Malwarebytes

SOLUTION BRIEF

MSP best practices for securing servers

Protecting servers shouldn't be optional

Servers are the backbone of any managed service provider (MSP). Not only are business-critical, back-office systems running in them, they also process and store a huge amount of sensitive company and client data. This is why they are every organized online attacker's most sought-after and prized target. Their weapons of choice? Spyware and ransomware.

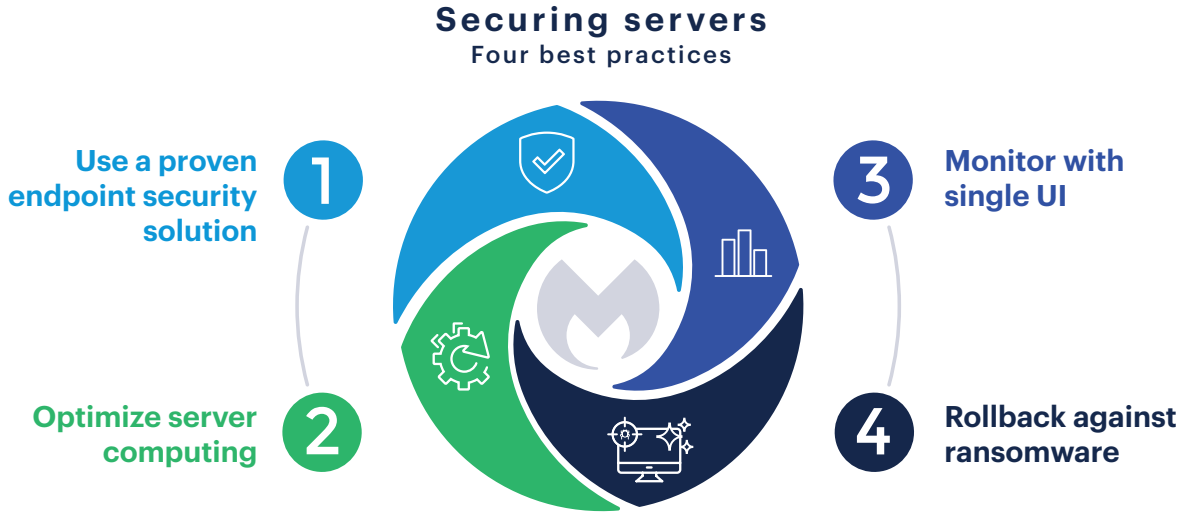
OVERVIEW

Several malware types pose a wide range of risks to mission-critical servers. For MSPs to protect their clients' essential assets against internet-born threats, we offer four best practices.

Spyware is a type of malware capable of stealing information from any computing device it finds itself infecting, may these be your clients' workstations, mobile devices, or servers. A threat actor can program them to steal sensitive client data, usually online credentials, payment information, emails, chat discourse, and browser history. More powerful ones can even steal media, such as photos, audio recordings, and video clips. Spyware is an old form of malware, yet it remains an effective and essential part of a threat actor's toolkit because it's sneaky and does the job well.

Ransomware, on the other hand, is a younger form of malware and with far different capabilities—and impacts. Unlike spyware, ransomware goes after and encrypts mission-critical application files in on-premise workstations and backend systems alike. This eventually leads to system failure, significantly disrupting normal operations of your clients and costing them money and productivity.

With threats like these, current protection practices aren't enough. It is more important than ever for MSPs to create an endpoint security strategy that does not only address security issues in client workstations but in their servers as well.



Best practices for securing servers

Use an endpoint security solution that is purpose-built for servers

The majority of endpoint protection solutions on the market are geared more towards workstations and less so towards servers. Applications that offer little server-specific protection—not to mention no support for certain platforms like Linux—leave servers more vulnerable to attacks. An endpoint solution pre-built with server policy "templates" allows MSPs to deploy a software agent to client servers to rapidly apply robust, best-practice security policies to ensure they are sufficiently protected from the start.

Optimize server computing with a light-weight agent and cloud processing power

Most client servers are running at maximum capacity, processing terabytes of data every day. Any software agent that impacts server performance would slow this down, impairing overall business productivity. As such, it is important for MSPs to ensure that the security agent they use is light weight in terms of disk space and memory usage.

Further, server endpoint security should offload more compute-intensive tasks to a cloud platform to maximize disk performance while minimizing utilization.

Monitor servers and workstations together in a single UI

When it comes to your SOC team monitoring your client's workstations and servers, having a single, common UI to manage them simplifies the task. If, for example, ransomware successfully enters the network via a phishing email delivered to an employee on a workstation, a great endpoint solution doesn't only detect and alert the team, but also gives them granular data, such as indicators of compromise (IoCs) found on affected endpoints—both workstation and server—in a single pane of glass. This kind of visibility across an organization's network is critical to keeping SOC teams efficient but very difficult to achieve with endpoint security solutions that require a unique UI for each product.

Be able to rollback against ransomware

There is no doubt that ransomware can cripple an MSP client in a snap, and mitigating the damage is not easy, cheap, or quick. Wouldn't it be so much better to get business up and running again not in a few days, weeks, or months, but a few hours? This is where a Ransomware Rollback feature comes into play. This feature can return ransomware-affected servers to their previous state before infection within minutes—with clients not having to undergo costly mitigation and remediation steps, which could take weeks or months, and not having to pay the ransom.

LEARN MORE

To learn more about Malwarebytes endpoint security applications for servers and our MSP Partner Program, visit us at www.malwarebytes.com/msp

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.