EBOOK

5 EFFECTIVE WAYS TO REDUCE CYBERSECURITY RISK IN 2021

Introduction

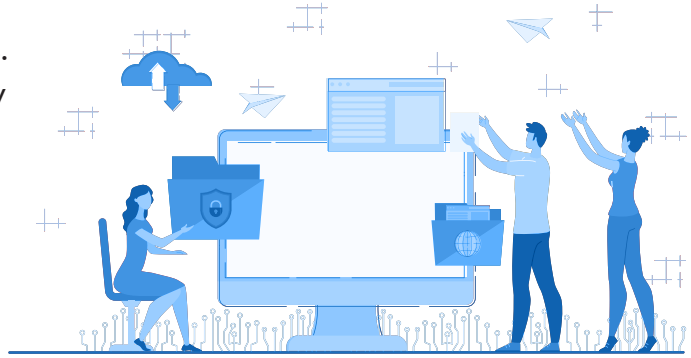
With the rapid rise in cyberattacks in the past year, cybersecurity has quickly become the top priority for businesses around the world. With companies forced to switch to remote work to survive the pandemic, the stakes have never been higher. In 2020 alone, the National Vulnerability Database (NVD) published 18,362 vulnerabilities in total.[1] Many organizations, including U.S. government agencies, have recently fallen prey to various kinds of cyberattacks.

The 2020 Cost of a Breach Report by the Ponemon Institute states that it takes, on average, about 280 days for companies to identify and contain a breach.[2] This is a major concern since the longer a breach goes undetected, the more damage it can cause. IT leaders must constantly be vigilant to keep their infrastructure and data secure.

Managing security, of course, isn't just a one-time job. It is a continuous process that requires time, proactive effort and keeping up with ever-changing technology.

This eBook outlines five security measures an organization can take to reduce its exposure to cyber risk.

1. Gain Complete Visibility of Assets



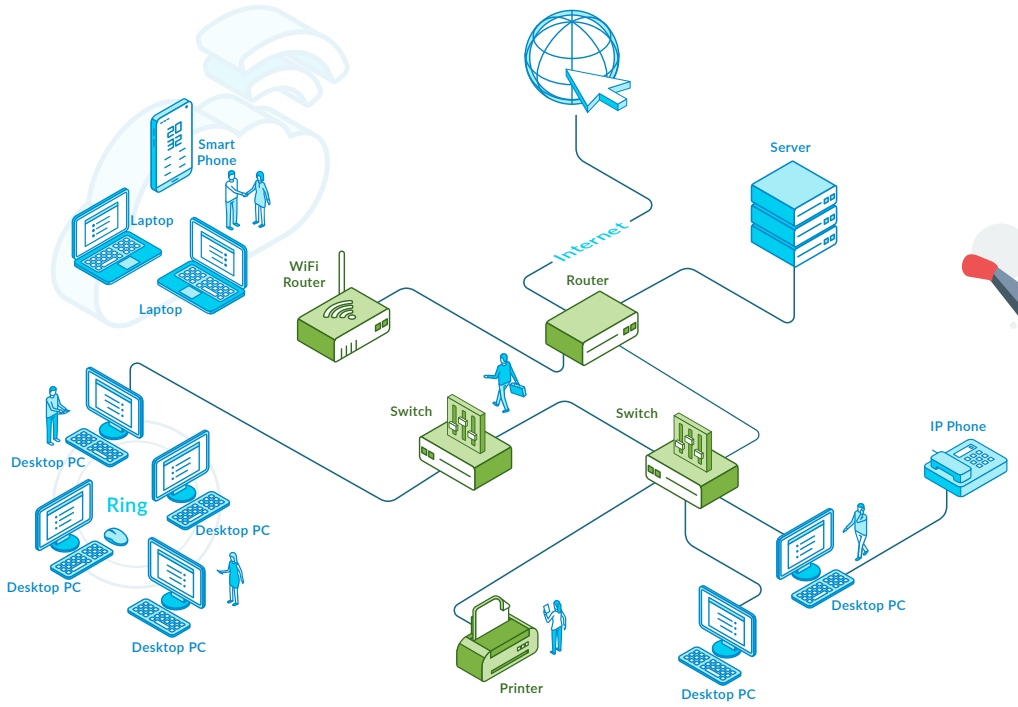
Complete visibility requires the ability to discover all endpoints and network devices. A remote monitoring and endpoint management solution takes care of the discovery process. With the discovery data, your endpoint management tool should then build a network topology map showing the connectivity of all devices.

