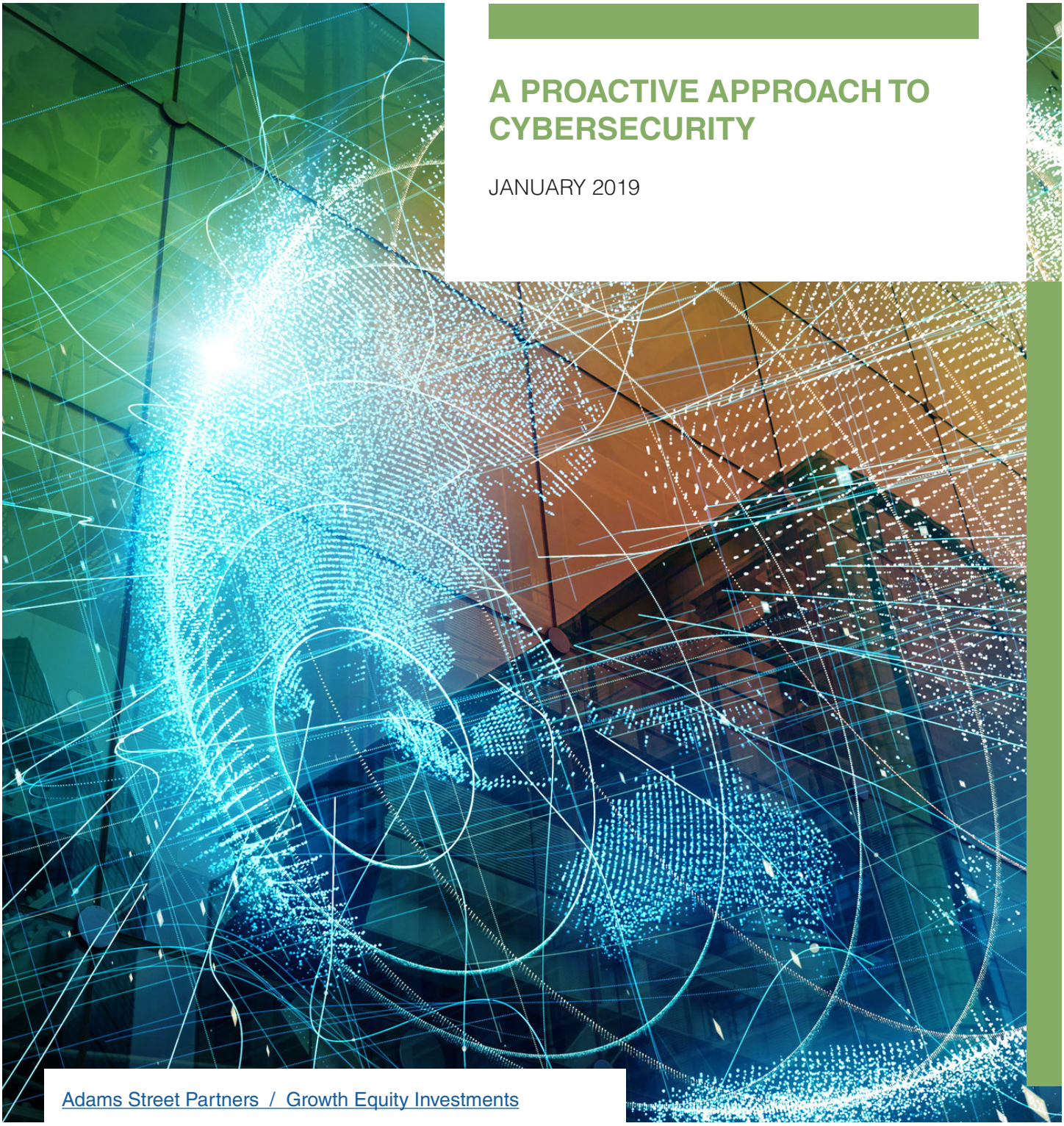
ADAMS STREET
PARTNERS

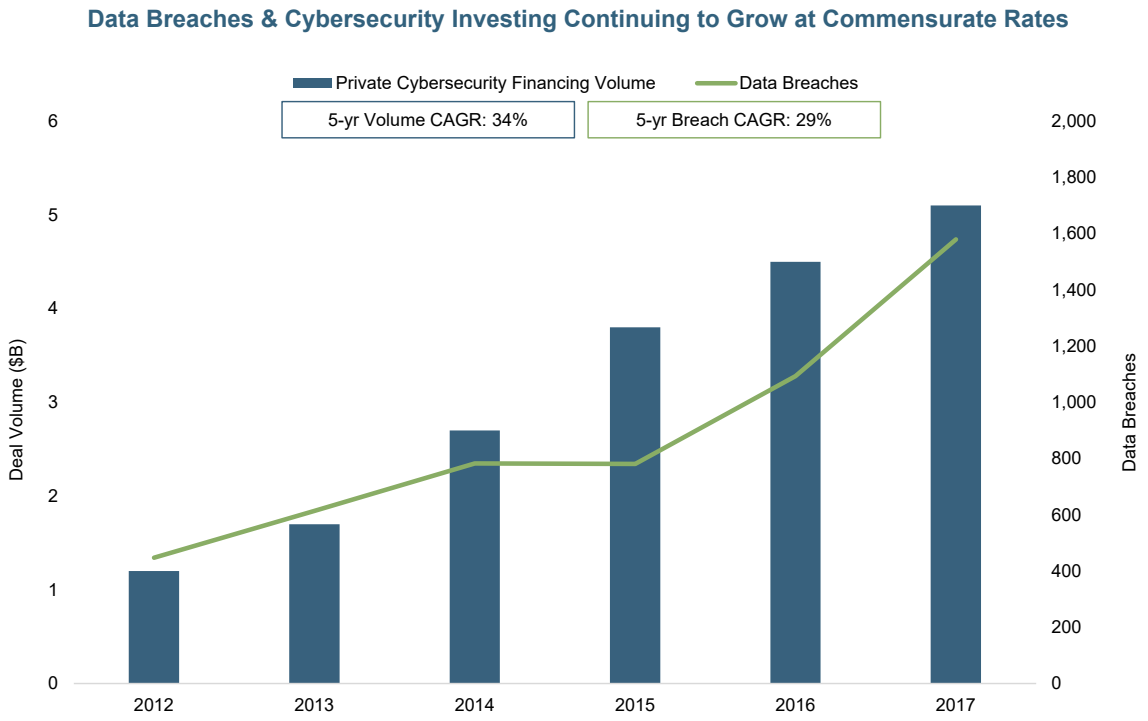


A PROACTIVE APPROACH TO CYBERSECURITY

JANUARY 2019

Adams Street Partners / Growth Equity Investments

2018 marked yet another banner year for the cybersecurity industry. Private financings, public stock appetite, and M&A interest in cyber technologies have all remained robust due to the increases in costly – and often very public – data breaches and other cyber attacks.



Source: "Cybersecurity Almanac" January 2018, Momentum Cyber.

At Adams Street, we've seen the increase in appetite for scaled security companies, as we have had four liquidity events in our existing security companies in the past year alone. At the same time, we are active in pursuing new opportunities, making four new cybersecurity investments in the past year as well.

As investors, one of the most significant macro-trends we've seen unfold throughout the industry is a shift from a "prevent and react" approach to a more proactive strategy that prioritizes visibility and intelligence, as well as active defense, detection, and response capabilities. It's a transition that has been going on for some time and has influenced a significant portion of our cybersecurity investment thesis. Here's how we're seeing organizations implement a proactive security framework and a highlight of some of our portfolio companies that are helping them:

Know (and Protect) Your Gaps

Knowledge is power, and this holds especially true for cybersecurity. Organizations struggle with the lack of visibility and control over the various attack vectors coming at them. Every organization has a unique threat profile. Industry threat profiles from Verizon's 2018 data breach report demonstrate how the threats posed to a healthcare company are drastically different from those posed to a financial services or retail firm.

