EBOOK

GETTING STARTED WITH VULNERABILITY MITIGATION

MANAGE THREATS IN PLAIN SIGHT

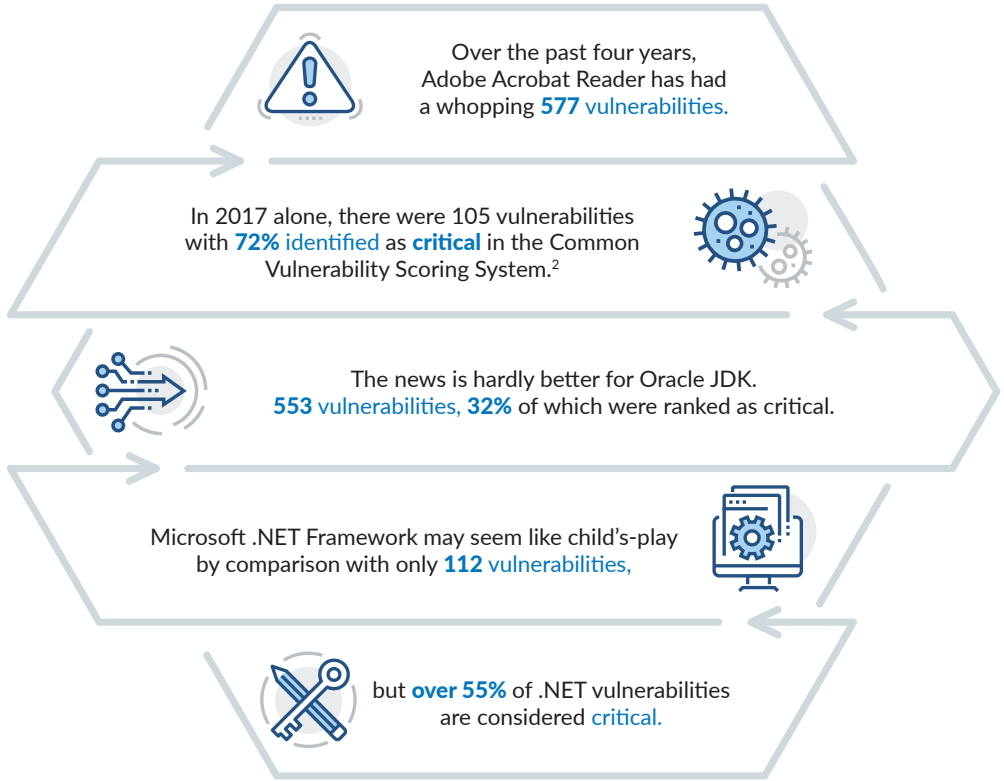
Vulnerability Mitigation Begins with Managing Threats in Plain Sight

Three common types of software make you more vulnerable than you realize. With a few simple steps you can change this. Here's how.

Top 3 Vulnerable Applications[1]

1. Adobe Acrobat Reader DC
2. Oracle Java SE Development Kit (JDK)
3. Microsoft .NET Framework

An IT administrator would be hard-pressed to find a network without applications derived from these three types of software. All three are pervasively used, and they far more vulnerable than many realize. Worse yet, these three applications are only the tip of the iceberg, and just a small sample of a much larger world of vulnerable third-party software.



The hidden threat in securing your infrastructure from vulnerabilities lies with IT's difficulty in managing third-party software.

2017 was billed as the worst on record[3] for cybersecurity. No doubt, the continued rise of modern threat vectors has IT on high alert. In essence, IT professionals view their role as responsible for keeping the door shut. However, even with IT administrators keenly aware that most exploits can be averted simply by keeping the environment current, the task is no small feat and often isn't done as well as it needs to be.

