Brief: FireEye Is Evolving Into An Enterprise Security Vendor

Recent Acquisitions Indicate FireEye Is Ready To Advance Security Automation

by Jeff Pollard, Joseph Blankenship, and Kelley Mak

March 30, 2016

Why Read This Brief

FireEye's acquisition of automation specialist Invotas International comes just 10 days after its acquisition of threat intelligence specialist iSight Partners. With these and prior acquisitions, FireEye continues its evolution from a malware analysis specialist to an enterprise security vendor with solutions for prevention, detection, and remediation. The Invotas acquisition also shines a spotlight on the emerging market for security automation solutions. For security and risk (S&R) pros considering FireEye, this report examines the strengths and weaknesses of its strategy.

Key Takeaways

Invotas Acquisition Demonstrates The Growing Need For Automation

This acquisition highlights the extent to which integration complexity and workflow enablement has become a key concern for CISOs. It also indicates that CISOs may be ready to move from interest to adoption of automation solutions that address this concern.

FireEye Matures By Combining Intelligence, Analytics, And Workflows

FireEye's strategy extends far beyond malware analysis. It's now focused on building an integrated platform of technology offerings. With presence in multiple areas of the modern security stack, S&R pros have many options to engage with and deploy FireEye's suite of solutions.

Brief: FireEye Is Evolving Into An Enterprise Security Vendor

Recent Acquisitions Indicate FireEye Is Ready To Advance Security Automation

by Jeff Pollard, Joseph Blankenship, and Kelley Mak
with Stephanie Balaouras, John Kindervag, Claire O'Malley, and Peggy Dostie
March 30, 2016

FireEye Now Has A Portfolio For Detection And Remediation

On February 1, FireEye announced its acquisition of security automation vendor Invotas for an undisclosed sum.[1] The purchase of Invotas comes hot on the heels of FireEye's acquisition of iSight Partners on January 20 for $200 million.[2] It is one of four acquisitions demonstrating the vendor's desire to expand its security footprint while also innovating the way security teams deal with targeted attacks (see Figure 1).[3] These acquisitions have also helped FireEye develop a comprehensive and diverse portfolio that combines threat intelligence, security analytics, and orchestration to deliver a complete approach for detection and containment or remediation. Today, FireEye is:

- **Demonstrating a willingness to act quickly on acquisitions.** The ability to identify specific gaps in its product and service portfolio and a willingness to plug them is becoming a hallmark of FireEye. This ability is one element, but the boldness to act quickly grants FireEye two advantages: 1) the opportunity to set the tone for potential valuations and 2) first choice of potential acquisition targets. The Mandiant acquisition signaled the coming age of high-profile breaches.[4] nPulse brought network visibility and packet capture.[5] iSight Partners augments the existing collection with additional sources beyond incident response engagements.[6]
- **Poised to act on security analytics.** FireEye has a breadth of technology that covers the network and endpoint. The data exhaust from these technologies and the Invotas acquisition will enable FireEye to both develop insight and act on it automatically across the environment.[7] Historically, SOC analysts pivoted between three to four technologies and interfaces to respond to a breach. Now, imagine that when there is an anomaly on an endpoint, it triggers an alert; an agent on the endpoint captures memory; a packet capture is initiated on all network traffic; the endpoint is shifted to a new VLAN for containment; and the user ID and password are reset — all automated, with limited or no resource involvement and no tool switching required.
- **Ready to help S&R pros enact Forrester's rules of engagement.** The only way to prevent the exfiltration of toxic data according to predetermined risk tolerance levels set by the business is to automate the response.[8] When S&R pros define security policy according to declared business needs, automation tools like Invotas help coordinate a swift response. They do this by leveraging