Financial	
Who	79% external, 19% internal
What	36% personal, 34% payment, 13% bank
How	34% hacking, 34% physical

Healthcare	
Who	43% external, 56% internal
What	79% medical, 37% personal, 4% payment
How	35% error, 24% misuse

Retail	
Who	91% external, 10% internal
What	73% payment, 16% personal, 8% credentials
How	46% hacking, 40% physical

Information	
Who	74% external, 23% internal
What	56% medical, 41% credentials, 9% internal
How	57% hacking, 26% error

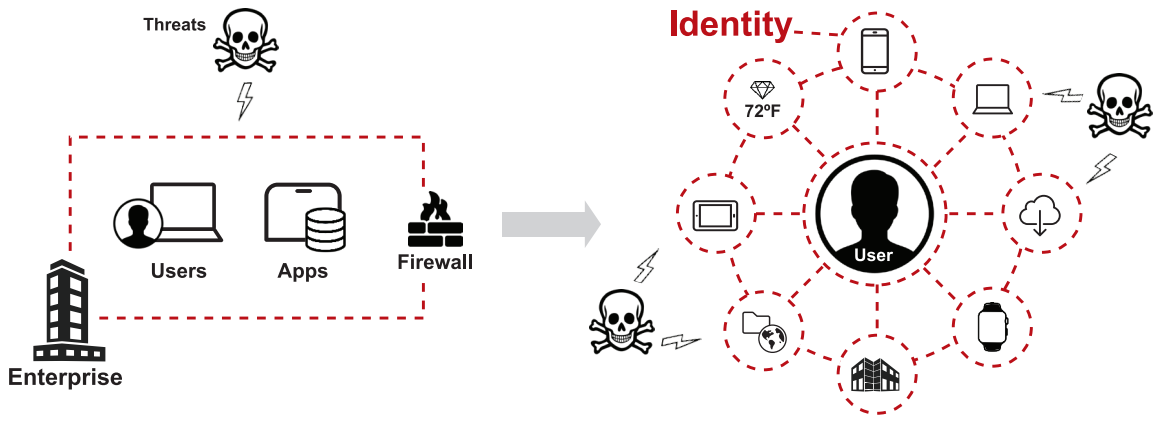
Source: "2018 Data Breach Investigations Report" March 2018, Verizon

There isn't a "one size fits all" solution for every organization; organizations with extremely sensitive data will naturally be more susceptible to insider threats and data exfiltration, while companies with a significant web presence will face greater threats from botnets and account takeover attacks. However, companies of all shapes and sizes can invest in technologies that highlight where they face critical vulnerabilities. Automated penetration testing, vulnerability management solutions such as SkyBox Security, and third-party risk management technologies are all great examples of solutions that bring significant value, filling in knowledge gaps throughout organizations.

Focus on Identity as a Vector for Attacks

One area that every organization needs to invest in is identity. Digital transformation has continued to push zero-trust security frameworks to the forefront of enterprise security strategies. At the heart of any zero-trust strategy is the ability to identify and authenticate users. We saw the beginning of this movement years ago when we invested in TeleSign (acquired by BICS last year), who provided some of the first two-factor authentication programs for many of today's leading internet brands, and ThreatMetrix (acquired last year by RELX group), who was a pioneer in establishing digital identities and created a global network of 1.4 billion known identities.

Identity is the New Perimeter



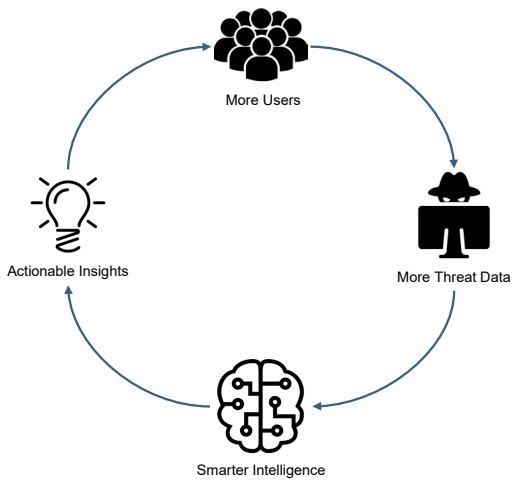
Source: "Best Practices for Improving Enterprise Security With Identity" Feb 2017, Ping Identity

