Kaseya

10 CYBERSECURITY SPELLS

to Protect Your Network From Ransomware Scares

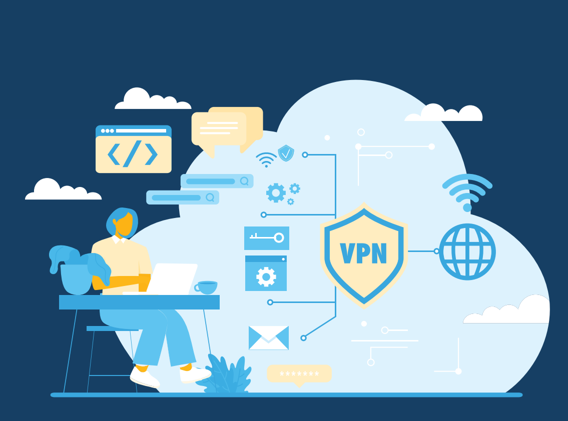
Here's a spooky ransomware stat that will send shivers down your spine. In just the first half of 2023, cybercriminals extorted a little under half a billion dollars from their victims in ransomware payments — a 64% increase from 2022. With the specter of this menacing threat growing at an alarming rate, these 10 powerful cybersecurity spells will help keep your organization safe.

1 PERFORM SECURITY ASSESSMENTS REGULARLY

Hackers lurk in the shadows, ready to exploit the first vulnerability they encounter in your IT environment. Conducting regular security assessments is an easy way to identify and plug gaps in your network before bad actors take advantage of them. Here are a few security checks to keep in mind:

- Identify, monitor and detect your critical assets and plug potential security gaps caused by external vulnerabilities.
- Check for system protocol leakage — outbound protocols that shouldn't be allowed.
- Assess network share permissions and fix wireless network security issues.
- Identify and fix lack of web browser controls.

2 SHIELD YOUR REMOTE WORKERS WITH A SECURE VPN



VPN gives your remote employees a cloak of anonymity against the prying eyes of hackers. The solution conceals their identity and encrypts their connection and communication with the company network, thus enhancing security. Tips to keep in mind when using a VPN:

- Use an endpoint management tool to deploy, configure and monitor VPN clients on remote endpoints.
- 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).
- Automate the process of redeploying the VPN client if it goes down.

3 SECURE YOUR BYOD POLICY

A BYOD policy, although convenient, can quickly become a security challenge if not managed well. Strengthen your policy by clearly specifying security requirements and installing a monitoring agent on enrolled devices for effective management. Here are some suggestions:

- Enforce strong password policies and 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.
- Provide components such as SSL certificates for device authentication.

4 AUTOMATE PATCH AND VULNERABILITY MANAGEMENT

By automating patch and vulnerability management, you can stay one step ahead of bad actors and address security gaps before they become security nightmares. You get:

- Real-time visibility into the patch status of your on- and off-network devices.
- Visibility into the software vulnerabilities that impact your IT environment.
- Auto-remediation of vulnerabilities through proactive scanning and automated patching.

5 INVEST IN A RELIABLE BACKUP AND DISASTER RECOVERY SOLUTION

Dodge security curveballs by investing in a robust backup solution that can restore your systems and data quickly. A good backup solution should be able to do the following:

- Integrate with your endpoint management solution for seamless backup management.
- Ensure clean, instant recoveries.
- Back up your SaaS data for speedy restoration in case of malware, phishing or user errors.
- Automate testing for guaranteed recovery.

6 IMPLEMENT MULTIFACTOR AUTHENTICATION (MFA) AND SINGLE SIGN-ON (SSO)

MFA and SSO are two ways your employees can access company systems, applications and databases securely. This setup provides stronger protection even if login credentials fall into the hands of cybercriminals.

- MFA is a way for users to authenticate their identity by providing additional info along with a regular password, such as a one-time code, fingerprints or facial recognition.
- SSO lets users log in securely to multiple applications with one set of credentials.
- It reduces the likelihood of users reusing the same passwords for multiple logins or creating weak passwords.