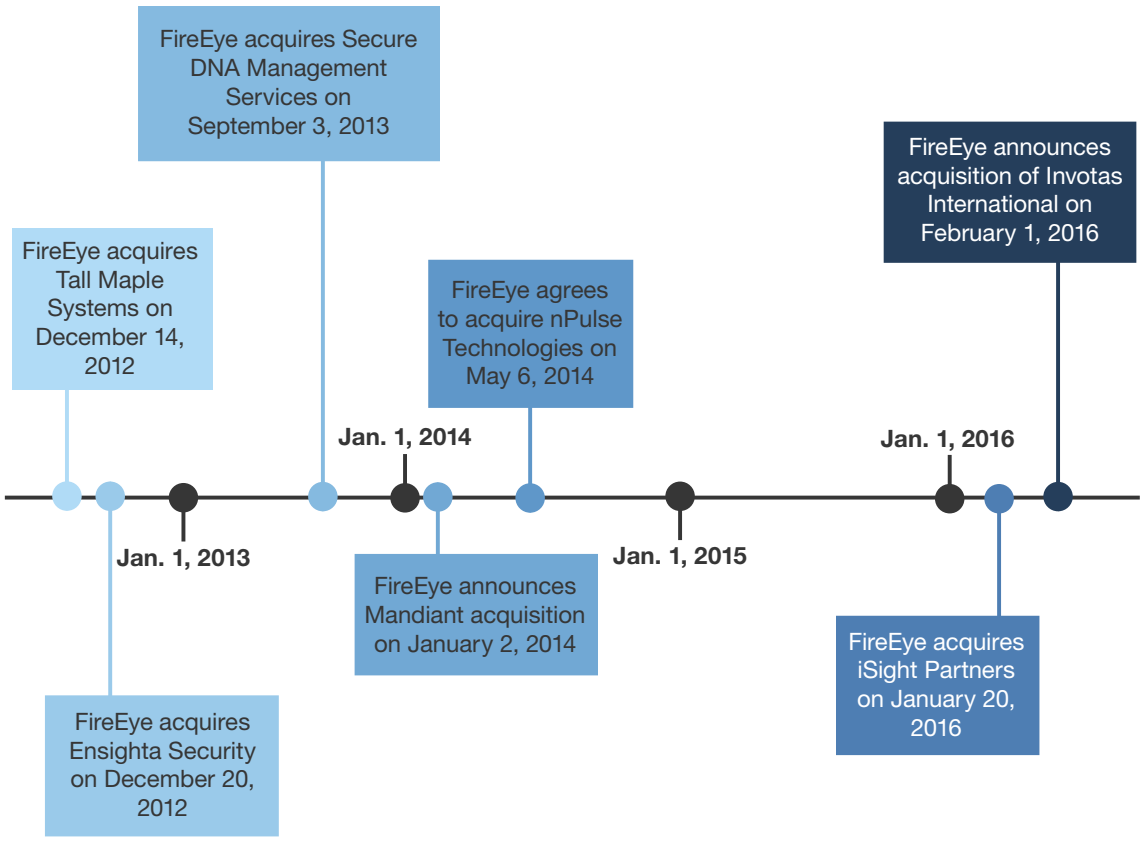
FORRESTER®
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2016 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

a security analytics engine that generates a response index based on factors such as importance and likelihood of a breach, thus allowing security teams to automate the right type of response based on the event.

› **Providing a clean interface for security automation.** There has always been a need for security orchestration and automation, but it hasn't been possible due to disparate systems that don't have efficient intelligence exchange. Invotas provides a programmable interface that can allow for this information export and ingestion. By bringing an interface to market that ties technology to processes — the true value gained by automation — FireEye can increase customer reliance on its technologies by owning the integration centerpiece.

FIGURE 1 Timeline Of FireEye's Acquisitions



© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FireEye's Invotas Acquisition Fills A Critical Need For Automation

Spun out by CSG International in November 2015 after its debut in 2014, Invotas' product, Invotas Security Orchestrator, helps large enterprises automate many tasks that security operations teams perform manually, allowing these teams to work at scale with great speed. This is an important acquisition for FireEye because Invotas will help S&R pros:

- **Address the deluge of security alerts and the skills shortages on their teams.** The 2015 M-Trends report from Mandiant showed that in 2014, the average time-to-detection was 205 days.[9] Automation solutions can solve the scale problem that exists between the volume of alerts, the talent and skill shortage, and adversary evolution. Making the repeatable automatic and minimizing human involvement lets security practitioners focus on tasks and responsibilities that truly require situational awareness and contextual decision-making. The workflow functionality brought by automation allows staff to shift the cognitive loop from "What happened?" and "What do we do next?" to "What does it mean to the business?"
- **Integrate and orchestrate point solutions in their security ecosystem.** Expense in depth is the precursor to a Frankenstein monster's security stack that is both daunting and horrible to manage. Invotas can break the barrier between silos and create workflows between endpoint, network, and identity technologies without making S&R pros rely on vendor alliances and partnerships for API development efforts.[10]

