration tools seek to simplify complex security ecosystems, often layering additional context in a single pane of glass user interface
- Automation platforms inject efficiency in the IR workflow by automating many of the manual processes in alert investigation and remediation. Automation vendors leverage deep and accurate data-driven visibility into the customer's environment and provide context around this data. They achieve this both through proprietary IP and through partnerships with pure-play Orchestration vendors
- There is an ongoing debate about the optimal level of automation in IR. Certain vendors seek to automate the response to Tier 1 and certain Tier 2 alerts, while codifying workflows and/or writing scripts to guide analysts in responding to more complex events; other vendors favor a fully automated approach for remediating even the most complex Tier 3 alerts
- Automated IR is still relatively early on the customer adoption curve, and workflows and scripts that empower rather than disintermediate human analysts can help build customer confidence and drive early uptake. More heavily automated solutions can build confidence by offering semi-automated functionality and show increasing promise as they demonstrate their ability to remediate complex events
- Unifying the workflow, scripting tool, and automation approaches is a focus on analyzing *all* alerts rather than attempting to *prioritize* a select few for analysis while simultaneously freeing analysts to work on more complex and interesting tasks. In this sense, orchestration and automation platforms differ from threat hunting tools that seek to empower analysts by prioritizing the most critical threats to address
- IR is the most developed Orchestration and Automation use case today, but other use cases are beginning to emerge across organizations including vulnerability scanning, network access control, system provisioning, penetration testing, and patch management. Forward-leaning organizations are also recognizing value from Orchestration and Automation tools beyond the security silo and into their broader IT environments (e.g. tools enable Exchange teams to identify and remediate suspect emails in seconds versus hours)

Incident Response Data Funnel

Source: 451 Research

Security Orchestration & Automation Market Drivers

The market is emphasizing solutions that orchestrate and automate the security workflow and reduce attacker dwell time

- **Critical need to orchestrate and automate what historically has been a manual, static process prone to human error, alert fatigue, and weak product integration**
  - Replace with machine-speed decision-making and response
- **Combination of technology, intelligence and expertise delivers capabilities that span the entire security operations lifecycle including assessing, preparing for, detecting, preventing, analyzing, and responding to threats**
  - Capabilities allow organizations to shift from a reactive state of constant busy work to proactive security
- **The constraints of legacy SIEM installations with pricing policies based upon data volume in an era of "big data" are also driving demand**
  - Customers are seeking price-efficient platforms for handling lots of data to triage incidents; legacy SIEMs are proving too expensive and ill-equipped to handle this emerging use case
- **Automation is starting to go beyond prevention and detection technologies, reaching into other important components of IT infrastructure to protect organizations more reliably**
  - Policy execution; alert monitoring and prioritization; incident response planning; investigation, action, and remediation
- **While orchestration and automation platforms are still in the relatively early stages of market penetration, customer interest has been robust**
  - Drivers include skills shortages, manual and complex workflows, massive data volumes, low product interoperability, and an unsustainable spending trend
  - One recent survey showed nearly 75% of respondents had already taken steps to automate and/or orchestrate their incident response processes or planned to in the next 12-18 months and more than 90% planned to increase spending on incident response tools and platforms over the next 2 years

Vendor and customer motivation abounds: clear need to orchestrate security processes with tech-driven capabilities to sharpen the focus of SOC and incident response personnel

Sources: Enterprise Strategy Group, Enterprise Management Associates

Security Orchestration Segment is Primed for Disruption

The security orchestration segment is forecasted to grow from $826M in 2016 to $1.7B by 2021, a 15.3% CAGR

- Nearly 80% of surveyed companies believe that orchestration / automation tools would enable them to investigate more alerts
- Network forensics is anticipated to be a key contributor of growth from 2016 to 2021, as more and more companies are adopting network forensics solutions to drive accurate and efficient remediation
- Adjacent markets include threat intelligence, vulnerability management, incident and event management, security analytics, and managed security

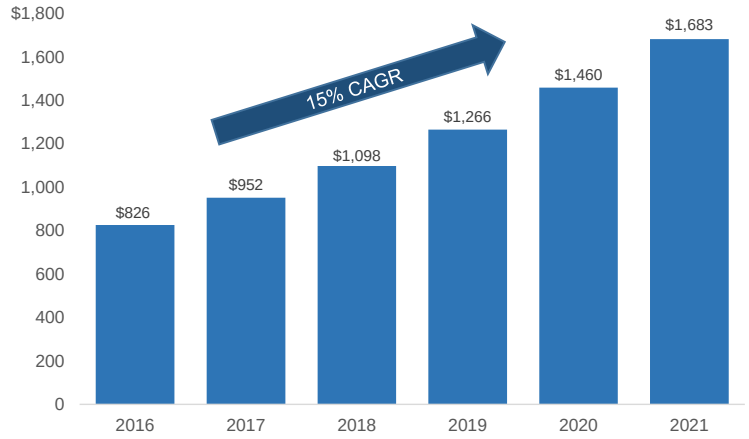
Verticals

- Government vertical is projected to grow at the highest CAGR from 2016 to 2021, as government agencies hold critical and sensitive information of citizens
- BFSI vertical is anticipated to contribute the largest market share, due to the increase in online banking transactions for business via web and mobile devices

Geography

- North America is anticipated to have the largest market share, due to the presence of large number of security orchestration vendors across this region
- APAC offers potential growth opportunities and today represents a largely greenfield opportunity

Security Orchestration Market: 2016-2021



Adjacent Markets (2018 Size in $B)

Sources: MarketsandMarkets, Enterprise Strategy Group, Gartner, Infonetics, NSS, IDC, M&M

Immediate Value Applied to Organizations

Elevating and unifying security management at a system-wide level has enabled:

