AVOIDING
PATCH DOOMSDAY

BEST PATCH MANAGEMENT PRACTICES

syxsense™

THE PATCH MANAGEMENT IMPERATIVE

Nearly every business in the world today depends on IT to support day-to-day operations and deliver products and services to customers. Core business processes within accounting, manufacturing, sales and other functions rely on the performance, availability and security of IT systems. Similarly, employee productivity depends on basic IT services such as email, Internet connectivity, and website access.

It should be no surprise that IT problems of any kind can have a negative impact on business success. At the same time, it can be shocking to learn that unpatched operating systems and application software are often responsible for the most IT problems.

Patches that resolve these problems are available—**they are simply not being applied**.

In April 2015, the United States Computer Emergency Readiness Team published an alert regarding unpatched software. It stated that cyber-threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations, and that as many as 85 percent of targeted attacks are preventable through patching. Many of the specific patches called out in the alert relate to not just the Windows operating systems, but third-party applications and tools that run on the OS.

Unpatched applications and systems not only expose security risks, they also open the door to data loss and corruption, as well as performance and availability issues.

Unfortunately, it is all too easy for software to become sufficiently out of date with patches that businesses face Patch Doomsday. When this crisis occurs, IT problem rates dramatically spike and remain high while IT struggles to return systems to compliance. To greatly reduce all of these issues and avoid Patch Doomsday, it is important for every organization to implement a strong patch management process.

PATCH MANAGEMENT

CHALLENGES

Patch management is a comprehensive process that involves identifying, prioritizing, acquiring, installing, and verifying patches and updates. But the implementation of a robust patch management process presents a number of its own challenges, particularly when performed manually.

IDENTIFICATION & PRIORITIZATION

IT professionals need reliable methods to identify and prioritize patches. Without this, it is easy to miss or delay the installation of important updates designed to prevent performance, availability or security problems.

TIME & RESOURCES

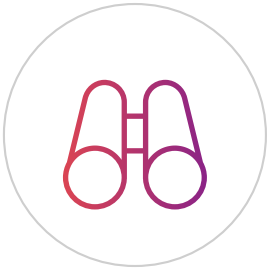
When a patch management process is implemented improperly, IT professionals lose precious time, preventing them from working on activities that add significant business value.

SPEED & SCALE

The moment patches are published, hackers begin seeking ways to exploit any related vulnerabilities in unpatched systems. This makes it crucial to apply all high-priority security patches as quickly as possible.

SCOPE

Vendor-specific tools such as Microsoft Windows Update do not address the full breadth of software that must be patched. Applications, plugins and tools from other vendors must also be patched regularly. For example, relying only on Windows Update will not keep users safe from Adobe security vulnerabilities.



VALIDATION

The right patches must be chosen carefully and tested for compatibility. If patch installations fail, systems may be left in an even less-desirable state than prior to patching.

FIVE WAYS TO OVERCOME THESE CHALLENGES:

- **Timely notification about the availability of new vendor patch releases**
- **Accurate and detailed information on the configuration of all your endpoints**
- **A mechanism for determining which patches are required for your environment**
- **Best practices for performing patch management**
- **A tool or set of tools for automating patch management**

BEST PRACTICES FOR

PATCH MANAGEMENT

Patch management is an ongoing process. New patches must be applied on an ongoing basis in order to keep operating systems and applications up to date.

Keep in mind that you can't manage systems that you don't know exist. You will need a complete and up-to-date inventory of devices that are part of your environment or that can connect to your environment.

Since endpoint devices are often added, removed or reimaged, the only reliable way to maintain an accurate inventory is by using automated device discovery. Along with device detection, it is also helpful to group devices based on relationships such as site location or business function.

For each system in inventory, you will need a detailed patch assessment. For a Windows environment, existing patch levels must be determined for all relevant versions of Windows OS, plus relevant versions of Microsoft and third-party applications.

This involves scanning and auditing each device to determine which patches are already installed. For speed and accuracy, patch levels should be determined using an automated tool.

PATCH TODAY, GONE TOMORROW

To complete the patch assessment process, a patch management tool must also maintain an up-to-date feed of current patches from Microsoft and third-party software vendors. With this, a patch management tool can find the differences between existing patch levels and currently available patches from Microsoft and other software vendors.

With this understanding of current patch levels and available patches, a viable patch management tool can now help determine what additional patches should be installed on each system by considering the risk level associated with each missing patch. This way, missing patches can be ranked by importance. This solution should also be able to determine updates that have been made publicly aware or are being weaponized.

Over the past 10 years, the industry has been using an open standard for vulnerability assessment called the Common Vulnerability Scoring System (CVSS). It is an expertly assessed score based on the true nature of each patch or update.

CVSS scores range from 0 to 10. Vulnerabilities with a base score in the range of 9.0-10.0 are critical, 7.0-8.9 are considered high, while those in the range of 4.0-6.9 are medium and those in the range 0.1-3.9 are low.

