Key Actions to Mitigate Security Risk in Hybrid IT Environments

KACE by Quest

Introduction

The current cybersecurity threat landscape is both complex and ever-evolving. While mitigating threats has always been challenging for IT professionals, factors such as reliance on public clouds, BYOD, and remote work are making it much more difficult to keep cybercriminals at bay.

One of the most effective ways an organization can protect its IT resources is to adopt a comprehensive and aggressive patch management strategy. But a recent Check Point Research report noted that 75% of cyber attacks exploited vulnerabilities that were at least two years old. This shows that unpatched software remains an ongoing issue for IT professionals who are often challenged to keep pace with the sheer volume of updates required to maintain a positive security posture.

68%

OF ORGANIZATIONS HAVE EXPERIENCED ONE OR MORE ENDPOINT ATTACKS

Ponemon

97

DAYS ON AVERAGE TO APPLY, TEST AND DEPLOY A PATCH

71%

SAY IT'S EXTREMELY CHALLENGING OR CHALLENGING TO KEEP UP WITH THE FREQUENCY OF PATCH UPDATES

The Most Common Cybersecurity Vulnerabilities

If an organization is to remain secure, its IT staff must make a concerted effort to address security vulnerabilities as they are discovered. Some of the most common types of vulnerabilities include:

VULNERABILITY EXPLOITS

ZERO-DAY VULNERABILITIES

SHADOW IOT DEVICES

UNSECURED APPLICATIONS

SUPPLY CHAIN

SOCIAL ENGINEERING

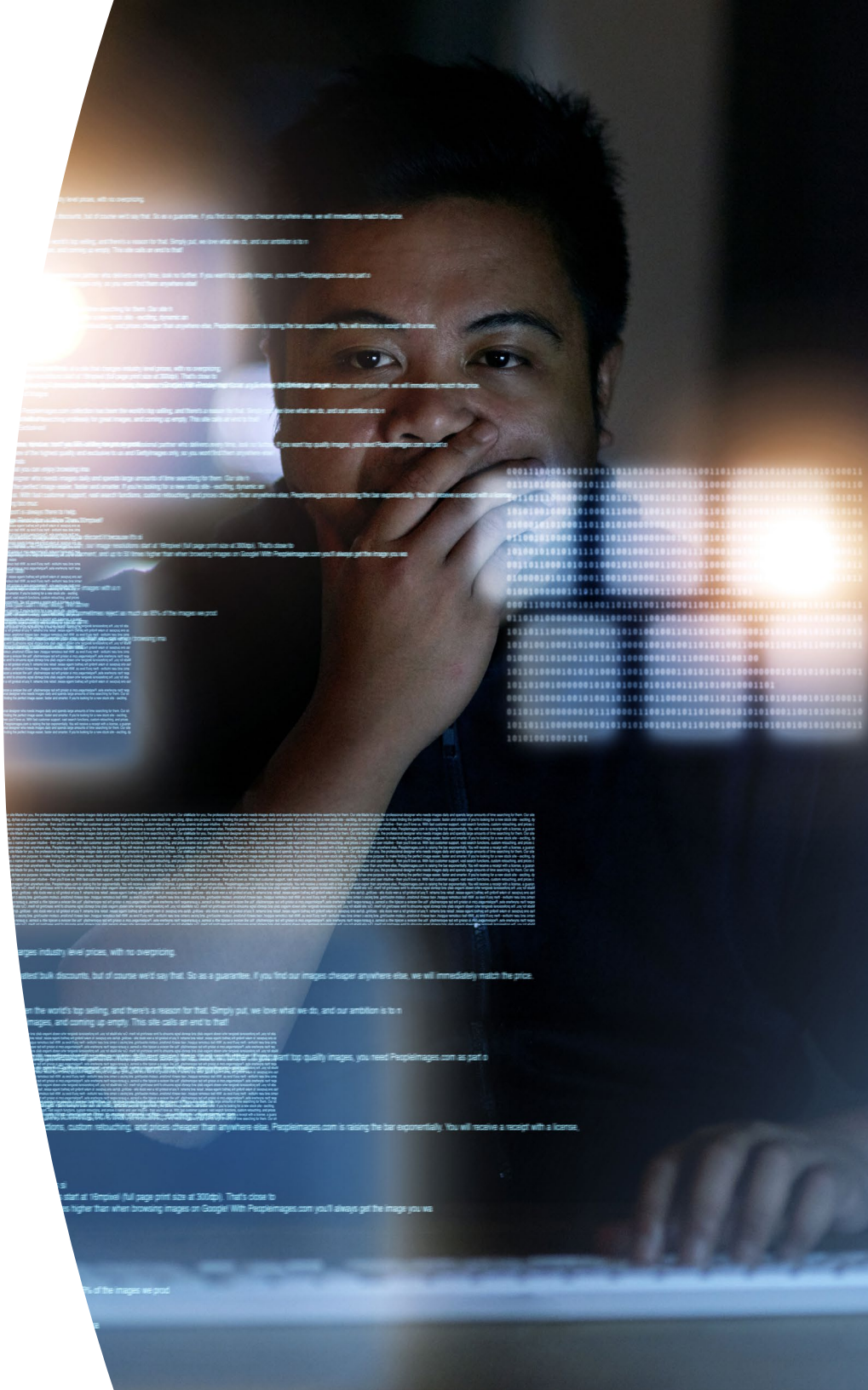
EMERGING THREATS FROM AI

While patching might not address every vulnerability, applying security patches as they become available can go a long way toward reducing the potential for breaches stemming from these vulnerabilities.