- **Greater operational efficiencies**
  - Disparate security tools are integrated and sharing information, enhancing security across the board while reducing the need for manual oversight and intervention
  - Group collaboration supporting tiered operations
- **Accelerated threat response**
  - Integration enables automation of basic tasks and threat mitigation while providing the incident response team with real-time information on threats that must be analyzed and neutralized
- **Higher-security, immediate ROI**
  - The whole is much greater than the sum of its parts
  - By taking security tools out of silos and plugging them into a highly intelligent and unified central system that can automate threat mitigation and policy compliance to a large extent, organizations get much more value out of their existing security tools and a rapid return on investment (ROI)
  - Incident response team is kept highly informed in real-time
- **A much-improved network security and compliance posture**
  - Integration provides the ability to automate and enforce policies: ensure that the right users and systems are appropriately accessing the right resources
  - By unifying security management, organizations can automatically identify policy violations, remediate endpoint deficiencies, and measure adherence to compliance mandates

Measuring ROI of Security Orchestration & Automation:

Before orchestration & automation:

- Number of alerts
- Analysts and costs (recruiting, training, bonuses)
- Analyst capacity

Cost to investigate all alerts = total analyst cost / % of alerts investigated

After orchestration & automation:

- Automation cost: charge per seat, per investigation, # of endpoints covered, etc.
- Use XX% of cost it would take to hire enough analysts to cover 100% of all alerts

Sources: CyberSponse, Hexadite, ForeScout

Landscape Evolution (Grouped by Capital Raised)

	Pure Play Orchestration & IR Automation	Adjacent Technologies
Public	FireEye, INVOTAS, IBM Resilient, ServiceNow, proofpoint, NETCITADEL	paloalto NETWORKS, LIGHTCYBER, Hewlett Packard Enterprise, niara, CISCO
Private $50M+	SECURONIX*, LogRhythm, exabeam	DARKTRACE, VECTRA, FIREMON, SKYBOX SECURITY, PROTECTWISE, ForeScout
Private $20-50M	Phantom, DEMISTO, THREATCONNECT	kenna, BLUVECTOR, tufin, Bay Dynamics, R-sam, Intsights (Detect. Analyze. Remediate.)
Private $10-20M	SECDO, HEXADITE, SIEMPLIFY	RISKSENSE, SafeBreach, VERODIN, LIEBERMANSOFTWARE*, sqrrl
Private <$10M	CYBERSPONSE (ADAPTIVE SECURITY), SYNCURITY, UPLEVEL, ayehu, DFLABS, swimlane, fast orientation, seceon, SECBI, DARKLIGHT	panaseer, cyber OBSERVER, ATTACKIQ, patternex, NOPSEC, Efflux Systems, algosec, packetsled, LogicHub

*Bootstrapped but generating significant revenue

Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

DISCLAIMER: This is only a representative list and may not include all relevant companies. If your company is not on the list and would like to be considered for future publications, please shoot us a note at edavis@agcpartners.com and we would be happy to consider adding.

Landscape Evolution (Cont'd)

Network Visibility / Threat Hunting

paloalto NETWORKS
LIGHTCYBER
packetsled
Hewlett Packard Enterprise
niara
LogicHub
VECTRA
patternex
DARKTRACE
BLUVECTOR
PROTECTWISE
sqrrl
Efflux Systems

GRC

R-sam

Identity

LIEBERMANSOFTWARE

Pure Play Security Orchestration & Automation

FireEye
INVOTAS
IBM Resilient
proofpoint
NETCITADEL
Phantom
DEMISTO
SECDO
HEXADITE
seceon
DFLABS
SECBI
servicenow
CYBERSPONSE ADAPTIVE SECURITY
ayehu
UPLEVEL
THREATCONNECT

Next-gen SIEM

LogRhythm
exabeam
SECURONIX

swimlane
SYNCURITY
DARKLIGHT
SIEMPLIFY
fast orientation

Vulnerability & Ecosystem Intelligence

kenna
Bay Dynamics
cyber OBSERVER
Intsights
Detect. Analyze. Remediate.
NOPSEC
ATTACKIQ
RISKSENSE
panaseer
VERODIN
SafeBreach

Network Security / Firewall Policy Orchestration

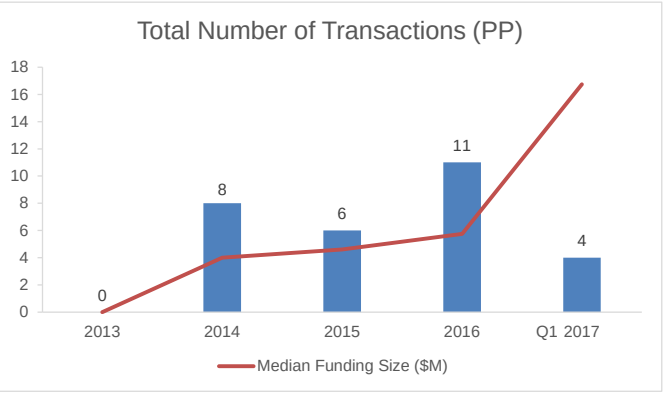
tufin
algosec
SKYBOX SECURITY
ForeScout
FIREMON

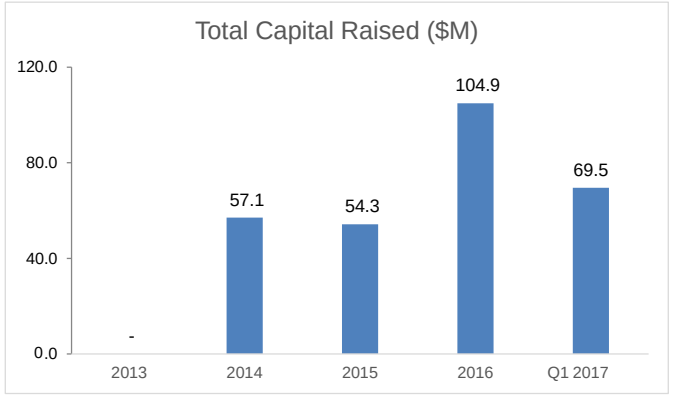
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

DISCLAIMER: This is only a representative list and may not include all relevant companies. If your company is not on the list and would like to be considered for future publications, please shoot us a note at edavis@agcpartners.com and we would be happy to consider adding.