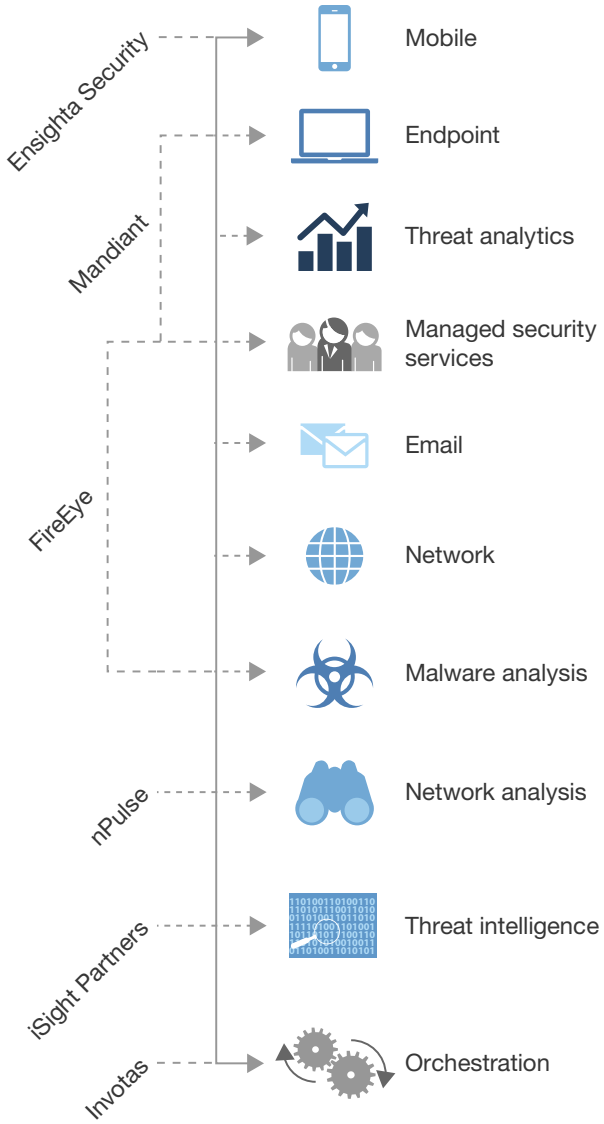
Long-Term Success Will Depend On FireEye's Ability To Integrate Its Acquisitions

While FireEye's portfolio looks promising, long-term success will depend on its ability to integrate its acquisitions into its own organization and into a consolidated solution suite that delivers on its promises. S&R pros considering Invotas, iSight, or FireEye solutions need to be aware that FireEye must:

- **Absorb the employees, customers, and systems of its acquired firms.** FireEye has made two acquisitions in just the first two months of 2016, which means it will need to simultaneously integrate the employees, systems, and customers of two separate companies. However, Invotas has only 19 employees, so it shouldn't present the same integration challenge as iSight.[11] In addition, given its track record with prior acquisitions, it's clear that FireEye understands acquisitions and integrations. As with any acquisition, customers will experience some bumps as support and account resources shift, but we expect the bumps to be minimal given the small size of these acquisitions.
- **Provide a detailed road map on the integration and strategy of FireEye's portfolio.** Threat Analytics Platform (TAP), iSight Partners, and Invotas for automation becomes a natural focus area for security teams moving forward. High confidence analytics technologies feeding orchestration tools is a must, and TAP's role in the portfolio is muddied if Invotas becomes the centralized point of execution rather than the existing analytics technology. Invotas creates the capability to tie disparate systems together for action but will require a detailed product and development road map to make that happen (see Figure 2).

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Breakdown Of FireEye's Product Portfolio



© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Recommendations

Evaluate FireEye As An Enterprise Security Partner

FireEye is a newer company that now has the capability to offer technologies and services against traditional security vendors such as Intel Security, Palo Alto Networks, and Symantec. Thinking of it as a malware analysis company or a professional services company is incorrect. Instead, understanding and analyzing the firm as a vendor with products across the technology stack, managed security services, and professional services is the right approach to determine the use cases it could solve for a team. S&R pros should:

- **Interrogate FireEye on its road maps for both organization and product.** When vendor acquisitions occur, customers often find themselves with an adjusted road map, different expectations, and different strategies when new leadership takes the helm. Understanding the current, transition, and future state of technologies increases in importance after acquisition. Current clients planning projects that could contain Invotas, iSight, or FireEye products and services should request to see road maps within 90 days of the close of acquisition to better inform their selection strategies.
- **Expect to see the clear benefits of Invotas integration within 12 months.** If Invotas integrates well and becomes a foundational layer of action for FireEye's product and service portfolio, S&R pros should see substantial benefits by automating the mundane as well as better integration of network, email, endpoint, and analytic technologies. Within 12 months, it will be immediately clear whether that foundation develops or whether the acquisition becomes a historical blip on the radar. For S&R leaders, automation should be a goal, but not an immediate one. Using the 12-month time frame lets a security team address current projects while keeping an eye on successful incorporation of Invotas into FireEye's offering.
- **Reexamine security policies, before investing in automation.** To enable automated detection and remediation, security teams will need to examine their security strategy and develop policies to take advantage of the technology. This may require extensive upfront professional services to implement successfully without having a negative impact on the business. Automated breach response has long been a security dream, but that dream will quickly become a nightmare if there are unforeseen consequences from automated actions. S&R pros don't want to lock out what they thought was an attacker only to find out they've actually shut out system administrators from critical line-of-business applications due to an error in process.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

What It Means

Security Automation Has Arrived

Automation technologies are in the creation phase; early adopters are only considering them as potential technology worthy of investment. However, if FireEye's past acquisitions are any indication, the company has a knack for knowing when a market is just about to explode. When FireEye purchased Mandiant, it did so just before reports of massive breaches became a staple of the 24-hour news cycle — and with every news report, a favorable mention of Mandiant as the chosen services firm. Forrester believes that FireEye's purchase of Invotas is a harbinger of the security automation market, the missing technology that finally turns a massive number of alerts into insight and action against evolving threat actors.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Endnotes

[1] Source: Josh Beckerman, "FireEye Buys Invotas International," The Wall Street Journal, February 1, 2016 (http://www.wsj.com/articles/fireeye-buys-invotas-international-1454375898).