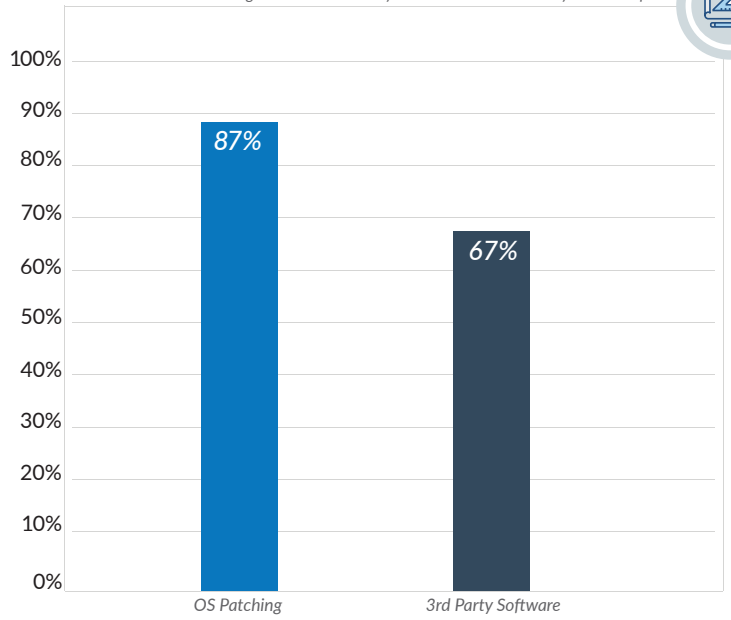
Unfortunately, complete and thorough vulnerability management is next to impossible for a number of reasons. First, the sheer volume of vulnerabilities to accept, reject, or manually review is overwhelming. There is virtually no way to systematically go through all of them on a timely basis. So, IT prioritizes the work by what seems most critical. And as a result, much of its focus is often on Microsoft.

Percentage of IT Organizations Offering Software Management Services by Type

As can be seen in Figure 1, the deference afforded to OS patching is clear. When it comes to patching, IT shops clearly focus their time and effort on securing the OS layer in their environment. Only two--thirds of IT shops spend any time managing third-party applications, and it is highly unlikely they are updated in a thorough manner.

The traditional thinking in IT is that securing Microsoft OSes equates to vulnerability control. IT is well entrenched in the culture of "Patch Tuesday" and "Windows Update," with technologies like WSUS widely used to optimize processes. Current operational best practices center almost entirely on automating the management of Microsoft patches. Dealing with Mac or third-party software is viewed as an afterthought and an annoyance.

Figure 1 - Source: Kaseya 2018 Benchmark Survey Results Report



It's no wonder why. The processes for managing Mac OS and third-party software updates are entirely ancillary and require another set of tools. IT Administrators have to sort through different data sets to determine vulnerabilities and machines to patch, and then set up separate testing environments. Because OS type and software are managed separately, they require different workstreams. Further, these multiple workstreams interfere with the ability to automate the update process in a meaningful way. IT picks its battles, and in the end, some of the work simply doesn't get done, leaving the environment exposed.

Third-Party Software Updates Deserve Serious Attention Now

Why change the approach to patch management now? In short, because the patching game is changing quickly and criminals go where the money is.

The old approach to patching and lifecycle management no longer works. For example, support for Windows XP ceased in 2014, and Microsoft emphatically warned it would no longer backport fixes to ward off zero day attacks. In essence, Microsoft told the world that organizations would be swimming at their own risk if they chose to use retired software. And then, in 2017 the world got a wake-up call when WannaCry and Petya ransomware attacks loaded the EternalBlue on a global scale in a matter of days. The sheer scale of the attack motivated Microsoft in an unprecedented move to release critical updates for Windows XP, Windows 8, and Windows Server 2003 – all long since discontinued.

Perhaps Microsoft saw the writing on the wall. In Windows 10 it introduced a significant shift in its lifecycle management program. According to Microsoft a "device needs to install the latest version (feature update) before [the] current version reaches end of service to help keep your device secure and have it remain supported by Microsoft."[4]

The shortened lifecycle allows Microsoft to develop faster. However, to minimize the number of unsupported OSes, Microsoft introduced an automatic update strategy where the latest Windows version is downloaded and installed automatically by the old OS. While IT administrators tell tales of the chaos the auto-install and -update approach introduced, the move aimed to further secure the OS and minimize it as an entry point for hackers.

Apple uses a similar strategy for MacOS.