Summary Transaction Activity

Private Placements





M&A Transactions

FireEye

Acquires

INVOTAS

February 2016

IBM

Acquires

resilient SYSTEMS

February 2016

Highlights & Key Takeaways

- **Orchestration and Automation Private Placement activity continues to grow YoY, despite a slowdown in the broader security financing market**
  - Median funding size and total capital raised have increased YoY over the past 2 years
  - Capital raised in 1Q'17 surpassed annual totals for 2013-2015 and is tracking well above FY 2016's pace

- **M&A**
  - Only been two acquisitions directly in the security orchestration and automation segment thus far, FireEye's acquisition of Invotas and IBM's acquisition of Resilient Systems; Proofpoint also acquired NetCitadel in May 2014 to enhance its incident response capabilities
  - May see further consolidation as the demand for breaking down silos of insight and barriers to effective action continues

Sources: 451 Research, Crunchbase, Capital IQ, Company Press Releases

Case Study: IBM Acquires Resilient

Acquisition Details

Announced ---------- February 29, 2016

Enterprise Value ---------- $145M

Acquirer ----------

Target ----------

IBM

Provides IT services, software and hardware for businesses and consumers globally; services include systems integration and network integration, application hosting and management, IT consulting and tech support; software includes information, data and infrastructure management and business intelligence (BI)

Resilient SYSTEMS

Provides cybersecurity incident response management SaaS that enables enterprise security teams to automate, orchestrate, analyze and mitigate IT security incidents such as malware and DDoS attacks

Deal Rationale

"At the intersection of the active and growing domains of security analytics and automation, we see a trend that satisfies **the need to tame unruly and often overwhelming data and turn it into actionable data.** That trend is shaping up around a concept we call the 'actionable situational awareness platform' (ASAP), in which internal monitoring/assessment and external intelligence are synthesized to **deliver a more immediate and useful experience for human analysts, and to close visibility and action gaps – channeled directly into automation where possible, to streamline operations and response**. The combination of IBM's QRadar, which plays a significant role in the SIEM market, with Resilient Systems' response automation platform, is a key manifestation of that trend, following closely on the heels of FireEye's recent acquisition of Resilient competitor Invotas. We expect further consolidations in pursuit of the ASAP concept as the **demand for breaking down silos of insight and barriers to effective action continues**." *Source: 451 Research, 3/1/16*

Sources: 451 Research, Company Press Release

Case Study: FireEye Acquires Invotas

Acquisition Details

Announced	February 1, 2016
Enterprise Value	$20M

Acquirer

FireEye

Provides virtual-machine-based anti-malware appliances for Web, email and file security globally for enterprises and government agencies. Also operates a subscription-based malware and threat identification directory that is generated from threats identified by its anti-malware appliances

Target

INVOTAS

Provided automated threat response, or unified threat management, software and SaaS for use by network security teams in the government, finance, military, energy, healthcare and retail sectors

Deal Rationale

"This deal could serve to **wake up the security industry to the possibilities created by automating most aspects of security operations and IR work**. It not only rounds out FireEye's offerings but also **creates the opportunity to connect and orchestrate each of its products in ways that aren't possible today**. This isn't just another product for FireEye to add to its lineup: Invotas is the **glue the company needs to integrate on a new level with its existing security products already sitting in datacenters**." *Source: 451 Research, 2/3/16*

"'The addition of Invotas' technology enables us to enhance our global threat management platform and advance ongoing efforts to provide our customers with a **centralized method to manage alerts and intelligence and then automate actions** based on FireEye-built playbooks or their own custom strategies." *Source: Acquirer press release, 2/1/16*

Sources: 451 Research, Company Press Release

Strong Buyer-Base for Security Orchestration & Automation Companies

- A fast-growing security orchestration and automation market can attract both the large strategic technology buyers as well as major buyout firms
- Striking premium revenue multiples anticipated – exemplified by the 14.5x revenue in the case of IBM buying Resilient Systems for $145M; reports have placed Resilient's quarterly revenue at $30-50M vs. $10M TTM when acquired one year ago, demonstrating ability to add value and scale in a broader security stack
- Even though the leading standalone orchestration and automation players are likely too small at present to serve as PE platforms, the vendors exhibit many qualities of future platform plays including fast growth, subscription revenue models, and ability to add scale through add-on acquisitions in highly complementary segments (e.g. threat intel, sandbox, data analytics, network visualization)
- Standalone orchestration and automation vendors are beginning to incorporate one another's capabilities to enhance their platform value proposition to customers and share of the security budget
- Standalone vs. consolidation activity will be driven in part by a discussion around the optimal model for adding value in customer environments: "Switzerland" (i.e. ingesting information from the broad vendor universe) vs. the engine driving efficiencies primarily (though not exclusively) within a single-vendor environment

Potential Strategic Buyers

FireEye, Rapid7, RSA, tenable, IBM, ServiceNow, Symantec, Trend Micro, Trustwave, splunk>, Cisco, Hewlett Packard Enterprise, paloalto networks, SecureWorks, CA technologies, NTT Security, McAfee, SOPHOS

Private Equity Buyout Firms

KKR, Thoma Bravo, ClearLake Capital, LLR partners, JMI Equity, Vista Equity Partners, Marlin Equity Partners, The Blackstone Group, TPG, BainCapital, FP Francisco Partners, Warburg Pincus, Summit Partners

Sources: Capital IQ, 451 Research

DISCLAIMER: This is only a representative list and may not include all relevant companies. If your company is not on the list and would like to be considered for future publications, please shoot us a note at edavis@agcpartners.com and we would be happy to consider adding.