Having full visibility of your IT networks is critical to detecting and resolving IT incidents that can disrupt services to the business. It is also crucial to IT security as well. For example, you must know what endpoints (Windows, Linux and macOS devices) are out there so you can regularly patch the software on those devices. (See below for more on patching)

Your remote monitoring and endpoint management solution gives you visibility and control of every endpoint and network device discovered on your network(s).

An endpoint management tool, such as **Kaseya VSA**, automates the discovery process and provides a network topology map of your IT environment. This includes both agent-based and agentless devices.

The VSA topology map also shows the up/down status of each device on the network and indicates if a node has any open alarms. This helps quickly identify potential problem sources so you can resolve issues faster.



2. Patch OSes, Browsers and Third-Party Applications

In 2020, about six percent of data breaches worldwide involved the exploitation of software vulnerabilities.[3] Kaseya's 2020 State of IT Operations Report showed that only 58 percent of organizations patch critical operating system (OS) vulnerabilities within 30 days while only about a third apply critical patches for third-party apps within 30 days of release.

Failing to patch all your software, including third-party applications, can put your business at major risk. Automate the process of patching with an endpoint management solution to ensure patches are deployed in a timely manner. You should strive to apply critical patches within 15 to 30 days of availability.

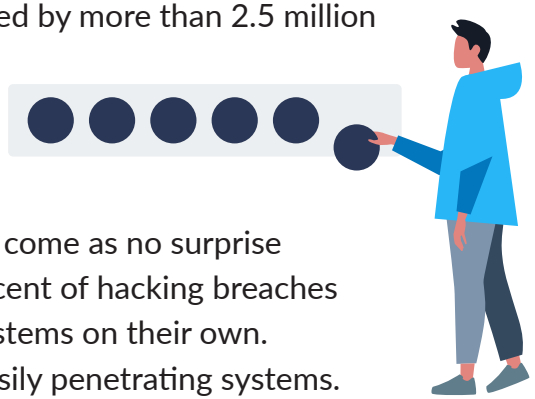
Your endpoint management solution must be able to:

- Scan regularly for updates and missing patches
- Have visibility into the patch status of all endpoints
- Automate the patch process under the control of policies and profiles that manage patching complexity and ensure reliable outcomes
- Automatically notify about failed updates
- Patch remote, off-network devices (e.g. work-from-home users' computers)

With so many employees working remotely, patching off-network devices is extremely important to maintain endpoint security.

3. Implement Multifactor Authentication (MFA)

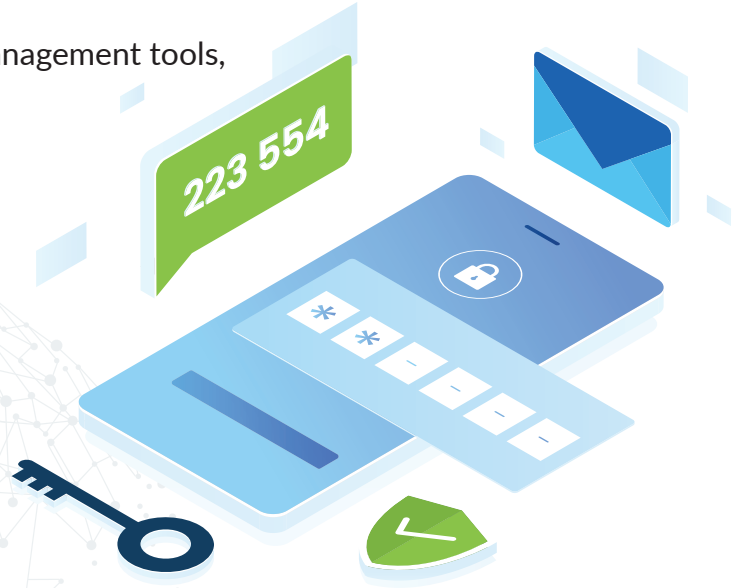
How many times have you heard of people using passwords like "password123?" Probably more times than you can count. Password manager NordPass revealed that in 2020, "123456" was the most used password – used by more than 2.5 million people – and exposed more than 23 million times in data breaches.[4] The second most popular password was "123456789." NordPass observed that the third most popular password, "picture1," took just three hours to crack.