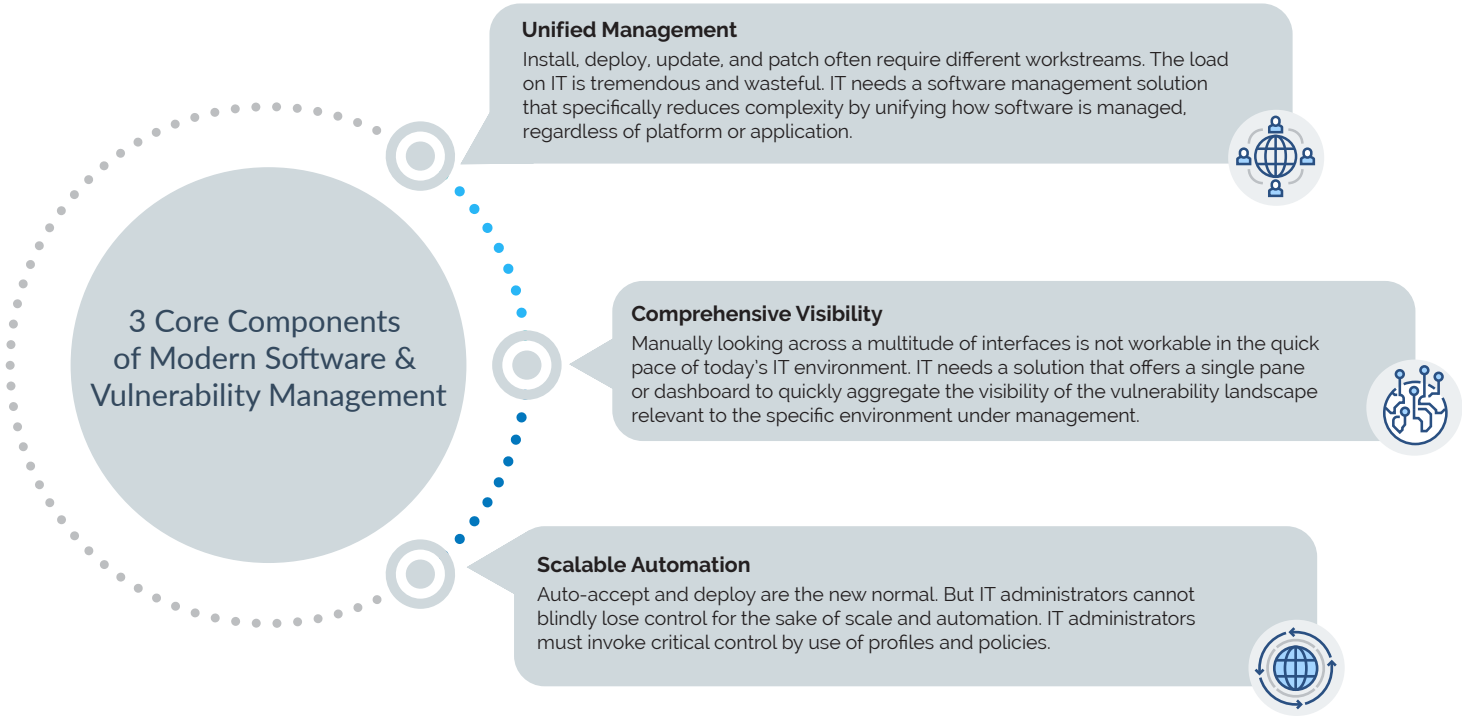
However, criminals do not sit still. They know that as the OS becomes a less viable means to wreak havoc, they need to shift their focus. And they know that third-party software presents a gaping hole that IT administrators have challenges managing.

Hence, the time is now for IT to shift its approach to holistic vulnerability management, and that strategy must include Windows, Mac, and third-party software.

Evolve away from Patch Management toward Software and Vulnerability Management

IT must expand its thinking to include comprehensive management of vulnerabilities across all Windows, Mac, and third-party software.

Updating Adobe Acrobat Reader DC, Oracle JDK, and Microsoft .NET Framework is a great first step to better secure your world. But that is only the beginning. The right approach is to modernize your software and vulnerability management strategy.



Recommended Best Practice

Auto-accept ALL patches and updates and minimize exceptions

Get Started Today The time to get started with a modern software and vulnerability management strategy is now.

Contact Kaseya to learn how we can help you transform your approach.

Page 2, 3, & 4:
1 Reference: Data extrapolated from https://www.cvedetails.com/index.php

2 Critical is defined as a 9 or 10 in the CVSS
Common Vulnerability Scoring System, CVSS, is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability. For additional information on CVSS v2, please see http://www.first.org/cvss and http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

3 https://www.pcworld.com/article/3243108/security/biggest-hacks-security-breaches-2017.html

4 https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

About Kaseya

Kaseya is the leading provider of complete IT management solutions for managed service providers (MSPs) and midsized enterprises. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage and secure IT. Offered both on-premise and in the cloud, Kaseya solutions empower businesses to command all of IT centrally, easily manage remote and distributed environments, and automate across IT management functions. Kaseya solutions manage over 10 million endpoints worldwide.Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

04092018