The Future for Orchestration & Automation: Standalone or Consolidation?

STANDALONE

- ✓ "Switzerland" of incident response
- ✓ Ingest information from multiple sources and provide value across diverse, multi-tool ecosystem

- ✗ Need to capture new budget dollars
- ✗ Building scale is challenging and expensive
- ✗ Need to develop/acquire machine learning, behavioral analytics, threat hunting, IR, AI, etc. to capture market share as a platform security tool

vs.

CONSOLIDATION

- ✓ Leverage embedded tools and sell to installed customer base
- ✓ Quickly get to scale
- ✓ Proven successful platforms built around orchestration / automation companies – core part of parent's strategy

- ✗ Prioritizing insights from the parent's ecosystem may hinder "best-of-breed" multiplier functionality and messaging

Source: 451 Research

Top Funded Pure Play Security Orchestration & Automation Companies

Company	Headquarters	Total Funding	Year Founded
LogRhythm	Boulder, CO	$125M*	2003
exabeam	San Mateo, CA	$65M	2013
DEMISTO	Cupertino, CA	$26M	2015
Phantom	Palo Alto, CA	$25M	2014
SIEMPLIFY	New York, NY	$14M	2015
HEXADITE	Boston, MA	$11M	2014
SECDO	New York, NY	$10M	2014
DFLABS	Milano, Italy	$6M	2003
CYBERSPONSE ADAPTIVE SECURITY	Arlington, VA	$6M	2011
swimlane	Louisville, CO	$6M	2014

- The pure-play orchestration and automation companies have been lightly capitalized as a whole, particularly relative to more established segments like EDR and EPP
- The majority of pure-play orchestration and automation companies were founded in the past 2-3 years
- The segment's two highest-funded vendors, LogRhythm and Exabeam, are next-gen SIEM providers that now offer native orchestration and automation capabilities, and are increasingly competing head-to-head against the pure-play orchestration and automation vendors
- 9 of the top 10 funded companies are located in the U.S., though many have Israeli pedigree

**Includes $10M debt raised in last round (E-1)*
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

Conclusion

- Security orchestration rescues complex, reactive processes; automating security processes is increasingly a “need to have”
- Security orchestration does not require you to discard your current tools but instead weaves in an orchestration layer to connect the dots among the tools and better inform SOCs in the event of an incident
- Further M&A activity is likely in the near future, but only time will tell whether these orchestration startups become consolidated or grow into standalone platforms
- The most successful orchestration and automation vendors will demonstrate 451 Research’s concept of ASAP while also offering robust out-of-box integration with SOC technologies including detection, threat intelligence, and investigative systems

2017 Private Placement Activity

($US in millions)

Date Announced	Target Name	Largest Investor(s)	Target Description	Amount	Round
03/09/2017	RiskSense	Jump Capital, Paladin Capital Group, Sun Mountain Capital, EPIC Ventures, CenturyLink	Provides pro-active cyber risk management SaaS	$14.0	A
02/13/2017	Intsights	Blackstone, Blumberg Capital, Glilot Capital Partners, Vintage Investment Partners, Wipro Ventures	Provides an automated system that detects, analyzes, and remediates threats in real time, in the dark, deep and open web	15.0	B
02/09/2017	Demisto	ClearSky Security, Accel Partners, Slack Fund	Provides a Bot-powered Security ChatOps platform that combines intelligent automation with collaboration	20.0	B
02/07/2017	Exabeam	Cisco Investments, Lightspeed Venture Partners, Aspect Ventures, Icon Ventures, Norwest Venture Partners, Shlomo Kramer	Provides a security intelligence platform that combines data collection, machine learning for advanced analytics, and automated incident response	30.0	C
02/01/2017	LogicHub	Storm Ventures, Nexus Venture Partners	Provides a security intelligence automation platform that captures and automates security analysts' intelligence, knowledge and expertise to prioritize threats more effectively	8.4	A
01/18/2017	ProtectWise	Arsenal Venture Partners, Tola Capital, Top Tier Capital Partners	Delivers pervasive visibility, automated threat detection and unlimited forensic exploration on-demand and entirely from the cloud	25.0	B
01/10/2017	Phantom	KPCB, TechOperators, Blackstone, Foundation Capital, In-Q-Tel, Rein Capital, Zach Nelson, John Thompson	Provides a community-powered security automation and orchestration platform	13.5	B
01/05/2017	Swimlane	ND	Provides a security operations management platform that centralizes an organization's security alerts, automates resolution, and dynamically produces metrics-based dashboards and reports	6.0	A
			2017 Median:	**$14.5**	

Notes: Gray shading represents private placements for pure play orchestration and automation companies
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

2016 Private Placement Activity

($US in millions)

