Virtual Patching: The protective shield for vulnerable systems

Virtual patching closes off weaknesses to the malicious actors in the shortest possible time

DOES THIS SOUND FAMILIAR?

Patching servers is complex. Before you install a patch, you must thoroughly test it. This requires time you don't have since your IT department is already overburdened. The industry standard urgently recommends that you need a rollback process if a patch causes problems.

Oftentimes, security gaps remain open over longer periods until an employee finds time to look after them and updates for some legacy systems are no longer available because the end of support is long past. Also, some medical technology devices cannot be patched because they would no longer function properly afterwards. Therefore, although you cannot afford open weaknesses, you are forced to live with unpatched systems.

EASIER SAID THAN DONE

You can use a next-generation firewall (NGFW) or an intrusion detection/intrusion prevention system (IDS/IPS) to try to defend against attacks as best possible at the network level before they reach the vulnerable systems. Unfortunately, there are a couple of problems with this approach.

NGFW and IDS/IPS solutions generally use exploit filters to block attacks. One filter is valid for a specific exploit in each case. However, since cybercriminals continuously develop new methods for utilizing weaknesses, the security system needs more filters, increasingly slowing it down.

New exploit filters are often developed under a lot of time pressure; therefore, they do not fit precisely, and they send more alerts than needed to be on the safe side. With each new filter added, the number of false positive alerts increases, making life even more difficult for the security team.

Since exploit filters never entirely cover a weakness, there is residual risk that the security system will miss attacks and the weaknesses will be utilized.

WHAT NOW?

You need an IPS solution that uses virtual patching. This technology does not look at the individual exploits, but at the weakness, and completely covers a weakness to protect it from future exploits. The security solution looks the same as before from the outside, but the weakness can no longer be utilized by cybercriminals.

Ideally, a virtual patch should be available as soon as possible after a weakness becomes known. Trend Micro™ Zero Day Initiative™ (ZDI), the world's largest bug bounty program, detected 60.5% of worldwide known vulnerabilities thanks to the help of independent security researchers from all over the world.

Virtual patching based on ZDI data can close off weaknesses that aren't published yet, providing customers with a valuable head start. Find out more about current weakness research from the **Omdia Research white paper**.

TREND MICRO TIP

IPS with virtual patching can already defend against a large share of attacks at the network level, reducing the load on subsequent security systems. They can then catch the threats that still get through. It is worthwhile to invest into a reliable solution with extended Detection and response (XDR) capabilities, which collect reports from all connected security systems, filters out the relevant ones, and correlates them into usable warnings. Learn more about the XDR payoff in the **ESG Research report**.

WHAT WE CAN DO FOR YOU

- Protect even unpatched legacy systems and medical technology without having to touch their software.
- Automatically protect you within 24 hours after a weakness becomes known. For weaknesses that are first found by the ZDI, select solutions provides an average of 81 days of extra coverage compared to other methods.
- Immediately close off critical weaknesses before a manufacturer's patch becomes available.
- Less false positives alerts compared to NGFW and IDS/IPS systems with exploit filters.

TRUSTED CYBERSECURITY PARTNER BY YOUR SIDE

Virtual patching is included in several Trend Micro solutions. Trend Micro is ranked #1 in **Gartner IDPS Market Share worldwide with 23.5% share for 2020**. According to Omdia, the ZDI has been the leading provider in global vulnerability research and discovery since 2007.

Trend Micro (listed on the Tokyo stock market) has over 30 years of experience as a security solutions specialist. The company has been successfully managed for 15 years by its co-founder Eva Chen, internationally recognized as a leading woman in IT. Since its founding in 1988, Chen and her management team have ensured that the company has grown healthily and reinvests extensively in research and development, even in times of crisis.

Her motto: "Our only competition is cybercriminals, who must be stopped."