Get Ready for Next-Generation Endpoint Security

November 16, 2015

Cyberattacks against endpoints remain one of the most popular techniques used by the bad guys. The ongoing strategy of gaining unauthorized access to sensitive data by compromising network edge devices continues to grow. And stopping these new cyberthreats can be extremely difficult.

What are these new cyberthreats and how can they be stopped? The Ponemon Institute issued this white paper describing the State of the Endpoint in 2015 – which covers both end user and endpoint (device) risks. Here's a brief excerpt to help:

"Negligent employees are seen as the greatest source of endpoint risk. The primary reason for the difficulty in managing endpoint risk is negligent or careless employees who do not comply with security policies.

This is followed by an increase in the number of personal devices connected to the network (BYOD), employees' use of commercial cloud applications in the workplace and the number of employees and others using multiple mobile devices in the workplace.

This year, mobile endpoints have been the target of malware. Seventy-one percent of respondents say in the past 24 months managing endpoint risk has become very difficult. In fact, 75 percent of respondents (an increase from 68 percent in last year's study) believe their mobile endpoints have been the target of malware over the past 12 months.

In recognition of the growing risk, endpoint security is becoming a more important priority. Sixty-eight percent of respondents say endpoint security is becoming a more important part of their organization's overall IT security strategy.

Mobile devices, such as smart phones, have seen the greatest rise in potential IT security risk in the IT environment. Eighty percent of respondents say smart phones are a concern followed by vulnerabilities in third party applications (69 percent), mobile remote employees (42 percent) and the negligent insider risk."

In order to take on this difficult task, a new category of security protection has emerged which is commonly called "Next-generation endpoint security."

Another Network World report pointed out this summer:

"Rather than looking for signatures of known malware as traditional anti-virus software does, next-generation endpoint protection platforms analyze processes, changes and connections in order to spot activity that indicates foul play and while that approach is better at catching zero-day exploits, issues remain.

For instance, intelligence about what devices are doing can be gathered with or without client software. So businesses are faced with the choice of either going without a client and gathering less detailed threat information or collecting a wealth of detail but facing the deployment, management and updating issues that comes with installing agents. ..."

As we entered 2015, security experts listed endpoint intelligence and user behavior analytics as two important trends to watch this year.

"With the recent evolution in the threat landscape in mind, 2015 will see the emergence of the next generation of endpoint protection products. We know the need exists and security vendors are starting to respond. Existing endpoint protection products, like anti-virus, may serve a purpose, but we know that they are not effective against all the components of today's advanced attacks. The key to success for this next generation of products will be applying intelligence gathered from previous attacks and combining this with incident response best practices to provide an enhanced level of detection and protection. ..."

A just-released report surveying endpoint security across the federal government highlighted some alarming lapses. The study from MeriTalk and Palo Alto Networks, called " Endpoint Epidemic," found that 44 percent of endpoints are unknown or unprotected and barely half of federal government employees have taken critical steps to secure endpoints, such as scanning for vulnerable/infected endpoints.

The summary from MeriTalk raised several serious areas that need to be addressed: "

"In reviewing the proactive steps Feds are taking to prevent, detect and mitigate endpoint threats, several areas of concern emerged. First, securing the endpoints – 80

percent of Federal IT managers say they don't micro or virtually segment endpoints and 59 percent don't employ real-time patching for high priority vulnerability disclosures. Second, securing the network from unknown files – just 28 percent have identified dubious files from endpoints. Third, ensuring the network is protected contextually by user, application and devices; half of Federal IT managers say their agency isn't taking key steps to validate users and apps. And, fourth – personal devices; less than half of Federal IT managers say their agency requires employees to register the personal devices they use for work. These same devices are then used for "risky" behaviors such as uploading work documents to a cloud app.

And the situation is not much better in the private sector. ITbusinessedge.com recently reported:

"A Promisec survey revealed that the situation isn't any better in the private sector – and is actually getting worse. The survey found that only 32 percent of security professionals admitted to having advanced endpoint security in place, which is lower than last year's 39 percent. The Street discussed an increasing number of respondents (73% this year vs 58% last year) consider endpoints to be "most vulnerable" to a cyber-attack. Although more respondents recognize that endpoints are vulnerable to a cyber-attack, fewer companies today said they have endpoint protection in place compared with last year."

Solutions Please

Another Network World report listed "six pillars of endpoint protection"i that are needed against the latest cyberattacks on our endpoints. They include:

- Prevention
- Dynamic Exploit Detection
- Dynamic Malware Detection
- Mitigation
- Remediation
- Forensics

And there are many vendors who have jumped into this space, in addition to traditional vendors who have realigned their offerings. Dark Reading offers this analysis:

A wave of next-generation endpoint security startups have come out of stealth in the past year or two including Cybereason, enSilo, Hexis, SentinelOne, Tanium, Triumfant, and Ziften. Venture capital firms are all over this space, too: endpoint security startup Tanium is now valued at a whopping $3.5 billion, topping all venture-backed cybersecurity firms worldwide. Tanium, which boasts Target, Visa, NASDAQ, and Verizon among its customers, tipped the scales last month when it secured an additional $120 million in VC from TPG, Institutional Venture Partners, T. Rowe Price, and Andreessen Horowitz.

The startups join existing security firms that focus on various approaches to advanced endpoint protection such as Bromium, Cisco Systems, Cylance, CrowdStrike, Mandiant,

Bit9/Carbon Black, CounterTack, ForeScout, Invincea, and Palo Alto Networks, RSA Security, Tripwire, and others.

Tanium makes the bold claims of:

- 15-second visibility and control over every endpoint, even across the largest networks.
- 10,000 times faster than any endpoint tools you have today – 5,000 or 500,000 endpoints – it doesn't matter.

Bit9/Carbon Black meanwhile boasts that it is:

- The Top Choice of Security Professionals
- #1 In Endpoint Protection.
- #1 In Incident Response.
- #1 in Market Share.

Wrap-Up

One thing is clear as we head into 2016: Endpoint security is again a very hot security marketplace – by whatever name you want to use. More solutions are becoming available in the "next-generation endpoint security" market, and different approaches are offered to solve different problems. Get ready for another round of consolidations in 2016, and this end user space becomes even more crowded.

At the same time, I urge security leaders to take a new look at these developments. Visit the company websites and get demos of product offerings at security and technology events. The market is rapidly evolving and the new problems and innovative solutions are real.

http://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-you-need-next-generation-endpoint-security.html