We are also seeing organizations fortify their perimeters with identity features. The reason for this adoption of an identity-as-a-perimeter security strategy is that hackers continue to have significant success in using stolen credentials to execute attacks. 81% of breaches are due to stolen credentials[1], which has continued to fuel the rise in two different attack types that aim to steal credentials: phishing and botnet-based account takeovers. Phishing attacks are specific, targeted attacks that are socially-engineered to entice employees to disclose credentials, while botnet-based account takeovers are brute-force attacks aimed at using stolen credentials. We've seen two of our portfolio companies combat these threats through different methods. Cofense (formerly PhishMe) sits at the center of a movement to an "employee-centric" model of security that educates and empowers employees to be the first line of defense in identifying potential phishing emails, which are then analyzed and blocked by Cofense's platform. PerimeterX uses advanced machine learning to screen web and application traffic to identify and block bot traffic to protect the identities of users on their customers' networks. Proactive identification and protection served as the key themes of these investments and are concepts we continue to believe in.

Leverage Network Effects

While the number of security products available can be intimidating from a customer (and an investor) standpoint, one of the best things to come out of the amalgam of solutions in the market is the amount of threat, vulnerability, and user data being collected. As we've seen in other industries, security organizations that gain a critical mass of users and data can create a network effect in which each incremental user increases the value of the platform to all users. This generates a positive feedback loop in which that data improves the solution, which in turn attracts more customers. This dynamic is especially true in security, where detection rates and minimization of false positives reign supreme in customer bakeoffs.

The Security Flywheel

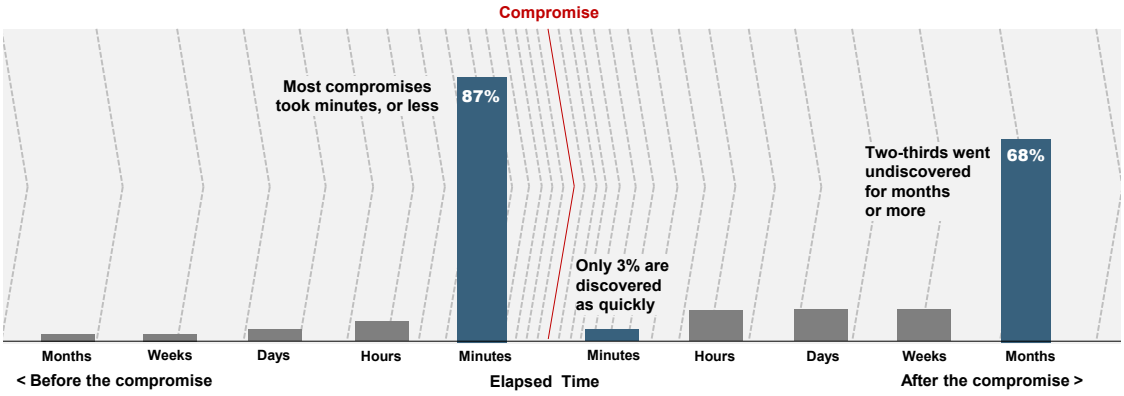


We've seen a number of our portfolio companies, both past and present, leverage network effects to their benefit. Security Information and Event Management (SIEM) products like LogRhythm (acquired by Thoma Bravo last year) were the first technologies to ingest massive amounts of log data from across their customer base to deliver better threat insights. ThreatMetrix's platform similarly became more valuable as it added more customers and identities. Today, we've seen Cofense's platform gain value as it adds more employees, which in turn increases their data collection points, making them one of the largest repositories for phishing data in the market. Additionally, PerimeterX ingests a significant amount of botnet activity from across their customer base, which then strengthens their algorithm's ability to differentiate between human and bot behavior and limit false positives. We continue to be attracted to security businesses that creatively leverage the power of network effects.

1. "When People Are the Perimeter, We Need a Zero Trust Approach to Security", September 2018 by Yassir Abousselham

Invest in Modern Security Operations

Let's say an organization has done everything mentioned above. They've identified and secured knowledge gaps in their architecture, they've implemented policies to know who is on their network, and they leverage network effects. Unfortunately, there is still a very real probability that this organization will still get attacked despite their proactive defenses. That's why organizations still need to build strong detection and response capabilities.



