STRONGER ENDPOINT SECURITY

FOUR TRENDS TO CONSIDER WHEN IMPROVING YOUR DEFENSES

JANUARY 2017
GOOD ENDPOINT SECURITY IS KEY TO BUSINESS SUCCESS

Professionals who are responsible for security are under pressure to protect their organizations from sophisticated cyber threats. A lot of security staff focus most of their attention, manpower and resources on network security. But this approach often forgets the primary point of entry and the most vulnerable systems to any attack — endpoints.

Because endpoints are most often the key entry point of attacks, providing extensive visibility into endpoints makes them a valuable source of threat data. The number of endpoints and their external exposure in any organization and the data they can provide make them a critical element to overall network security.

Several emerging trends can impact how a security team formulates their overall security strategy for endpoint protection:

• The number of endpoint devices continues to grow
• An insufficient application of machine-to-machine protection
• Misconfigurations and employee mistakes continue to contribute to breaches
• The number of IT security professionals continues to fall behind demand
THE NUMBER OF ENDPOINT DEVICES CONTINUES TO GROW

In today’s organizations, data is no longer restricted to traditional enterprise security perimeters. Security teams often have limited visibility into the devices that employees use, and those devices often lack fundamental security protections.

Almost all employees use their own devices for both personal and professional activity. And they tend to use multiple devices — from laptops and smartphones to tablets — giving would-be attackers an even greater multitude of available targets. Defenders must then try to protect an ever-increasing number of systems.

The growth of the endpoint attack surface means that there is an ever-greater risk of enterprise data being compromised. And locking essential data down is more important for the success of the enterprise.

Organizations believe that as much as 45% of all their corporate data is held on endpoint devices such as laptops, tablets and smartphones — which pose arguably the largest risk to data security.¹

Close to 80% of workers claimed to have used multiple devices to achieve objectives while on the job.²

According to the 2016 Datastrophy Study, 80% of IT decision-makers believe protecting data is vital to their brand/reputation — with a further 83% saying its loss would be seriously disruptive or business-destroying.³

1 Arieanna Schweber (April 14, 2016). “45% of Corporate Data is Held on Endpoint Devices, Often Unprotected.”
3 Arieanna Schweber (April 14, 2016). “45% of Corporate Data is Held on Endpoint Devices, Often Unprotected.”
An objective of endpoint security has always been to stop known threats before they get into a network. This has traditionally been done with AV and anti-malware solutions and managing user activity and account access.

Machine-to-machine activity increases the available threat surface. It also tends to have less direct protection due to limited capacity and unique use characteristics. This makes it more difficult for security teams to monitor and detect unauthorized activity between non-user endpoint systems.

An example of machine-to-machine systems would be General Electric (GE). GE places up to 250 sensors in each of the 5000 turbines it uses to generate energy for customers around the country. These sensors use machine-to-machine communications to generate and send data in real time to a centralized monitoring facility where GE looks for issues such as proper temperature levels on the bearings and vibration and exhaust. If the readings fall outside of a prescribed level, GE can perform a pre-emptive fix.¹

GE ensures that their operations run smoothly by monitoring these sensors and quickly detecting and responding to any suspicious or unauthorized activity.

As a security team formulates any endpoint strategy, they need to consider machine-to-machine activity. This includes POS (Point of Sale) and other devices where their interactions can increase the overall attack surface.

Read more about machine-to-machine communications >

By 2020, there will be more than 12 billion global machine-to-machine connections (up from 4.9 billion in 2015)
Todays attacks are well-crafted and targeted, and frequently delivered as a spear-phishing email. These targeted efforts can deceive the most sophisticated and trained user, causing significant financial, brand and operational damage to organizations. Regardless of security systems and determined efforts to continually train users — all it takes is one busy employee to click on a spear-phishing email to unleash a targeted attack.

To help reduce risk from targeted attacks, training your employees to have a basic understanding of security — and to know that not every email can be trusted — has to be an ongoing activity. Unfortunately, even with the best of intention and constant training, it can never be 100% effective. However, training employees to look for tell-tale signs of a spear-phishing email can help reduce organizational risk.

Areas of discrepancy that can be reviewed that can highlight or distinguish the differences between a spear-phishing email vs ‘good’ email

- “From” line: Do you know the sender and does the sender email address look legit?
- “Subject” line: Does the subject line make sense given the content of the email?
- Bit-mapped logo or brand marks, misspellings, poor grammar and punctuation anywhere in the email
- Examine embedded URLs more closely to look for strange words or phrases

84% of organizations said a spear-phishing attack successfully penetrated their organization in 2015. The average impact of a successful spear-phishing attack is $1.6 Million. Spear-phishing victims saw their stock prices drop 15%.

Companies used to rely on signature-based products such as antivirus software to automatically protect their endpoints from cyber attack.

New attacker methodologies enable a constantly evolving breed of cyber attacks called advanced persistent threats (APTs). Unique APTs can be created and used to craft attacks that circumvent automated signature-based defenses.

Because attackers can bypass baseline security measures, organizations must have a stronger security solution. In addition to point products, organizations need IT security professionals. These experts must be able to continually monitor and proactively investigate their endpoints for suspicious activity.

Not having enough IT professionals mean it’s difficult for organizations to reduce the time they take to detect, respond to and remediate cyber attacks vital to their continuity and success, especially as the average cost of a breach continues to rise.

“The 2016 Cost of Data Breach Study from IBM and the Ponemon Institute put the average cost of a data breach at $4 million.”

On average, it takes companies nearly 3 months (80 days) to discover a malicious breach and then more than 4 months (123 days) to resolve it.

“Depending upon whom you believe, there will be 1 million or more cybersecurity job openings that remain unfilled in 2016. This shortage is already a problem for CISOs, look for it to become a growing headache for cybersecurity product and (especially) services vendors this year as well.”

– Jon Oltsik, ESG

6 Ponemon Institute, LLC (June 2016). 2016 Cost of Data Breach Study: Global Analysis.
7 Ibid.
8 Jon Oltsik (January 5, 2016). "Cybersecurity Industry Predictions for 2016."
EXECUTIVE SUMMARY

Protecting and defending every endpoint in your network is a significant challenge for as organizations of any size, whether large or small — and across all industries. Some organizations rely on traditional endpoint security solutions — but these solutions only protect endpoints from specific, known signature-based attacks.

Organizations need to address the need to:

1. With the continued growth of endpoints, existing staff need better visibility into all endpoints
2. Improve Machine-to-Machine protection with advanced network and endpoint threat detection and visibility
3. Continue to educate, at the same time, have the means to more quickly discover and minimize the impact of users mistakes
4. Improve existing staff capabilities with comprehensive tools and threat intelligence

Learn more about how FireEye Endpoint Security can protect your endpoints — and your network — from advanced threats.
ABOUT FIREEYE, INC.

FireEye® is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 825 of the Forbes Global 2000.