Date Announced	Target Name	Largest Investor(s)	Target Description	Amount	Round
12/07/2016	Kenna Security	PeakSpan Capital, OurCrowd, USVP, Costanoa Venture Capital, Hyde Park Angels	Provides a vulnerability and risk intelligence platform the enables organizations to measure and monitor their exposure to risk	$15.0	B
12/06/2016	SECDO	Rafael Development, Marius Nacht	Provides a preemptive incident response platform that combines automated alert validation, contextual investigation, threat hunting and rapid remediation	10.0	A
11/30/2016	AttackIQ	Index Ventures, Qualcomm Ventures, Telstra Ventures	Provides an automated security platform that helps organizations test, measure and perform security validation and improve their defense in depth strategy	8.8	A
11/15/2016	Siemplify	83North, G20 Ventures, Alex Daly, Dave Strohm	Provides a security operations platform that unifies the diverse security tools used in organizations	10.0	A
10/25/2016	Uplevel Security	First Round Capital, Aspect Ventures	Provides an automated, intelligence-driven incident analysis and response platform	2.5	Seed
09/27/2016	SecBi	Jerusalem Venture Partners, Orange Digital Ventures, Connecticut Innovations, Amichai Shulman	Provides an adaptive investigation platform that combines advanced machine learning capabilities, cybersecurity expertise, and user feedback	5.0	A
08/30/2016	LogRhythm	Riverwood Capital, Adams Street Partners, Siemens Venture Capital, Delta-v Capital, EDBI, Exclusive Ventures, Silver Lake Waterman	Provides security intelligence and analytics, empowering organizations to rapidly detect, respond to and neutralize damaging cyber threats	50.0	E-1
08/30/2016	IntSights	Blumberg Capital, Blackstone, Glilot Capital Partners, Wipro Ventures	Provides an automated system that detects, analyzes, and remediates threats in real time, in the dark, deep and open web	7.5	A
08/01/2016	Syncurity	Tim Sullivan, Tim Webb	Provides an agile incident response platform that streamlines security operations by force multiplying people, process, and technology in a virtual SOC to drive better security outcomes	ND	ND
07/28/2016	PacketSled	Keshif Ventures, Blu Ventures, JHS Ventures	Automates incident response by fusing business context, AI, entity enrichment and detection with network visibility	5.0	A
07/26/2016	PatternEx	Khosla Ventures	Provides a threat prediction platform that combines artificial intelligence and analyst intuition	7.8	A
07/26/2016	SafeBreach	Deutsche Telekom Capital Partners, Hewlett Packard Pathfinder, Maverick Ventures, Sequoia Capital, Shlomo Kramer	Simulates hacker behavior, allowing organizations to see the impact from a breach before it occurs	15.0	A
07/13/2016	Bay Dynamics	Carrick Capital Partners, Comcast Ventures	Provides a cyber risk analytics platform that helps companies measure, communicate and reduce cyber risk	23.0	B
07/05/2016	Darktrace	KKR, Summit Partners, Ten Eleven Ventures, SoftBank Capital	Provides AI algorithms that mimic the human immune system to defend enterprise networks	65.0	C

Notes: Gray shading represents private placements for pure play orchestration and automation companies
**Includes $10M debt from Silver Lake*
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

2016 Private Placement Activity (Cont'd)

($US in millions)

Date Announced	Target Name	Largest Investor(s)	Target Description	Amount	Round
06/28/2016	Verodin	Cisco Investments, Rally Ventures, Crosslink Capital, Blackstone	Empowers customers to measure and continuously validate the cumulative effectiveness of layered security infrastructures	$10.0	A
06/22/2016	LightCyber	Access Industries (Claltech), Battery Ventures, Glilot Capital Partners, Amplify Partners, Vertex Ventures, Shlomo Kramer	Provides behavior-based profiling SaaS, enabling breach-detection and visibility into advanced or targeted attacks, insider threats and malware that have circumvented traditional security controls	20.0	B
05/25/2016	Demisto	Accel Partners, Kevin Mahaffey, Michael Fey, Secure Octane, Stuart McClure	Provides a Bot-powered Security ChatOps platform that combines intelligent automation with collaboration	6.0	A
05/04/2016	DFLabs	Evolution Equity Partners	Provides automated incident, breach response, and orchestration security	5.5	A
03/18/2016	Vectra Networks	Wipro Ventures, DAG Ventures, Khosla Ventures, Accel Ventures, IA Ventures, AME Cloud Ventures, Intel Capital, Juniper Networks	Provides real-time attack visibility and non-stop automated threat hunting powered by artificial intelligence	43.8	C
03/07/2016	CyberSponse	ND	Provides automated incident response (IR) solutions for cyber security threat management	3.9	ND
02/18/2016	Siemplify	83North, Dave Strohm, Alex Pinchev, Alex Daly, Tom Kilroy, Moti Gutman	Provides a security operations platform that unifies the diverse security tools used in organizations	4.0	Seed
02/10/2016	Hexadite	Hewlett Packard Ventures, Ten Eleven Ventures, YL Ventures	Provides an agentless intelligent security orchestration and automation platform	8.0	A
02/05/2016	PatternEx	ND	Provides a threat prediction platform that combines artificial intelligence and analyst intuition	2.0	Seed
02/03/2016	Skybox	Providence Equity Partners	Provides enterprise IT security vulnerability assessment, change management and firewall and compliance auditing SaaS	96.0	PE
01/21/2016	ForeScout	Wellington Management	Provides agentless visibility and control of traditional and IoT devices the instant they connect to the network	76.0	G
			2016 Median:	**$9.4**	

Notes: Gray shading represents private placements for pure play orchestration and automation companies
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

2015 Private Placement Activity

($US in millions)

