FireEye Continues Aggressive Expansion Strategy

September 29, 2014 - IDC Link

By: John Grady; Christina Richmond

The market for advanced threat prevention solutions continues to be one of the most dynamic and interesting areas within IT. With massive data breaches seemingly making news on a weekly basis, organizations continue to prioritize spending on solutions that help detect, analyze, and remediate these sophisticated attacks. Security vendors of all sizes and disciplines have built, acquired, or partnered for technologies that address some part of the attack chain. Despite this increased focus and competition, FireEye has managed to maintain a leadership position in the market on impressive revenue growth.

To accomplish this, FireEye has had to evolve markedly over the past 12 months. Following a successful IPO in September 2013, the vendor acquired security consulting and services firm Mandiant. Known primarily for its proficiency in incident response, Mandiant also provided FireEye with endpoint technology to extend its presence beyond the network, as well as a managed security services framework for future expansion. In February, FireEye introduced an IPS module add-on for its NX series Network Threat Prevention Platform, formally entering one of security's more established markets. The acquisition of nPulse Technologies in May added full packet capture and network forensics capabilities to the portfolio, creating a full spectrum endpoint-to-network and detection-through-investigation product set.

On September 17, 2014, the vendor announced the newest addition to its portfolio: FireEye as a Service. FireEye as a Service is based on the concept that, to adequately defend against modern advanced attacks, three pillars are required: technology, intelligence, and expertise. These pillars become the framework for what FireEye calls an Adaptive Defense security model, which enables greater agility and a quicker response to threats. With FireEye as a Service, the vendor's customers are able to deploy its solutions as a product and incur a capital expense or as a service and account for the solution operationally. FireEye is leveraging its Mandiant assets to deliver this service directly to customers. In addition, customers already utilizing an overall managed security service deployment through a traditional MSSP can add FireEye as a Service from participating partners.

Because of the varying levels of security expertise and sophistication across organizations, the implementation of these pillars must be flexible. FireEye as a Service is made up of multiple components to address a broad spectrum of the attack chain. Products are deployed on-premise for detection and are monitored by analysts in FireEye's global SOCs. When potential incidents are identified, these analysts utilize FireEye's forensics capabilities to determine scope and begin containment. Finally, incident response services provide deeper investigative capabilities and remediation of affected systems.

In addition to this new services offering, FireEye has expanded its threat intelligence portfolio with Advanced Threat Intelligence. The subscription provides organizations with granular detail on attacks by correlating specific actors, motivations, types of malware, and compromise indications to help better understand and scope incidents. Moreover, the service provides predictive intelligence on targeted industries and data types, groups of bad actors, and other analysis to help organizations better prepare for potential attacks.

Security has always been about more than technology. Skilled people and the adherence to process are core to a strong security posture for any organization. This is exceedingly true when considering the issues organizations face around modern attacks. Through acquisition and organic development, FireEye has

successfully expanded its presence from a network-based threat detection company to a holistic cyber-attack solution provider.

Subscriptions Covered:

Security Products, Security Services