Kaseya®

Securing your devices can be challenging, especially when your employees are working remotely. All endpoints, both on- and off-network, must be patched and secured on an ongoing basis.

Here is a checklist to help build a robust cybersecurity strategy for your business.

✔

	1. Perform a security assessment	Assessing your company's security threats is the first step towards keeping your IT environment secure. Security assessments should include checks for vulnerabilities in your IT systems and business processes, as well as recommending steps to lower the risk of future attacks. Identify: ▶ Your critical assets ▶ External vulnerabilities that could be potential security gaps that would allow hackers access to your network and information ▶ System protocol leakage - outbound protocols that shouldn't be allowed ▶ Lack of web browser controls ▶ Wireless network security issues ▶ Network share permissions

	2. Set up a secure VPN for remote workers to access applications that require it	VPNs encrypt internet traffic making it unreadable to anyone intercepting it. It's important to have an easy and automated process to set up VPN on your remote endpoints.
		
		Here are a few guidelines:
		▶ Use a strong encryption method for VPN
		   ▶ Consider Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPsec)
		   ▶ Consider OpenVPN over Point-to-Point Tunneling Protocol (PPTP)
		▶ Use an endpoint management tool to deploy, configure and monitor VPN clients on remote endpoints
		▶ Automate the process of redeploying the VPN client if it goes down

	3. Have a Bring Your Own Device (BYOD) policy that specifies security requirements	Outline essential elements for your BYOD policy to ensure maximum endpoint security: ▶ Chart out the minimum required security controls for devices ▶ Provide components such as SSL certificates for device authentication ▶ Enforce strong password policies ▶ Control and monitor the installation of apps ▶ Define policies to be followed in case an employee leaves the company and data needs to be wiped ▶ Your BYOD policy should require an agent to be installed on the endpoint for managing the device

Kaseya®

✔

4. Automate software patch management and vulnerability management

Install, deploy and update software on each endpoint automatically using an endpoint management solution.

▶ Have real-time visibility into the patch status of your on-and-off network devices.
▶ Have visibility into the software vulnerabilities that impact your IT environment
▶ Set up auto-remediation of vulnerabilities through proactive scanning and automated patching

5. Back up systems and SaaS application data with integrated backup and disaster recovery solutions

Implement a robust backup solution that:

▶ Integrates with your endpoint management solution for seamless backup management
▶ Automates testing for guaranteed recovery
▶ Ensures clean instant recoveries

Back up your SaaS data for speedy restoration in case of malware, phishing or user errors.

6. Implement multi-factor authentication (MFA) and single sign-on (SSO)

SSO and MFA increase authentication security by:

▶ Reducing the need to remember user credentials
▶ Requiring additional information, beyond passwords, to log into the user's account. For example, with two-factor authentication, you would get a one-time passcode
▶ Letting users log in securely to multiple applications with one set of credentials

7. Educate your employees and monitor your exposure to the dark web

Monitor the dark web to take proactive steps to prevent a security breach

▶ Scan the dark web for stolen credentials
▶ Set up alerts if any company data or employee personal data is found on the dark web
▶ Change the passwords as needed and implement strong password policies
▶ Educate employees with simulated phishing emails and security awareness training videos

8. Detect and respond to insider threats

Insider threats occur when employees within the organization expose confidential information, either through negligence or malicious intent.

In 2019, about 57 percent of data breaches globally involved insiders, with 15 percent of data breaches occurring due to misuse of privileges.[1]

Enhance your organization's security by taking these steps to respond to these threats:

▶ Monitor unauthorized logins and restrict privileged user access
▶ Track unusual or odd-hour login behavior
▶ Set alerts when wireless connections are added to the network

✓		
	9. Deploy an antivirus/anti-malware and endpoint detection and response (EDR) combined solution	Go beyond traditional antivirus and anti-malware and implement an EDR solution to combat cyberattacks. EDR solutions record system activities and events taking place on endpoints and provide security teams with the visibility they need to uncover and remediate incidents. A sophisticated EDR solution identifies and removes cyber threats from your environment by ▶ Constantly monitoring your environment for security incidents and anomalies ▶ Providing real-time threat detection and automated remediation ▶ Delivering fast incident triage, investigation and response ▶ Offering pre- and post-compromise attack visibility (Root Cause Analysis)
	10. Implement and practice your incident response plan	All organizations need to be prepared for major security incidents that could drastically affect their business. Plan and practice a step-by-step incident response strategy that incorporates the following: ▶ Define the roles and responsibilities of each member of your incident response team ▶ Have a business continuity plan ▶ Identify the tools, technologies and resources that must be in place. ▶ Define all critical network and data recovery processes ▶ Identify and remediate the root cause of the incident – apply patches, update systems, remove malware, etc. ▶ Have a communications plan for both internal and external stakeholders.

FOR COMPREHENSIVE LAYERED SECURITY OF YOUR DEVICES AND DATA,

SPEAK TO OUR REPRESENTATIVES HERE.

Sources:

1. 2019 Insider Threat Report, Verizon

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.

05042020