Date Announced	Target Name	Largest Investor(s)	Target Description	Amount	Round
12/15/2015	SECEON	ND	Provides a cyber security advanced threat management platform that visualizes, detects, and eliminates threats in real time	$1.9	ND
12/01/2015	ThreatConnect	SAP, Grotech Ventures	Delivers a Threat Intelligence Platform (TIP) in the cloud or on-premises to effectively aggregate, analyze, and act to counter sophisticated cyber-attacks	16.0	B
11/17/2015	ProtectWise	Tola Capital, Arsenal Ventures Partners, Crosslink Capital, Paladin Capital Group, Trinity Ventures	Delivers pervasive visibility, automated threat detection and unlimited forensic exploration on-demand and entirely from the cloud	20.0	B
11/12/2015	Panaseer	Albion Ventures, Notion Capital, Winton Technology Ventures, C5 Holdings, Elixirr	Provides a data-driven risk management security platform that advances, simplifies, and automates how an organization identifies, measures, communicates and mitigates risk	2.3	Seed
10/13/2015	IntSights	Glilot Capital Partners	Provides an automated system that detects, analyzes, and remediates threats in real time, in the dark, deep and open web	1.8	Seed
09/29/2015	Exabeam	Icon Ventures, Aspect Ventures, Norwest Venture Partners, Shlomo Kramer	Provides a security intelligence platform that combines data collection, machine learning for advanced analytics, and automated incident response	25.0	B
09/28/2015	Phantom	TechOperators, Blackstone, Rein Capital, John Thompson, Zach Nelson	Provides a community-powered security automation and orchestration platform	6.5	A
07/22/2015	Darktrace	Summit Partners	Provides AI algorithms that mimic the human immune system to defend enterprise networks	22.5	B
07/15/2015	Ayehu	Benhamou Global Ventures	Helps IT and Security professionals to identify and resolve critical incidents, simplify workflows and maintain greater control over IT infrastructure through automation	2.2	ND
07/08/2015	SafeBreach	Sequoia Capital, Shlomo Kramer	Simulates hacker behavior, allowing organizations to see the impact from a breach before it occurs	4.0	Seed
06/25/2015	Verodin	ND	Empowers customers to measure and continuously validate the cumulative effectiveness of layered security infrastructures	2.1	Seed
05/31/2015	Cyber Observer	Shaul Shani	Provides a real-time infographic view of the security status, performance and preparedness across security domains, and identifies deviations from predefined thresholds	1.0	Seed
04/14/2015	Phantom	Foundation Capital, Rein Capital, John Thompson, Tom Noonan, Zach Nelson, John Becker	Provides a community-powered security automation and orchestration platform	2.7	Seed
04/09/2015	Niara	Venrock, New Enterprise Associates, Index Ventures	Provides machine learning-enabled behavioral analytics SaaS	20.0	B
03/24/2015	Rsam	JMI Equity	Provides governance, risk and compliance (GRC) solutions	32.0	Venture
03/17/2015	Darktrace	Invoke Capital, Talis Capital, Hoxton Ventures	Provides AI algorithms that mimic the human immune system to defend enterprise networks	18.0	A
02/18/2015	Sqrrl	Rally Ventures, Accomplice, Matrix Partners	Enables organizations to target, hunt, and disrupt advanced cyber threats	7.0	B
			2015 Median:	**$6.5**	

Notes: Gray shading represents private placements for pure play orchestration and automation companies
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

2014 Private Placement Activity

($US in millions)

Date Announced	Target Name	Largest Investor(s)	Target Description	Amount	Round
12/09/2014	Tufin	Vintage Fund, Marker Investment Fund	Provides a security policy orchestration platform that enables enterprises with the ability to streamline the management of security policies across complex, heterogeneous environments	$8.0	ND
11/20/2014	ThreatConnect	Grotech Ventures	Delivers a Threat Intelligence Platform (TIP) in the cloud or on-premises to effectively aggregate, analyze, and act to counter sophisticated cyber-attacks	4.0	A
10/14/2014	Kenna Security	Costanoa Venture Capital, USVP, Tugboat Ventures, Hyde Park Angels	Provides a vulnerability and risk intelligence platform the enables organizations to measure and monitor their exposure to risk	4.0	A
09/10/2014	LightCyber	Battery Ventures, Glilot Capital Partners, Marius Nacht	Provides behavior-based profiling SaaS, enabling breach-detection and visibility into advanced or targeted attacks, insider threats and malware that have circumvented traditional security controls	10.0	A
09/02/2014	Syncurity	MACH37	Provides an agile incident response platform that streamlines security operations by force multiplying people, process, and technology in a virtual SOC to drive better security outcomes	ND	Seed
08/05/2014	Vectra Networks	Accel Partners, Khosla Ventures, IA Ventures, AME Cloud Ventures, Intel Capital, Juniper Networks	Provides real-time attack visibility and non-stop automated threat hunting powered by artificial intelligence	25.0	C
08/01/2014	Champion Technology [dba DarkLight]	ECA Ventures	Provides a cybersecurity analytics and automation platform leveraging artificial intelligence	ND	Seed
07/22/2014	LogRhythm	Riverwood Capital, Adams Street Partners, Access Venture Partners, Piper Jaffray	Provides security intelligence and analytics, empowering organizations to rapidly detect, respond to and neutralize damaging cyber threats	40.0	E
07/15/2014	Bay Dynamics	Comcast Ventures	Provides a cyber risk analytics platform that helps companies measure, communicate and reduce cyber risk	8.0	A
07/01/2014	Hexadite	YL Ventures, Moshe Lichtman	Provides an agentless intelligent security orchestration and automation platform	2.5	Seed
06/10/2014	ProtectWise	Paladin Capital Group, Arsenal Ventures Partners, Crosslink Capital, Trinity Ventures	Delivers pervasive visibility, automated threat detection and unlimited forensic exploration on-demand and entirely from the cloud	14.1	A
06/10/2014	Exabeam	Norwest Venture Partners, Aspect Ventures, Shlomo Kramer	Provides a security intelligence platform that combines data collection, machine learning for advanced analytics, and automated incident response	10.0	A
05/23/2014	CyberSponse	ND	Provides automated incident response (IR) solutions for cyber security threat management	0.6	ND
03/27/2014	Fast Orientation	MACH37	Allows organizations to query, analyze, and respond to enterprise security events in real-time	ND	Seed
01/02/2014	Skybox Security	Susquehanna Investment Group	Provides enterprise IT security vulnerability assessment, change management and firewall and compliance auditing SaaS	6.0	ND
			2014 Median:	**$8.0**	