UNDERSTANDING CVSS SCORES

The following table lists five updates and compares the vendor severity with the CVSS score. Notice that there are some discrepancies between the scores—each of these scores was given different ends of the severity spectrum. CVSS scores are considered more reliable.

UPDATE NAME	VENDOR SEVERITY	CVSS SCORE
CVE-2019-0787	Critical	High, 8.8
CVE-2019-1138	Critical	High, 7.4
CVE-2019-1214	Important	Low, 3.5
CVE-2019-1215	Important	High, 7.8
CVE-2019-1235	Important	High, 7.8

TABLE 1. VENDOR SEVERITY VERSUS CVSS SCORE

CREATING A BASELINE

With an accurate report of missing updates ranked by the most important, the next step is to create a baseline.

A baseline is a group of updates that you intend to deploy to each of your systems every month. The number of updates added to this baseline will vary from month to month and should include the most recent patches with the highest CVSS rankings.

Note in Table 2 that a new baseline is created each month and includes all the updates from previous months. This will allow any new systems you build, or any systems that are rebuilt, to automatically receive updates and catch up to the current baseline. This makes software compatibility testing easier because all systems will be at the same patch level.

Table 2 shows five new updates for each baseline. When getting started with continual patch process, it is best to begin with a small number of new patches and work upward over time.

Some organizations can successfully deploy 20 new updates in each successive baseline. A good way to do this is by increasing the number of new patches by two or three each month.

JANUARY	FEBRUARY	MARCH
Update 1	January	January
Update 2	Update 1	February
Update 3	Update 2	Update 1
Update 4	Update 3	Update 2
Update 5	Update 4	Update 3
--	Update 5	Update 4
--	--	Update 5

TABLE 2. MONTHLY BASELINES

Note that Table 2 shows five new updates for each baseline. When getting started with continual patch management process, it is best to begin with a small number of new patches and work upward over time. Some organizations can successfully deploy 20 new updates in each successive baseline. A good way to do this is by increasing the number of new patches by just two or three each month.

TESTING PATCHES

Before deploying any update, you should fully test it against appropriate systems. This means performing a set of tests on suitable systems that are representative of your IT environment. When choosing which machines to use for testing, administrators should remember the following important rules.

#1

DO NOT TEST ON
YOUR OWN MACHINE

If the patch fails or crashes your system, it could seriously delay the overall patch process. It is also difficult to troubleshoot and resolve the problems with the patch while using a broken system.

#2

CHECK UPDATE FOR AN
UNINSTALLER

If the update doesn't have an uninstaller, it may require a cumbersome, error-prone manual process to uninstall it. Any update that does not have an uninstaller should be initially deployed and tested by itself on a system that can be quickly rebuilt if needed.

PATCHING IN STAGES

Patches should be tested in stages across separate groups of systems. It helps to create logical groupings of devices so that patch deployment can be completed and verified for success on low-risk systems before moving on to the next logical group of systems.

STAGE 1:

VIRTUAL MACHINE

Review success of the installation

STAGE 2:

IT COLLEAGUES

Review the installation impact to end-user

STAGE 3:

SAFE SYSTEMS

Review installation impact to end-user and network

Performing each test with an open mind is crucial. If any issue occurs to your test systems, no matter how trivial it may seem, it should be investigated to resolution. Knowing that your updates are fully tested breeds confidence not only in yourself, but also in your colleagues.

While testing can take up most of the day, it is a vital step in the patch management process and should not be rushed.

DEPLOYMENT & REPORTING

With patch testing completed and all problems resolved, your patch management tool should make it easy to deploy your latest patch baseline across all target systems without disrupting end users.

When patches are deployed during the business day they can negatively impact end users. For example, if reboots are required there may be a significant loss of productivity.

A good patch management tool should have the ability to deploy patches overnight. It should utilize technologies like Wake-On-LAN to deploy required patches even when endpoints are asleep. It should also handle reboots and return endpoints back to their shutdown or sleep mode.

The final but critical step in your monthly patch process should be to report your success. It is important that management see the patch coverage for the entire environment. A leading patch management tool should allow you to easily create automated reports that quickly convey patch status.

It should support bright colors, timeline views and a security risk assessment to accurately gauge your company's existing vulnerability exposure. It doesn't hurt to share statistics about the success rate of your patches. The work you've put in to patch testing should be recognized.

CONCLUSION

IT problems of any kind can have a large negative impact on business success. Since unpatched operating systems and applications are often responsible for the majority of IT problems, it is crucial to have a solid patch management process. Without one, your company is moving down a path toward Patch Doomsday.

