SOLUTION BRIEF

Virtual Patching with Morphisec

Industry best practices demand patching software vulnerabilities as soon as a patch is released, in order to shorten the time period in which the organization is at risk. But industry surveys show that IT organizations are overburdened with patches, and many IT administrators admit they simply can't keep up. A recent Ponemon study found that nearly 60% of data breaches were caused by exploiting a software vulnerability that was known, but which the victim organization had not yet patched[1].

Patch Management

Patch management is the process of acquiring, testing and installing updated software. Unfortunately, many organizations find themselves adhering less than strictly to their patch schedule. The reasons for this failure are numerous.

QUANTITY

The sheer number of patches released across an organization's typical software stack is overwhelming. For example, consider the number of released security patches in 2015 across a small sample of installed applications:

- Windows 7: 120
- Adobe flash: 13
- Internet Explorer: 13

If we take 2015 as a representative year, looking at this set of patches, which is just a subset of a standard endpoint software stack, an organization needs to patch 146 times a year; an average of a patch every 2.5 days. This is simply not feasible.

COST

Time is money, and patching takes time. You also have the costs of system downtime and productivity loss, which can turn into more than just install and reboot time. Microsoft Azure and Office 365 users worldwide were locked out of their accounts after an update that affected the multi-factor authentication service[2]. And who can forget the patching mess as vendors rushed out unstable fixes after the Meltdown/Spectre bombshell.

ORGANIZATIONAL LAN

You can only patch systems that are inside the VPN, and not busily working at the time of the patching process. This means that your most vulnerable machines, ones belonging to employees that travel frequently, and that use dubious WiFi connections in coffee shops, will not be patched often, in the best of cases.

SCALE

Manual patching does not scale. Automatic patching requires you to review each patch carefully and assess its impact on your business, prior to deployment.

MORPHISEC VIRTUALLY PATCHES OS AND APPLICATION VULNERABILITIES

Morphisec keeps your business protected from vulnerability exploits when patches are not yet available or deployed.

- Reduces risk from unpatched vulnerabilities in your operating system and applications
- Cuts costs and disruption from patching
- No updating configurations or setting filters
- Works invisible to end user, with zero impact on operations
- Functions seamlessly across virtual, physical or hybrid IT environments

MORPHISEC
Moving Target Defense

[1] Source: https: //www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465

[2] Source: https: //www.tomshardware.com/news/microsoft-multifactor-authentication-locked-out,38164.html

Virtual Patching

The term virtual patching was originally coined by Intrusion Prevention System (IPS) vendors. It is the process of addressing a security vulnerability by blocking attack vectors that could exploit it. Various technologies can be used to shield vulnerabilities before they can be exploited. An organization can therefore be protected without incurring the cost and the operational pain of downtime for emergency patching, patching cycles, and of course, the added cost of breaches in an unpatched system.

NETWORK-LEVEL VIRTUAL PATCHING

Some vendors believe virtual patching can be implemented only by network solutions that perform packet inspection and matching to the database of known vulnerabilities. This is a reasonable approach if attacks exploiting vulnerabilities had a single, known manifestation – but they don't. Additional problems with this approach are the performance hit associated with analyzing network packets and comparing them to a large number of signatures, and the resulting slowing of the network.

VULNERABILITY SCANNING

Other vendors use a combination of detection with vulnerability scanning. While this may work for known vulnerabilities, it leaves a gap in protection from the time a zero-day is discovered until the solution is updated to include it. And it does not help during the pre-discovery period – which can be months or years – at all.

Morphisec Virtual Patching

Morphisec's software covers endpoint vulnerabilities exposed by gaps in patching cycle.

PROTECTS UNPATCHED VULNERABILITIES

Morphisec instantaneously prevents attacks on unpatched operating system and application vulnerabilities. Patented Moving Target Defense technology dismantles the attack pathways so the targeted vulnerability can't be exploited. Morphisec's prevention capabilities do not depend on updates or patch availability; protection is in place even before a vulnerability has been discovered and a patch developed. Consider the Flash vulnerability CVE-2018-4878. It was used in attacks for nearly four months before it was discovered, reported and a patch developed. Morphisec's virtual patching covered the vulnerability from the moment an attack was created.

REDUCES PATCHING COSTS

With Morphisec, organizations can extend their patching cycles yet reduce risk. IT departments are able to implement patching schedules that cause fewer business disruptions and require fewer resources. And emergency patching is essentially eliminated. For example, Morphisec customers did not have to rush to implement the very problematic patches for the Meltdown and Spectre CPU vulnerabilities, as they were protected against any code execution that follows from these vulnerabilities.

SAFEGUARDS OPERATIONS

Morphisec uses a tiny 2 Mb agent with no runtime components and zero impact on endpoint performance. It operates invisibly to the end user, with no interruptions for updates or scans.

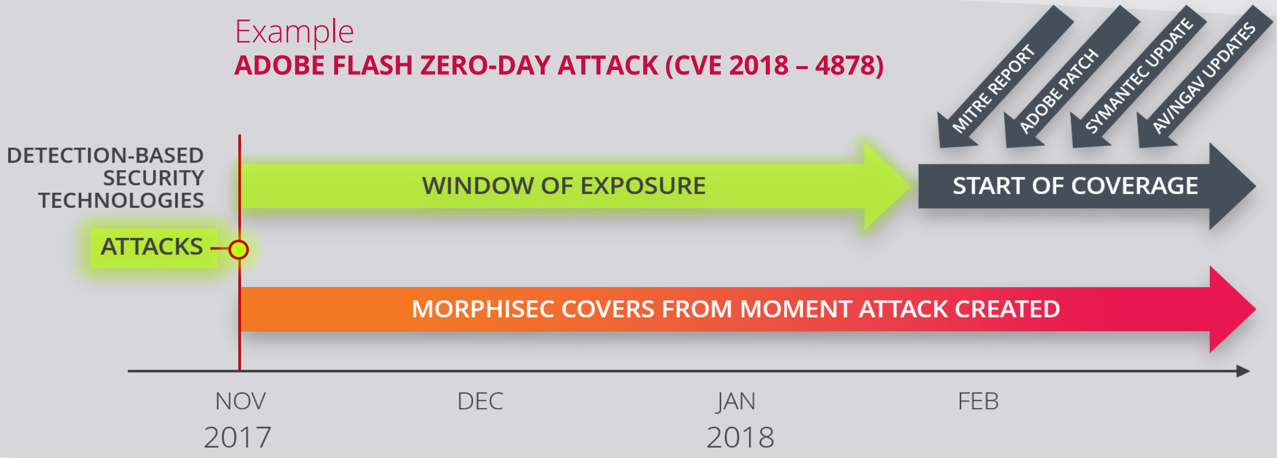
WANT TO LEARN MORE ABOUT

Virtual Patching with Morphisec?

SCHEDULE A DEMO: DEMO@MORPHISEC.COM

Example

ADOBE FLASH ZERO-DAY ATTACK (CVE 2018 – 4878)



MORPHISEC
Moving Target Defense

www.morphisec.com
+1 617-209-2552