Brief: Endpoint Security Innovation Is Intensifying

The Time Is Now To Protect Your Digital Workforce With A Reinvigorated Endpoint Security Strategy

by Rick Holland and Chris Sherman
with Stephanie Balaouras and Josh Blackborow

WHY READ THIS BRIEF

For your employees to do their very best work, they need access to a wide range of business applications and sensitive information — often from whatever endpoint device they deem appropriate. Unfortunately, adversaries target employee desktops and laptops and use them as a beachhead into the corporate infrastructure where your servers reside. Today's threats have long since surpassed traditional antivirus capabilities, and security and risk (S&R) professionals need endpoint security solutions that build resiliency against these threats. After many prolonged years of scant innovation, a new generation of endpoint security solutions is finally emerging. In the first half of 2015, Cybereason, Digital Guardian, Fidelis Cybersecurity, Resolution1 Security, Savant Protection, and Tanium have all made the headlines for either significant investment rounds or acquisitions in endpoint security. In this brief, Forrester examines the current innovations in the endpoint security market and includes specific recommendations on how to navigate the vendor landscape and select the right partner that is most appropriate for your cybersecurity needs.

AFTER YEARS OF STAGNATION, ENDPOINT SECURITY IS FINALLY DELIVERING

Ever since the first commercially available antivirus engines came to market in the late 1980s, S&R pros have centered their endpoint threat protection strategies on blacklisting-based solutions. However, as malware increases in sophistication and the number of new variants and methods of obfuscation rises, antivirus technologies have steadily become less effective at stopping advanced threats to employee endpoints and servers. As a result, a number of competing technologies and vendors have risen up and taken aim at the stagnant antivirus market, many armed with fresh VC funding or new IP obtained through acquisitions. For instance, in the first half of 2015:

- **Tanium raised $52 million.** On March 31, security and systems management vendor Tanium raised $52 million with venture capital powerhouse Andreessen Horowitz.[1] Tanium has now raised an astounding $142 million in two rounds.[2] Tanium straddles two worlds; you can leverage it for endpoint security or systems management. Tanium customers can perform threat detection and incident response alongside patch management and software deployment.

- **Israeli startup Cybereason raised $25 million.** On May 6, endpoint visibility and control (EVC) vendor Cybereason announced a $25 million Series B round led by Spark Capital. Defense contractor Lockheed Martin, a Cybereason customer, also participated in the round.[3] Cybereason was also an RSAC Innovation Sandbox finalist.[4] Cybereason provides automated detection and response and has powerful visualization that enables defenders.

- **Fidelis Cybersecurity acquired Resolution1 Security.** Fidelis didn't waste any time; just weeks after General Dynamics spun it off on May 12, Fidelis acquired EVC vendor Resolution1 Security. Resolution1's approach is to enable customers to proactively hunt the adversary, and the vendor has a strong focus on automated incident response workflows. It's an impressive acquisition; Fidelis now has strong network and endpoint security solutions coupled with its professional services offerings. Fidelis, like Crowdstrike and FireEye, will now have its own EVC solution to leverage during incident response engagements. Competitors should take note of the new Fidelis.[5]

- **Digital Guardian acquired Savant Protection.** On May 12, Digital Guardian (formerly Verdasys) announced its acquisition of Savant Protection, an application whitelisting technologies provider with considerable adoption in POS, server, and industrial control systems (ICS) environments. Digital Guardian has plans to integrate the Savant Protection technology into its endpoint security platform, which already provides a unique mix of internal threat-focused data leak prevention (DLP) and external threat-focused EVC, by the end of 2015. Bringing whitelisting into the fold will give Digital Guardian a well-balanced set of preventive-, reactive-, and response-focused capabilities ideally suited for security teams looking to move away from paid AV within static and compliance-heavy environments.[6]

- **CounterTack raised $15 million.** On June 2, CounterTack announced it had closed a $15 million Series C round led by TenEleven Ventures. CounterTack has raised $49.5 million in three rounds. CounterTack's Sentinel is an on-premises EVC solution focused on detection and response.[7]

But The Market Is Crowded, And Many Promising Vendors Won't Survive

Forrester is tracking more than 40 endpoint security vendors. These vendors offer application integrity protection, application privilege management, application whitelisting, endpoint execution isolation, and endpoint visibility and control (see Figure 1). Forrester expects that, during the next 18 months:

- **Startups with good technology but poor go-to-market strategies will fizzle out.** The market simply can't sustain the number of endpoint security vendors out there. This isn't the Hunger Games: There will be more than two victors, but all the tributes won't survive.[8] It isn't enough to have innovative technology; startups also need a sales and marketing strategy that lands them on the vendor selection shortlist. Vendors with solutions that harm the user or administrator experience, well, the odds won't ever be in their favor.[9]

- **Large vendors will gobble up startups to fill critical gaps in their portfolios . . .** The portfolios of both Bluecoat and HP are missing endpoint security offerings. If they want to better compete against the likes of FireEye and Palo Alto Networks, which both have compelling network and endpoint capabilities, they would do well to make an acquisition.[10] Buyers want integrations,

and despite talk of competitors partnering on integrations, it isn't always a high priority. With multiple solutions in one vendor's portfolio, there is more control, which eliminates the need for reluctant cooperation between competitors.