Beyond Vulnerabilities - Organizational Challenges in IT

As important as it may be for organizations to apply security patches in a timely manner, IT pros are faced with numerous challenges that can make it difficult to keep pace with newly released patches. Some of the biggest challenges standing in the way of effective patch management include:

- Difficulty patching 3rd party products
- An understaffed IT department
- Being overwhelmed with other day-to-day tasks
- The sheer volume of patches that software vendors release each month
- Unscheduled patch releases (such as Microsoft patches that come out at a time other than “Patch Tuesday”)
- Buggy patches and patches that are difficult to install
- Alert fatigue
- Software that automatically updates itself rather than relying on a centralized patch management solution, leading to a lack of accountability



The Challenge of BYOD and the Emergence of Remote/Hybrid Workstyles

The task of applying security patches to all network endpoint devices has always been challenging, but in recent years two trends have caused this task to become far more complex.

1. BYOD

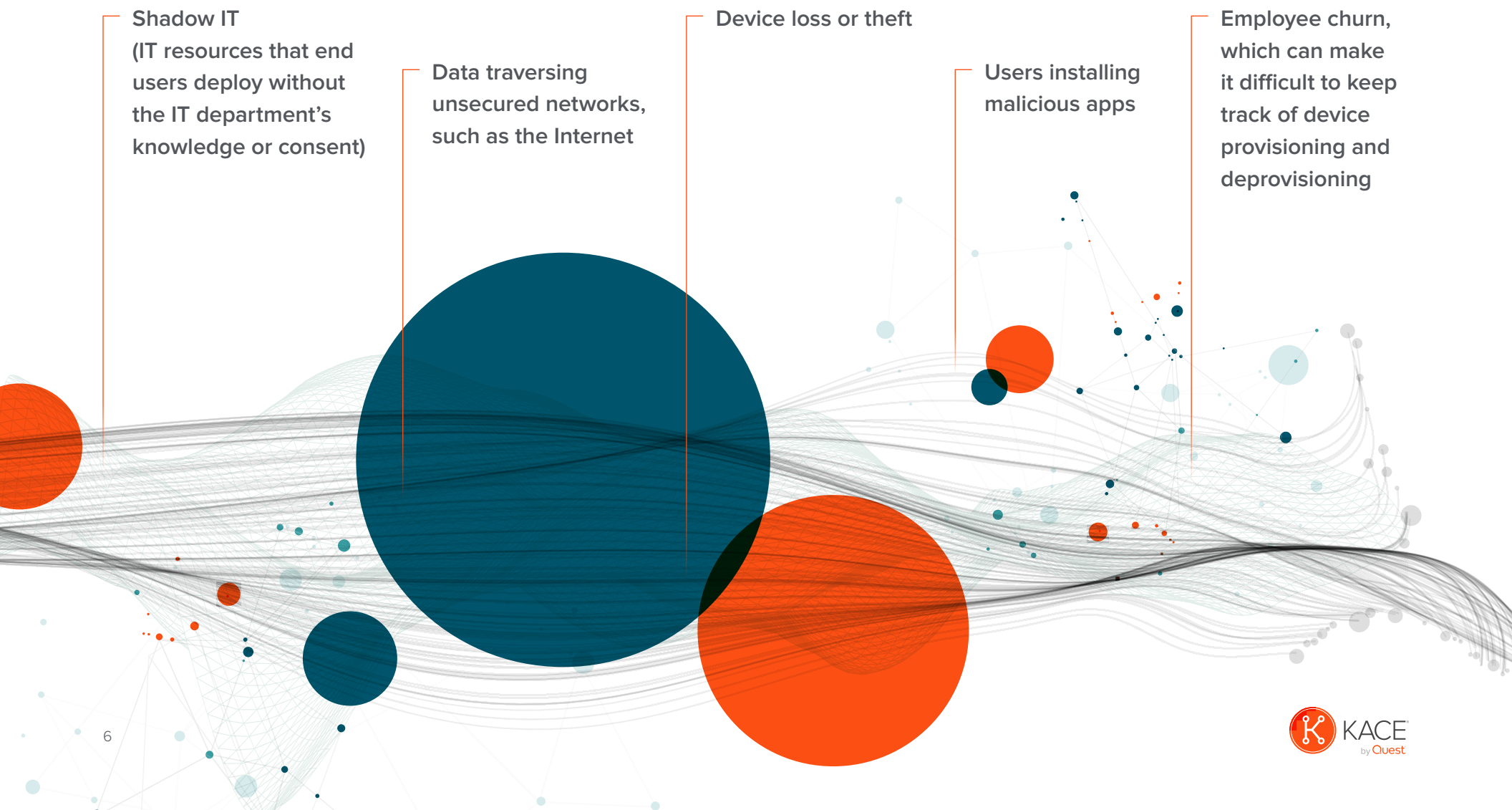
The first of these challenges is the BYOD trend. Because users are accessing sensitive resources from personal devices, any security deficiencies on those devices could potentially put the organization's data at risk. As such, the organization must have a strategy for patching (and for verifying the patching status) of any device that its users work from regardless of whether the organization owns the device or not.