Notes: Gray shading represents private placements for pure play orchestration and automation companies
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

2013 Private Placement Activity

($US in millions)

Date Announced	Target Name	Largest Investor(s)	Target Description	Amount	Round
12/31/2013	PacketSled	Keshif Ventures	Automates incident response by fusing business context, AI, entity enrichment and detection with network visibility	$3.0	Seed
11/30/2013	Niara	Index Ventures, New Enterprise Associates	Provides machine learning-enabled behavioral analytics SaaS	9.4	A
10/21/2013	Sqrrl	Atlas Venture, Matrix Partners	Enables organizations to target, hunt, and disrupt advanced cyber threats	5.2	A
07/05/2013	Tufin	Marker, MoneyTime Ventures	Provides a security policy orchestration platform that enables enterprises with the ability to streamline the management of security policies across complex, heterogeneous environments	8.8	C
05/03/2013	ProtectWise	Crosslink Capital, Trinity Ventures	Delivers pervasive visibility, automated threat detection and unlimited forensic exploration on-demand and entirely from the cloud	3.1	Seed
			2013 Median:	**$5.2**	

Notes: Gray shading represents private placements for pure play orchestration and automation companies
Sources: Capital IQ, Crunchbase, TechCrunch, Pitchbook, Company Press Releases

AGC's Dedicated Security Orchestration and Automation Team

Eric Davis
Partner

- Eric is a Partner in the investment banking group at AGC Partners. He has over 15 years of experience in the financial services industry focusing on acquisition financing, capital raising, and early-stage equity investing
- Prior to joining AGC as a Principal, Eric was a Vice President in Citigroup's Technology, Media & Telecommunications and Infrastructure & Energy Finance groups
- He also previously worked as a Vice President of Project Finance and Investments at eleQtra, Inc., an emerging markets infrastructure development and investment fund
- Eric holds a MALD with a concentration in International Business from the Fletcher School at Tufts University and a B.A. in Political Science from Middlebury College

Maria Lewis Kussmaul
Co-Founder, Partner

- Maria is a co-founder of AGC Partners and is a Partner in the investment banking group focused on the IT security sector
- Prior to co-founding AGC, Maria was a co-founder, general and venture partner of Castile Ventures, a seed and early stage venture capital firm
- Maria's early Wall Street career spanned three firms – Smith Barney, Shearson Lehman and Cowen & Co., culminating as global head of Cowen's Data Networks & Internet investment banking activities
- Previously, she was named to the Institutional Investor All-American Research Team for 13 consecutive years
- Maria holds a B.A. in Economics from Rutgers University, an M.B.A. from Wharton School of Business and a Chartered Financial Analyst designation

Ben Howe
Co-Founder, CEO

- Ben is a co-founder and the CEO of AGC Partners
- In 26 years as an investment banker, Ben has completed more than 300 transactions
- Prior to AGC, he served as Managing Director, Head of M&A and Executive Committee Member at SG Cowen Securities, and prior to that served as Head of Technology Investment Banking for the East Coast and Europe at Montgomery Securities
- He serves as co-chairman of Excel Academy, which has four charter schools in East Boston, and served on the board of Portsmouth Abbey and the advisory board of Trinity College
- He holds a B.A. in Economics from Trinity College and an M.S. in Accounting from The Stern School of Business at NYU

Russ Workman
Partner

- Russ is a Partner in the investment banking group at AGC Partners focused on IT security and defense technologies
- Before joining AGC, Russ began his investment banking career in the technology banking group at Jefferies & Co. and has advised on more than 50 completed strategic advisory and capital raising assignments
- Before banking, Russ was a US Air Force Officer managing the acquisition of intelligence and information warfare systems for the Intelligence Community, and performed cyber vulnerability assessments of Air Force electronic systems
- Russ holds an M.B.A. in Finance and Accounting from the Wharton School of Business, an M.S. in Operation Research from Northeastern University, and a B.S. in Operations Research from the US Air Force Academy

Ranked the Top Technology Boutique Bank

- M&A and Growth Equity focus – Enterprise value between $50M and $350M
- Reputation for closing deals large and small at premium valuations
- A record 32 announced transactions in 2016 with buyers from around the world including Microsoft, Oracle, HPE, Rakuten and Carlyle, and more than 45 current engagements
- High transaction volume fuels deep market knowledge and extensive worldwide technology contacts
- One of the largest tech banking teams in the world with 50 employees
- 14 years in business, 302 completed transactions, and 52 consecutive quarters of profitability
- Headquartered in Boston with offices in Silicon Valley, New York, London, and Minneapolis

Tech M&A Banking Review Top 2016 Dealmakers

451 Research

TECHNOLOGY

	Firm	# Trans.
1.	Morgan Stanley	45
2.	William Blair & Co	30
3.	J.P. Morgan Securities Inc.	29
4.	Goldman Sachs	27
5	Evercore Partners	23
6.	**AGC Partners**	**22**
7.	Houlihan Lokey	22
8.	Raymond James	22
9.	GCA Altium	20
10.	BOA Merrill Lynch	17
11.	Jefferies	17
12.	Qatalyst Partners	16
13.	Arma Partners	15
14.	Petsky Prunier	15
15.	Pacific Crest Securities	13
16.	Pagemill Duff & Phelps	13
17.	Robert W. Baird & Co.	12
18.	JEGI	12
19.	Signal Hill	12
20.	Credit Suisse Securities	11

SECURITY

	Firm	# Trans.
1.	**AGC Partners**	**7**
2.	Morgan Stanley	7
3.	Goldman Sachs	4
4.	Jefferies	3
5.	Mooreland Partners	2
6.	RBC Capital Markets	2
7.	Aelios Finance	1
8.	Atlas Technology Group	1
9.	BOA Merrill Lynch	1
10.	Barclays Capital	1
11.	Boston Meridian	1
12.	Bridge Street Advisors	1
13.	Bryan, Garnier & Co	1
14.	Citigroup Global Markets	1
15.	Clearsight Advisors	1