Source: "2018 Data Breach Investigations Report" March 2018, Verizon

Verizon data demonstrates that while most compromises take minutes or less to execute, 68% of breaches take months or longer to even discover and only 3% are discovered in the amount of time it takes to execute an attack. Part of the problem is a lack of visibility and intelligence as discussed earlier. Another significant problem is the current skills and operations gap in cybersecurity. Security operations teams not only struggle with a massive supply demand imbalance (Cybersecurity Ventures estimates a global shortfall of 3.5 million cybersecurity jobs by 2021[2]), but security analysts are often overwhelmed by the thousands of alerts from their numerous security products.

We've seen organizations and some of our portfolio companies themselves tackle this problem in different ways. ThreatQuotient saw an opportunity to expand the capabilities of their threat intelligence platform and added contextual intelligence, prioritization, and response functions which allow customers to automate and orchestrate how they respond to incoming threats. Other products around the SOAR (security orchestration, automation, and response) space have come to market with the goal of providing a common system for different best-of-breed security products to communicate with each other, which we've seen gain significant adoption at the enterprise level. Within small and medium-sized enterprises, we've seen many organizations look to outsource more of their security operations to providers such as Arctic Wolf Networks, who provide Security Operations Center (SOC) automation services that can decrease a significant number of tasks for security operations teams. All of these approaches are critical towards establishing a modern approach to security operations, which can allow overworked security teams to proactively detect threats and orchestrate responses to breaches in a more efficient manner.

Bringing it All Together

The cybersecurity landscape continues evolve, and the challenges facing organizations today – both large and small – do not seem to be going away anytime soon. Thankfully, the security sector continues to invest heavily in innovation to combat looming threats, and organizations are taking notice of the need for strong security programs. As investors, we continue to invest in companies that help organizations implement a proactive security strategy. We're excited about the innovation occurring in the space and believe in the talent and vision of the many entrepreneurs leading the charge in securing the world's technology infrastructure.

2. "Cybersecurity Jobs Report, 2017 Edition", Herjavec Group

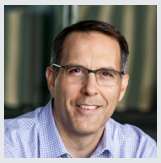
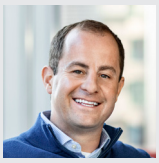
Adams Street Growth Equity Investment Capabilities Overview

Adams Street Partners invests directly into private companies. The team typically invests between $10M-$30M in technology and healthcare companies, targeting category-leaders in Application Software, Mobile / Internet, Infrastructure Software, Fintech, Digital Health and Life Sciences. The Growth Equity team has 6 Partners, 1 Principal, and 4 Associates with 4 Partners dedicated to technology investments and 2 Partners dedicated to healthcare investments.

Our Growth Equity Investment Criteria

- **Stage:** $5M-$10M minimum revenues, typical companies between $10M-$100M of revenues and $50M-$500M TEV
- **Growth:** Generally 30%+
- **Lead & Price Rounds:** Generally take Board seats (80% of the time)
- **Check Size:** $10M-$30M (avg. $15M-$20M initial check)
- **Capital Committed Annually:** Approx. $200M; $2B+ in AUM since inception

Experienced Team with Domain Expertise

					
Tom Bremner	Jeff Diehl	Terry Gould	Robin Murray	Fred Wang	Mike Zappert
Digital Health	Fintech Application Software	Biopharma Medical Device	Mobile / Internet Fintech	Cyber Security Infrastructure Software	Application Software Mobile / Internet

For more information, contact Fred Wang at fredwang@adamsstreetpartners.com

Founded in 1972, Adams Street Partners is one of the most respected and experienced private markets investment managers in the industry. With 190+ staff in ten offices – Beijing, Boston, Chicago, London, Menlo Park, Munich, New York, Seoul, Singapore, and Tokyo – our deep industry experience and global outlook provide clients with customized access to the spectrum of private markets strategies. As of June 30, 2018, Adams Street is 100% employee-owned and independent, and manages more than $35.5 billion in assets for more than 390 institutional investors, including corporate and public pensions, foundations, family offices, and endowments.

adamsstreetpartners.com