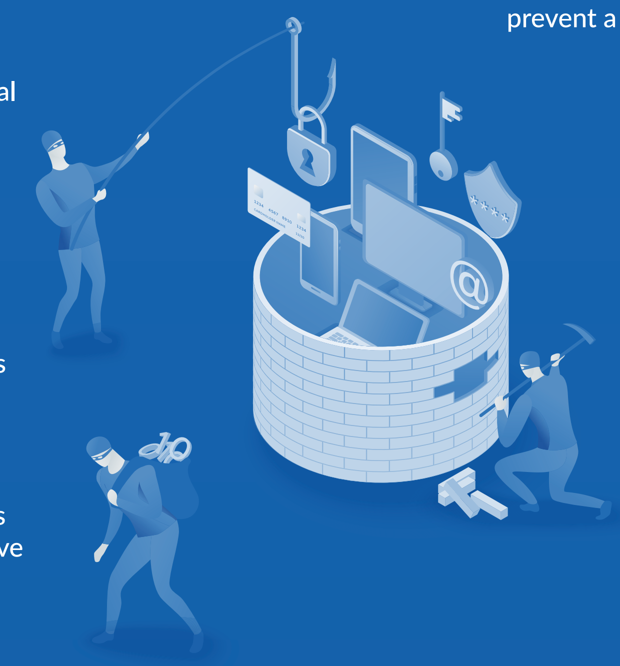
8 STAY ON THE LOOKOUT FOR INSIDER THREATS

Organizations are not just at risk from external threats but also from within. Insider threats include malicious attacks as well as employees' negligent use of systems and data. The following checks can help you respond to them on time:

- Monitor unauthorized, unusual or odd-hour logins.
- Set alerts for when wireless connections are added to the network or foreign RMM agents are installed.
- Restrict privileged user access and monitor for suspicious, ransomware-style notes.
- Automatically isolate potentially infected endpoints when one or more of the above conditions are met.

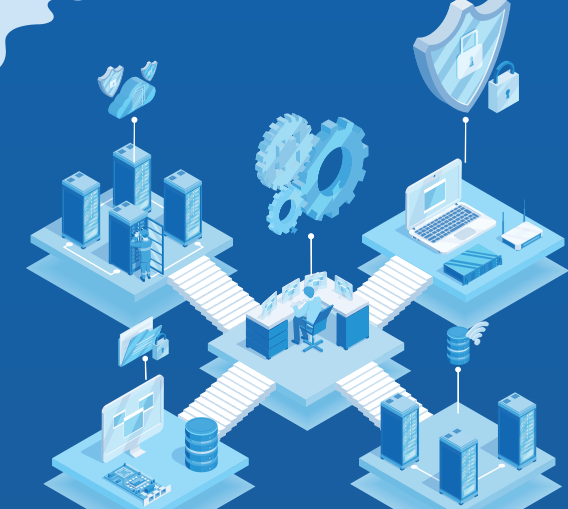
7 BEWARE OF THE DARK WEB

The dark web is a scary place where cybercriminals can find sensitive information to gain easy access to your company network. Monitoring this hidden realm can alert you to trouble brewing below the surface so you can take timely precautions and prevent a security breach.



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

9 UNLEASH THE POWER OF EDR



While antivirus (AV) and antimalware (AM) solutions are great for detecting signature-based threats, an endpoint detection and response (EDR) solution is highly effective at detecting ransomware and polymorphic threats. Here's why EDR is so powerful against cyberthreats:

- Constantly monitors your environment for security incidents and anomalies.
- Provides real-time threat detection and automated remediation.
- Triages, investigates and responds to incidents quickly.
- Provides pre- and post-compromise attack visibility (root cause analysis).

10 HONE YOUR INCIDENT RESPONSE PLAN

An incident response plan is necessary to address unforeseen security incidents that could significantly disrupt your business operations. Plan and practice it until it becomes second nature.

- Define the roles and responsibilities of each member of your incident response team.
- Identify the tools, technologies and resources that must be in place.
- Define all critical network and data recovery processes.
- Have a communications plan for both internal and external stakeholders.

Kaseya VSA is the only endpoint management tool with a unique emphasis on security. Automated patch management, policy-based configuration hardening, and integrated AV, AM, EDR and Managed SOC capabilities make it a formidable IT and security management solution. To discover more about VSA,

SCHEDULE A DEMO TODAY

Kaseya