- **. . . and to garner attention and improve their tarnished brands.** Traditional endpoint security vendors like Symantec would do well to acquire one of these new endpoint security offerings. Symantec isn't thought of as an innovative company; even if it were to develop a new capability, it would likely not capture the buyer's attention. Symantec and other traditional endpoint security vendors would be better served to take the Bit9 Carbon Black approach and acquire an innovative startup that would get them some positive publication.[11] Customers of a startup could benefit from this type of acquisition, as the smaller company would have access to new resources to expedite development of road map items that customers need.

Figure 1 Emerging Endpoint Security Vendors

Technology	Key vendors
Application integrity protection	• Abatis • Cylance • Digital Immunity • IBM Security Trusteer • Palo Alto Traps
Application privilege management	• AppSense • Avecto • BeyondTrust • Centrify • Viewfinity
Application whitelisting	• AppSense • Bit9/Carbon Black • Lumension Security • McAfee (Intel Security) • Viewfinity
Endpoint execution isolation	• Bromium • Bufferzone • Google Chrome • Invincea • Menlo Security
Endpoint visibility and control	• Bit9/Carbon Black • Confer • Crowdstrike Falcon Endpoint • Cybereason • Digital Guardian • FireEye HX • SentinelOne

122981 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Use These Seven Questions To Pick The Best Fit

You can't wait for the market to shake itself out. Protecting your firm's digital workforce is too important. According to the Verizon 2015 Data Breach Investigations Report, attackers were able to compromise an organization within minutes 60% of the time.[12] Mandiant's latest annual threat report says the average time to detection is 205 days.[13] Adversaries are doing a better job of data discovery in your environment than you are. New endpoint capabilities give you the ability to prevent, detect, and respond to attackers in a way that traditional AV simply cannot. To help you determine which vendors are the best fit for your unique environment and challenges, we developed a list of critical questions (see Figure 2).

Figure 2 Vendor Selection Questions

Question	Comments
How many of the following capabilities does your product offer: prevention, detection/monitoring, containment/response?	Prevention will fail, so prevention alone isn't enough. Detection/monitoring isn't sufficient, because once you see something bad you will want to take action. Invest in vendors that stack these functions.
What operating systems do you support?	Many vendors only support specific operating systems, which complicates heterogeneous environments.
What is your largest deployment size?	Deployment size is a good litmus test for enterprise maturity and scalability.
Do you operate in kernel, user land, or both?	Operating in the kernel equates to running an enterprise rootkit, and competition within the kernel can result in problems. You must thoroughly test any solution that operates in the kernel to make sure it plays nice. Deploying an agent in user space doesn't involve the same friction as deploying within the kernel, but if a machine is already compromised you cannot trust what a user space agent reports back.
Do you deliver your product on-premises or via cloud infrastructure as a SaaS service?	There are advantages to leveraging a cloud service, but many organizations are cloud-averse.
How does your product leverage threat intelligence, and does it consume or generate threat intelligence?	Solutions can create and consume threat intelligence in many formats: YARA, OpenIOC, CybOX/STIX, JSON.
What other solutions does your product integrate with?	You want to reduce operational friction through integrations. Make sure the vendor has integrations with other solutions in your portfolio. Example include network integrations that launch packet captures or malware analysis integrations that submit content for inspection.

122981 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

RECOMMENDATIONS

IT'S TIME TO PREPARE FOR A NEW ENDPOINT STRATEGY

S&R professionals should consider new endpoint security solutions that are better prepared to address today's overwhelming threat landscape. You may not be ready to remove your traditional antivirus solution, but you must complement it with new capabilities. Make sure that you:

- **Start building trust with your infrastructure and operations colleagues now.** Successfully deploying new agents to servers, workstations, and laptops requires organizational finesse. Your colleagues will hesitate to add any new software that could hurt performance and employee experience. Installing yet another agent isn't a popular proposition, so you must gain their support and trust. To get their buy-in, start socializing the benefits of a more-effective strategy that will reduce their operational efforts. For instance, fewer compromised hosts, and faster detection of compromised hosts, will reduce their reimaging and rebuilding efforts.