This information provides insight into how easily passwords can be cracked. That's why it should come as no surprise that the credentials of many people are available for sale on the Dark Web. In fact, about 80 percent of hacking breaches involve brute force or stolen credentials.[5] This shows that passwords can no longer protect IT systems on their own. To boost security, businesses need a stronger mechanism that can hinder cybercriminals from easily penetrating systems.

Two-factor authentication (2FA), a subset of MFA, ensures that all users logging into systems authenticate themselves with a second authentication mechanism other than a password, such as a code sent to their verified mobile phones, a text message on their phones or a USB key, which when inserted into their devices, allows them to log in securely.

IT administrators should use 2FA to log into their endpoint management tools, adding this extra layer of login security for their core IT management solution.



4. Implement Zero Trust Network Access (ZTNA)

Zero Trust Network Access is an alternative approach to securing access to internal applications compared to network-centric solutions like VPNs and firewalls. ZTNA is based on four key principles:

- It isolates the process of providing application access from network access.
- It makes outbound-only connections, which makes networks and applications invisible to unauthorized users.
- Application access is granted on a one-to-one basis. Authorized users can only access specific applications rather than gaining full access to the network.
- ZTNA takes a user-to-application approach rather than a network-centric approach to security.

A key consideration when choosing a ZTNA vendor is whether their solution integrates with Unified Endpoint Management solutions such as Kaseya VSA.

5. Manage Privilege Policies

A privileged user has administrative access to all your critical systems, which brings with it the risk of insider threats. As per the 2020 Cost of a Breach Report by the Ponemon Institute, seven percent of malicious breaches are caused by insiders.[6] Insider threats are mostly caused by employee negligence or due to disgruntled employees who choose to leak company data to cause the company harm.

While outsiders need to "break in" to get access to their victim's data, insiders with privilege access can be more dangerous to a company since they can abuse this access with ease. Use tools to detect insider threats by monitoring:

- Logins at unusual times
- Unauthorized applications installed on devices
- New devices on restricted networks
- Attempts to gain access to sensitive information

Manage access privileges carefully across all your IT systems and applications. Kaseya VSA allows you to control access to your endpoint management tool by setting up roles and scopes for each user.

How Kaseya VSA Helps

Kaseya VSA, our unified remote monitoring and management™ solution, gives you the visibility and control you need to reduce risk while maintaining system and service availability. It enables you to keep your IT infrastructure secure with automated patch management and vulnerability management. VSA is integrated with leading antivirus and antimalware solutions (AV/AM) as well as backup and disaster recovery (BDR) solutions so you can manage all your core IT security functions from a single console.

VSA by Kaseya

You can request a demo of Kaseya VSA right here.

Sources:

1. National Vulnerability Database, NIST
2. 2020 Cost of a Breach Report, Ponemon
3. Verizon Data Breach Investigations Report 2020
4. Top 200 most common passwords of the year 2020, NordPass
5. Verizon Data Breach Investigations Report 2020
6. 2020 Cost of a Breach Report, Ponemon

About Kaseya

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

02192021

EBOOK