AGC's Recent Security Transactions: 91 Deals Since Inception

2016

2015

2014

2013

2012

Denotes transactions with valuations greater than $100M

Security Market Experts – Thought Piece Leadership

Utilizing in-depth domain expertise, AGC Partners regularly publishes sector “Thought Pieces” covering key trends in information security and other tech sectors

2013-2017 Published Security Thought Pieces

- Cyber Risk Insurance
- Next-Gen Security Endpoint Security
- Connected Car Security
- The State of Healthcare Information Security
- Drones: The High Flying Growth of UAVs
- Defense Intelligence: The Rise of Cyber
- Critical Infrastructure Cyber Security Market Overview

2017 West Coast Information Security Conference

AGC Partners hosted its 13th Annual Information Security Conference in San Francisco, CA on February 13th, 2017, featuring 350+ senior executives from leading public and private information security companies globally. Keynote speakers included Niloo Howe (SVP, Strategy & Operations, Chief Strategy Officer, RSA), Patrick Morley (Chief Executive Officer, Carbon Black), Doug Song (Chief Executive Officer, Duo Security), and Oliver Friedrichs (Chief Executive Officer, Phantom).

Keynote Speakers

RSA · Carbon Black · Duo · Phantom

Industry Panel Topics & Participants

Active Defense

AGC Partners · TRAPX Security · Recorded Future · SecureWorks · CrowdStrike · illusive

AI in Cyber Security

Check Point Software Technologies Ltd. · JASK · Intsights · Microsoft · DarkTrace · deepinstinct

Next Gen Endpoint

NSS Labs · Carbon Black · Trend Micro · cybereason · CounterTack · SentinelOne

Cyber Risk Assessment

Stroz Friedberg · cyber GRX · Focal Point Data Risk · Deloitte · riskrecon · Coalfire

Directions in Enterprise Security

Securosis · IBM · RSA · proofpoint · tenable · Cisco

Disruptors in Security

451 Research · Akamai · Transmit Security · Duo · TechOperators Venture Capital · Cylance

Impact of DevOps

Atlantic Council · AttackIQ · BlackDuck · kenna · Twistlock · SignalSciences

Investing in Cyber Security

AGC Partners · Sunstone Partners · Sophos · Allegis Capital · Index Ventures · proofpoint

Security Automation

AGC Partners · R-sam · FireEye · Phantom · Demisto · ProtectWise

What Clients Say About Us

"Maria, Eric and the AGC team were great partners for us to collaborate with in this process. We benefited greatly from their market knowledge, relationships and outstanding ability to drive the process toward a successful conclusion. I look forward to continuing to collaborate with Maria and the AGC team as we move into the future."

— **Lars Harvey, CEO of IID Security**
(AGC acted as sole financial advisor to IID Security)

"It was such a great experience working through a successful process with the entire AGC team: Maria, Eric, Alex, and Hanna. It was because of AGC's security sector knowledge, relationships, and market leadership position that our entire transaction experience from start to end was a success. I am very excited about the future of APTEC with our new parent company Cyber Risk Management."

— **Aaron Perry, President & Founder of APTEC**
(AGC acted as sole financial advisor to APTEC)

"We were very pleased with the work of Maria, Eric, and the AGC team. Their deep sector knowledge, extensive industry relationships, and hard work guided us to a successful close with an excellent strategic partner. I look forward to working with them again in the future."

— **Mark Hatton, President and CEO of Core Security**
(AGC acted as sole financial advisor to Core Security)

"AGC did a fantastic job advising Xceedium during the M&A process. The management team, Board, and shareholders were all thoroughly impressed by Maria's deep industry knowledge and close relationships with the major security players. The entire AGC team served as a trusted advisor and helped make this transaction a success. We look forward to working with Maria and her team again in the future."

— **Glenn Hazard, CEO, Xceedium**
(AGC acted as sole financial advisor to Xceedium Utilities)

What Clients Say About Us (Cont'd)

"AGC did a fantastic job advising Prolexic during the financing process. The management team, Board, and shareholders were thoroughly impressed by Maria and Russ' deep industry knowledge and close relationships with the major security and private-equity players. The AGC team served as a trusted advisor throughout and we look forward to working with Maria and her team again in the future"

— **Scott Hammack, CEO of Prolexic**
(AGC acted as sole financial advisor to Prolexic)

"Maria and her team at AGC served as BreakingPoint's trusted advisor through a comprehensive and highly efficient process that culminated with the successful sale to Ixia. Through every step of the way, including complex final negotiations, AGC led BreakingPoint with professionalism and a deep commitment to our shareholders. My team and our investors couldn't be more pleased with the results, and we look forward to working with AGC again in the future."

— **Des Wilson, CEO of BreakingPoint**
(AGC acted as sole financial advisor to BreakingPoint)

"Maria and her team at AGC provided invaluable guidance throughout a complex process to deliver a great result for Fidelis' shareholders and employees. I look forward to working with Maria and the AGC team again in the future."

— **Peter George, President and CEO of Fidelis**
(AGC acted as sole financial advisor to Fidelis)

"Maria and the AGC team did an outstanding job in advising us throughout this process. We built a great company and weren't looking to sell, but when the opportunity presented itself Maria and her team jumped into gear. AGC's ability to run an efficient process in a narrow timeframe ultimately ensured that Dasient's shareholders received the best possible outcome. We are thrilled with the results of the transaction, and I look forward to continuing my relationship with Maria and the AGC team."

— **Paul Stich, CEO of Dasient**
(AGC acted as sole financial advisor to Dasient)