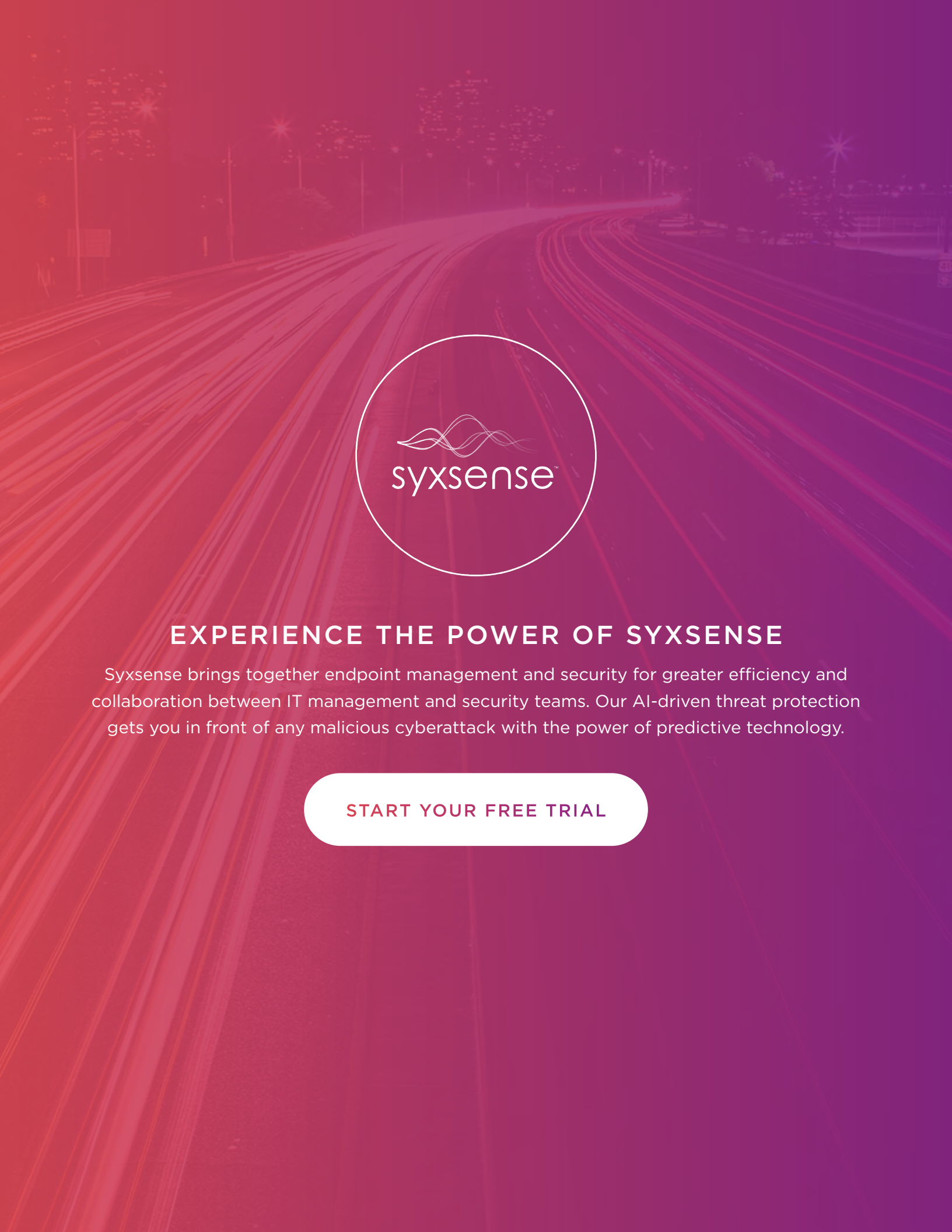
Patch management best practices are an important part of the solution. As outlined earlier, discovery and inventory management are important best practices that set the stage for patch scanning, assessment, ranking and baselines.

Patch testing, using appropriate systems across several stages, is also critical to ensure success. Reliable patch deployment and clear reporting round out the list of best practices.

Unfortunately, it isn't always easy to establish a trustworthy patch process, even with an understanding of best practices. Manual patch processes are time consuming, resource intensive and error-prone. Some automated patch management tools fall short, but it is always important to select a patch management solution that overcomes the key challenges in developing a patch management process.

A VIABLE PATCH MANAGEMENT SOLUTION SHOULD:

- Identify all devices that can access your network
- Determine existing patch levels
- Identify and prioritize new patches
- Reduce IT staff time spent on patching
- Manage your environment, including third-party patches



EXPERIENCE THE POWER OF SYXSENSE

Syxsense brings together endpoint management and security for greater efficiency and collaboration between IT management and security teams. Our AI-driven threat protection gets you in front of any malicious cyberattack with the power of predictive technology.

START YOUR FREE TRIAL

ABOUT SYXSENSE

Syxsense is the world's first IT and security-solution provider to offer patch management, vulnerability scans, and Endpoint Detection and Response (EDR) capabilities in a single console.

Syxsense has created innovative and intuitive technology that sees—and knows—everything, making it able to secure every endpoint, in every location, everywhere inside and outside the network, as well as in the cloud. Artificial intelligence (AI) helps security teams predict and root out threats before they happen—and to swiftly make them disappear when they do.

For more information about Syxsense, visit **syxsense.com**.

syxsense

www.syxsense.com

info@syxsense.com

(949) 270-1903