ATTAINING COMPREHENSIVE CYBERSECURITY AWARENESS AT MACHINE SPEED

How advanced threat intelligence and a new suite of automated tools from FireEye are helping agencies narrow their multicloud security gaps.

FireEye Government Chief Technology Officer Ron Bushar has seen his share of ransomware cases and security breaches over the past 12 months. The scenes are familiar. He and FireEye analysts would gather, side by side, with members of a government agency’s security team to assess what they were dealing with. The FBI would usually be there—sometimes so would the Secret Service—along with specialists from various security technology vendors.

In years past, FireEye would partner with Mandiant to investigate cybersecurity breaches: FireEye was the company that could tell you who the hackers were and how to respond. Since then, Mandiant incident response and intelligence experts have responded to tens of thousands of breaches around the world.

FireEye has earned its reputation for having a pulse on global hacking exploits—and for providing automated tools to detect and deal with them quickly. That reputation has continued to grow with a series of acquisitions, including most recently, Verodin (now known as Mandiant Security Validation), a security instrumentation provider, and Cloudvisory, which provides security visibility across multiple clouds.

“FireEye can now come in and deploy what we know about every variant of ransomware we’re seeing around the world, and start to look for it within minutes, regardless of which technology an agency is using,” says Bushar. “We can immediately say, ‘It’s probably this group. Here’s the techniques they use. Here’s how they got in. Here’s where to look to find where they deployed their ransomware. And here’s the best way to go about isolating this and getting your systems back online.’”

“Agencies have the same capacity problem that everyone else does in maintaining a talented skill set. And everybody’s overworked, right?” says Bushar, who served as a former Department of Justice assistant director for security operations before taking senior positions at Mandiant and FireEye.

The good news, he says, is that a combination of factors now makes it possible for agencies to achieve much greater visibility into their networks—on premises and in the cloud—and also dramatically shortens the time it takes to detect and block potential threats.

ACHIEVING PERVERSIVE VISIBILITY

Regardless of where agencies are in their IT modernization efforts, the steady march to cloud services has forced them to transform the way they think about security.

While many federal agencies must still maintain statically defined perimeter controls, those controls are largely aimed at prevention rather than detection. Moving data and applications to the cloud—and also dramatically shortens the time it takes to detect and block potential threats.

Achieving that visibility remains both a huge struggle and an urgent need for most enterprises: 43% of cybersecurity professionals across multiple industries, including government, listed “visibility into infrastructure security” as a key pain point they’re currently facing, according to a 2020 Cloud Security Report from Cyber Security Insiders.

Comprehensive visibility into infrastructure security requires multiple forms of visibility simultaneously, according to Holste. That includes having:

- A complete inventory of all relevant assets at all times. Without both a current and historical inventory of all in-scope assets, compliance audits and security analytics will yield incomplete and/or misleading results.
● Contextual details on the current state of every asset. Without visibility into the context of any and every asset, and the ability to search for those details when necessary, there is no meaning and no validity to concepts such as compliance assurance and anomaly detection.

● The complete historical record of security events for each asset. Without visibility into the actual behavior of workloads and users, there is no way to confirm that governance policies are working or that nefarious actors don't already own part of your infrastructure.

According to Holste, the integrated FireEye Cloudvisory solution gives agencies the capability to probe more deeply across multiple cloud environments, as well as containerized workloads, for potential vulnerabilities and threats. It also works with a wide range of security technologies and all the leading cloud providers. And it provides users with automated controls and policy rules that can be delivered at machine speed so that agencies can continually adjust their security policies as their operations continue to evolve in the future.

Whenever a developer spins up a new cloud service, for instance, they should be able to easily centralize telemetry, giving analysts the ability to go to a single location to review the security status of all cloud services.

ADAPTING SECURITY TO A REMOTE WORKFORCE

Just when many enterprise security teams were getting used to managing security across distributed IT environments, they suddenly had to contend with a newly distributed workforce.

That's meant not only adapting their security monitoring and detection controls, to accommodate a surge in employees working remotely, but also having to perform those security functions remotely as well. Having a robust suite of analytics and detection tools—that can monitor and enforce security policies, detect new types of vulnerabilities, and that can distinguish between shifts in behavior versus unusual behavior—has become more important than ever.

Recent additions within the FireEye Helix analytics platform now make it possible, for instance, to more rapidly identify abnormal VPN logon behavior, according to Gregory Smith, Senior Product Marketing Manager at FireEye. Organizations embracing cloud productivity suites, such as Office 365, can baseline and detect unusual behavior automatically.

Responding to cyber threats, however, remains a complicated and increasingly complex business, Bushar says.

“It takes a combination of expertise and knowledge of the threat environment, on a real-time basis, as well as the IT infrastructure and the way it has evolved over time. Your information can't be months old, or weeks old anymore. And you also have to combine it with agility on the technology side and be able to work at scale,” he says.

He credits FireEye’s Mandiant Threat Intelligence division, which can identify which threat actors are most likely to take an interest in a given enterprise, for helping chief information security officers to sharpen their defenses. Additionally, Mandiant Security Validation gives CISOs instrumentation tools to help manage and report security risks to senior management and provide a clearer rationale for IT and security investments.

But the real goal, he says, is delivering visibility and insights in ways that FireEye customers can act on.

“If you talk to anybody who’s working in the threat Intelligence space,” observes Bushar, “the number one complaint isn’t that people aren’t providing enough intelligence. It’s that they’re providing too much. But the second thing they say is, ‘I either can’t consume it in a way that is useful to me,’ or they don’t know what to necessarily do with the information. What we’re trying to do now with our intelligence function is to get beyond the human-readable reporting, which is still useful, and apply that intelligence at machine speed... but doing it in a way that actually enables proactive and predictive analysis.”

But at a high level, we’re really trying to enable, in the fastest and most seamless way possible, everything we know and learn about adversaries—their tools, their techniques, their motivations and their intent—and get that to our customers in the way that they want to consume it—at machine speed,” Bushar says.

Learn more about the complete suite of FireEye detection, protection, and response capabilities. That includes Network, Endpoint, and Email, and Cloud security solutions under a security operations platform, Helix. The ecosystem also includes a security instrumentation platform, Mandiant Security Validation, which continuously measures, tests, and improves cyber security effectiveness. Finally, Mandiant Consulting, Managed Defense, and Threat Intelligence services augment organizations with the resources and knowledge necessary to respond to and protect organizations against the most advanced threats.