[2] FireEye announced on January 20 the acquisition of threat intelligence vendor iSight Partners for $200 million, giving the antimalware vendor an entry into the crowded threat intelligence market. Once considered a darling of both the security industry and investor community, FireEye's stock price has slumped recently as the company struggles with competitive pressures and the loss of much of the human capital it gained with its acquisition of Mandiant in 2013. For more information, see the "Quick Take: FireEye Acquires iSight Partners" Forrester report.

[3] Source: Mike Lennon, "FireEye Acquires Security Orchestration Firm Invotas," Security Week, February 3, 2016 (http://www.securityweek.com/fireeye-acquires-security-orchestration-firm-invotas).

FireEye announced on January 20 the acquisition of threat intelligence vendor iSight Partners for $200 million, giving the antimalware vendor an entry into the crowded threat intelligence market. Once considered a darling of both the security industry and investor community, FireEye's stock price has slumped recently as the company struggles with competitive pressures and the loss of much of the human capital it gained with its acquisition of Mandiant in 2013. For more information, see the "Quick Take: FireEye Acquires iSight Partners" Forrester report.

Source: Dave DeWalt, "FireEye Enters Agreement To Acquire nPulse Technologies," FireEye Blog, May 6, 2014 (https://www.fireeye.com/blog/executive-perspective/2014/05/fireeye-enters-agreement-to-acquire-npulse-technologies.html).

Source: "Acquisitions in 2013," Market Vis.io (https://www.marketvis.io/stock/feye/financial/fy-2013/note/businesscombinationdisclosuretextblock).

Source: "Notes to Consolidated Financial Statements," Edgar Online (http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=9825254-384528-506744&type=sect&TabIndex=2&companyid=716732&ppu=%252fdefault.aspx%253fcik%253d1370880).

[4] Source: "FireEye Announces Acquisition Of Mandiant," FireEye press release, January 2, 2014 (https://www.fireeye.com/company/press-releases/2014/01/fireeye-announces-acquisition-of-mandiant.html).

[5] Source: Dave DeWalt, "FireEye Enters Agreement To Acquire nPulse Technologies," FireEye Blog, May 6, 2014 (https://www.fireeye.com/blog/executive-perspective/2014/05/fireeye-enters-agreement-to-acquire-npulse-technologies.html).

[6] FireEye announced on January 20 the acquisition of threat intelligence vendor iSight Partners for $200 million, giving the antimalware vendor an entry into the crowded threat intelligence market. Once considered a darling of both the security industry and investor community, FireEye's stock price has slumped recently as the company struggles with competitive pressures and the loss of much of the human capital it gained with its acquisition of Mandiant in 2013. For more information, see the "Quick Take: FireEye Acquires iSight Partners" Forrester report.

[7] As data volumes explode, it's becoming a Herculean task to protect sensitive data from cybercriminals and malicious actors while preventing privacy infringements and abuses — intentional and unintentional. Every day, vendors introduce a new product or service that claims to be the cure-all to data security challenges. For more information, see the "TechRadar™: Data Security, Q1 2016" Forrester report.

[8] It seems that not a day goes by that there isn't another massive security breach in the news. Consumers around the globe hear about continual threats to their personal data while name brand retailers and enterprises are spending millions to respond, remediate, and recover from the theft of sensitive customer data and intellectual property. As the costs of data breaches skyrocket and regulators add more compliance burdens to the enterprise, the security industry must find new ways to more comprehensively meet these threats and prevent the exfiltration of proprietary data into the hands of cybercriminals and other malicious actors. For more information, see the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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

[10] Targeted attacks continue to plague organizations, and these intrusions damage the brand, customer loyalty, and margins. Preparing for and responding to these attacks requires a focused and resolute strategy. We designed Forrester's Targeted-Attack Hierarchy Of Needs to give S&R professionals a framework to accomplish this. For more information, see the "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities" Forrester report.

[11] Source: Mike Lennon, "FireEye Acquires Security Orchestration Firm Invotas," Security Week, February 3, 2016 (http://www.securityweek.com/fireeye-acquires-security-orchestration-firm-invotas).

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.