2. Remote or Hybrid Work

The second challenge that tends to complicate patch management is the emergence of remote or hybrid work. Because users could potentially be working from anywhere, organizations need an endpoint management system that is location agnostic.

The Attack Surface Has Grown

Both the adoption of BYOD and remote or hybrid work actually point to a much larger issue facing organizations of all sizes. The organization's attack surface has grown exponentially in recent years and continues to grow. This means that there are a number of non-traditional threat vectors through which an attacker might gain access to an organization's sensitive IT resources. All of these potential threats point to the need for a cross-platform endpoint management solution:



KACE by Quest

Mitigating BYOD Risk

When users choose to work from personal devices, they can unknowingly put the organization and its data in harm's way. Personally owned devices need to be secured to the same level as corporate devices if they are to be used for accessing the organization's data. As such, there are four things that organizations should be doing right now to make sure that BYOD devices do not undermine their security efforts:

- Assess BYOD device health (and install any missing patches) prior to granting access to your network.
- Provide users with access to an enterprise app store containing secure network apps.
- Enable device location services, so that lost or stolen devices can potentially be recovered.
- Consider whether it is truly in your organization's best interest to allow BYOD.

Key Actions for Mitigating Risk Across the Organization

If an organization is to remain secure, it must proactively mitigate known security risks. Some of the key actions organizations can take toward risk reduction include:

ENDPOINT SECURITY PATCH MANAGEMENT	SECURITY TRAINING AND EDUCATION FOR END USERS	IMPLEMENTING POLICIES DESIGNED TO IMPROVE THE ORGANIZATION'S SECURITY POSTURE
MONITORING ENDPOINTS FOR SUSPICIOUS ACTIVITY	RESTRICTING ADMINISTRATIVE PRIVILEGES	FREQUENT DATA BACKUPS

The What and Why of Patch Management

While there are any number of things that an organization can and should do to help keep its IT infrastructure secure, patch management remains a central underlying theme — and for good reason. Security patches are designed to address known vulnerabilities.

Once a vulnerability is discovered, cyber criminals immediately go to work looking for a way to exploit that vulnerability. Criminals know that they only have a limited window of time before a patch vulnerability is released. However, these same criminals also know that some organizations will inevitably neglect to install the security patch, thereby making them vulnerable to attack so long as the patch is not installed.

It is worth noting that attacks against unpatched systems do not happen by chance. In many cases, cybercriminals will actively probe networks, looking for unpatched systems to attack.