- **Start evaluating solutions now.** S&R professionals have a long list of needs and a budget that doesn't address all of those needs. Even if you don't yet have budget, you can still evaluate technologies. You can also do extensive testing to ensure that you will have the support of your I&O peers when you can make the investment. There are even solutions like the Microsoft Enhanced Mitigation Experience Toolkit that may be included in your enterprise licensing agreement. There are also open source solutions like Google's Rapid Response or Immunity's El Jefe that you could evaluate. A delayed investment strategy can be beneficial as the market matures and vendors introduce additional capabilities onto their agents which will maximize the ability to prevent, detect, and respond.

- **Make laptops a top priority.** Any machine that moves in and out of your environment beyond the reach of your network security controls must have an additional layer of security deployed to it. In the age of the customer, highly mobile employees require additional protection as they operate outside your perimeter. Drive-by downloads and the continued use of strategic web compromises as an attack vector means you must reduce the likelihood that one of your employees will bring an infected machine back into your environment.

ENDNOTES

[1] Source: "Tanium Secures Additional $52 Million Investment from Andreessen Horowitz," Tanium press release, March 31, 2015 (https://www.tanium.com/news-and-events/press-releases/read/tanium-secures-additional-52-million-investment-from-andreessen-horowitz).

[2] Soure: "Tanium," CrunchBase (https://www.crunchbase.com/organization/tanium).

[3] Source: "Cybereason Closes $25 Million Series B Funding Round, Enters Strategic Partnership with Lockheed Martin," PR Newswire, May 6, 2015 (http://www.prnewswire.com/news-releases/cybereason-closes-25-million-series-b-funding-round-enters-strategic-partnership-with-lockheed-martin-300078253.html).

[4] The 2015 RSA Conference (RSAC) Innovation Sandbox marks the 10-year anniversary of its conception in North America. This contest has encouraged startups to demonstrate and share their security innovations. The conference leaders select representatives from venture capital firms, entrepreneurs, and large security companies as judges, who thoroughly assess each startup submission. Without these innovative startups, security and risk (S&R) professionals could never keep pace with the never-ending number of vulnerabilities and exploits that emerge with new business models, customer engagement models, and ongoing technology shifts. For more information, see the "RSAC Innovation Sandbox Finalists Spur Ingenuity In Security" Forrester report.

[5] Source: "Fidelis Cybersecurity Poised for Next Phase of Growth in Advanced Threat Defense Market, Estimated to Reach Nearly $1 Billion in 2016," Yahoo Finance, May 4, 2015 (https://finance.yahoo.com/news/fidelis-cybersecurity-poised-next-phase-160000433.html).

Source: Sean Michael Kerner, "Fidelis Cybersecurity Buys Resolution1 to Provide Advanced Protection," eWeek, May 12, 2015 (http://www.eweek.com/security/fidelis-cybersecurity-buys-resolution1-to-provide-advanced-protection.html).

[6] Source: "Summary of Changes from PCI DSS Version 3.0 to 3.1," Payment Card Industry, April 2015, (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_Summary_of_Changes.pdf).

[7] Source: Tom Bain, "CounterTack Announces $15M Series C Round of Financing," CounterTack press release, June 2, 2015 (http://www.countertack.com/press-releases/countertack-announces-15m-series-c-round-of-financing).

[8] In the book The Hunger Games, by Suzanne Collins, "tributes" are residents of the 12 districts of Panem who are forced/volunteered to participate in an annual Hunger Game. Historically, only one tribute survives the game.

[9] Source: Rick Holland, "Say 'Small Footprint' Again. I Dare You, I Double Dare You." Rick Holland's Blog, July 24, 2014 (http://blogs.forrester.com/rick_holland/14-07-24-say_small_footprint_again_i_dare_you_i_double_dare_you).

[10] On January 2, 2014, FireEye announced its acquisition of incident response and forensics specialist Mandiant for nearly $900 million in stock and $100 million in cash. With this acquisition, FireEye establishes a security portfolio unencumbered by traditional security solutions that have struggled to keep pace with the threat landscape. To learn more, see the "Quick Take: FireEye Acquires Mandiant" Forrester report.

On March 24, 2014, Palo Alto Networks announced an agreement to acquire Cyvera, a privately held endpoint security company, for approximately $200 million. With the acquisition, Palo Alto Networks rounds out its capabilities to provide security for the data center. For more, see the "Quick Take: Palo Alto Networks Acquires Cyvera" Forrester report.

[11] On February 13, 2014, Bit9 announced that it had merged with endpoint incident response startup Carbon Black, for an undisclosed amount. Bit9 also announced that it had raised $38.25 million to fuel the growth of the new company. The merger gives the new Bit9 the ability to detect and prevent attacks against the endpoint while providing real-time incident response capabilities. To learn more, see the "Quick Take: Bit9 And Carbon Black Merge" Forrester report.

[12] Source: "2015 Data Breach Investigations Report," Verizon (http://www.verizonenterprise.com/DBIR/2015/).

[13] Source: "M-Trends 2015: A View from the Front Lines," Mandiant (https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html).