The Value of Automating Your Security Defenses

The importance of ensuring that security patches are applied in a timely manner cannot be overstated. Even so, the previously discussed challenges such as an overburdened and understaffed IT department make comprehensive patch management difficult. The best way to overcome these challenges is for organizations to automate their security defenses. More specifically, organizations should work toward four goals:

1

STREAMLINE THE PATCH MANAGEMENT PROCESS TO MAKE IT MORE EFFICIENT AND LESS CUMBERSOME

2

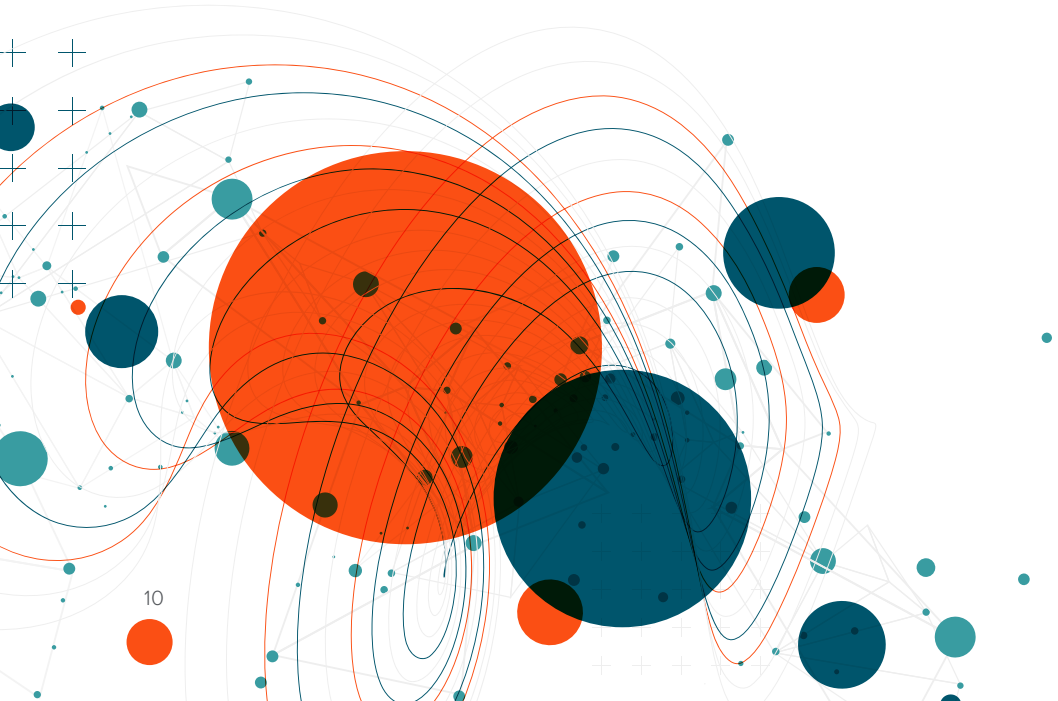
SIMPLIFY THE MANAGEMENT OF NETWORK ENDPOINTS

3

MAKE SURE THAT REMOTE DEVICES ARE JUST AS WELL PROTECTED AS LOCAL ENDPOINT DEVICES

4

AUTOMATE ENDPOINT SECURITY TASKS



KACE by Quest

KACE Cloud by Quest for Secure Device Patching and Endpoint Management

KACE Cloud by Quest was specifically designed to help organizations deal with the challenges of managing endpoints. Some of KACE Cloud's more notable capabilities include:

- Patch a wide variety of devices, operating systems, and third-party software
- Patch on-premises and remote devices, including BYOD devices
- Rich reporting capabilities, making it easy to verify patch deployments and identify any missing patches
- Automated, zero-touch deployments for Windows, MacOS, iOS, and Android devices. Once enrolled, these devices are inventoried, tracked, maintained, and kept up to date automatically. You can even use KACE Cloud to push software to devices and use location rules to determine when and from where users are able to access sensitive information.
- Apply security policies to devices so that you can track a device's location history, automatically lock a device, or even perform a remote wipe of a stolen device.

KACE Cloud is a must-have solution for endpoint management. In addition to being a best-of-breed patch management system, it is also able to help organizations effectively manage remote and BYOD devices. You can learn more about KACE Cloud and get a free trial at: https://www.quest.com/products/kace-cloud/

About Quest

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform manage-ment and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.