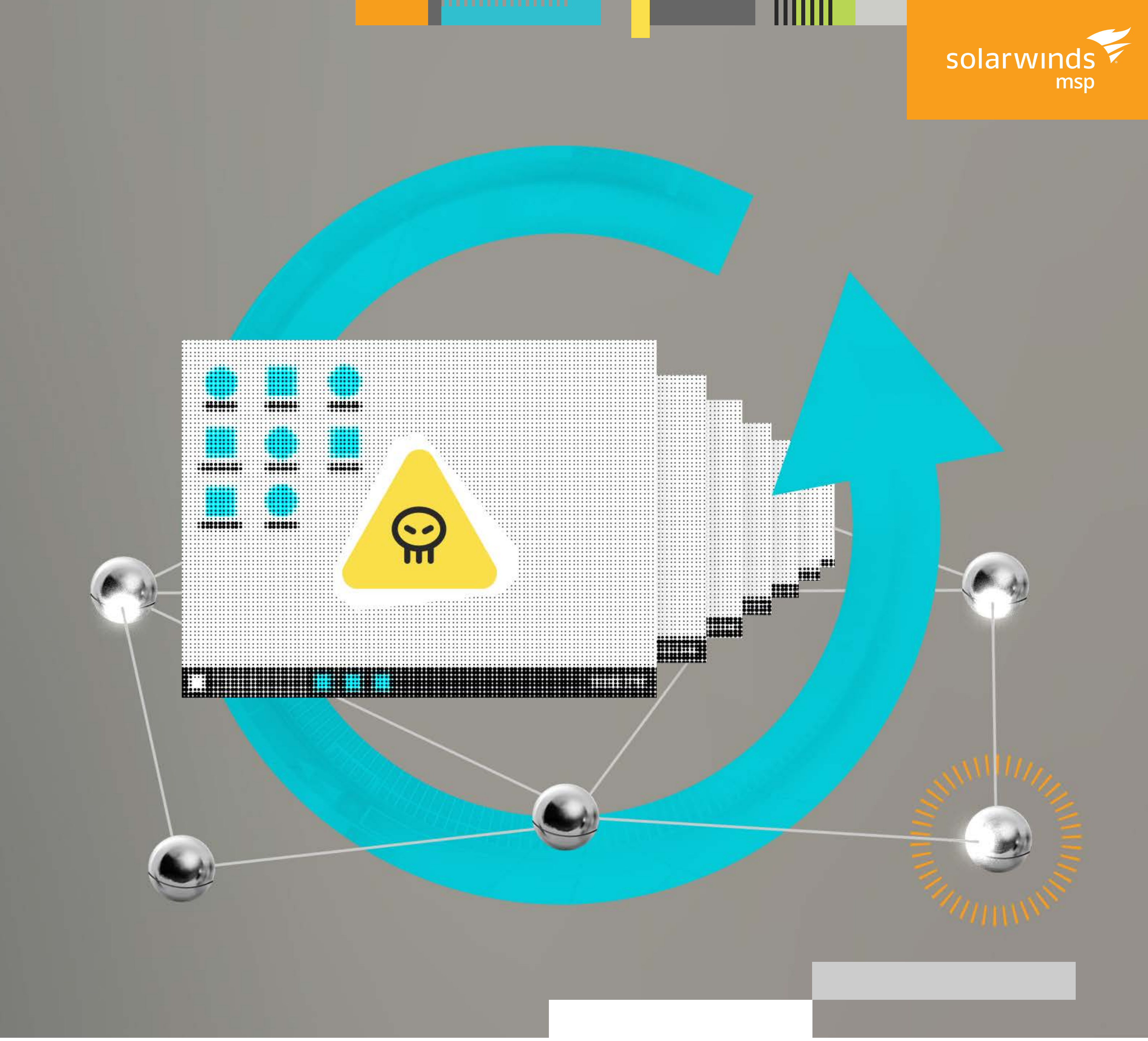


eBOOK

SolarWinds EDR Rollback: A Cybersecurity Time Machine

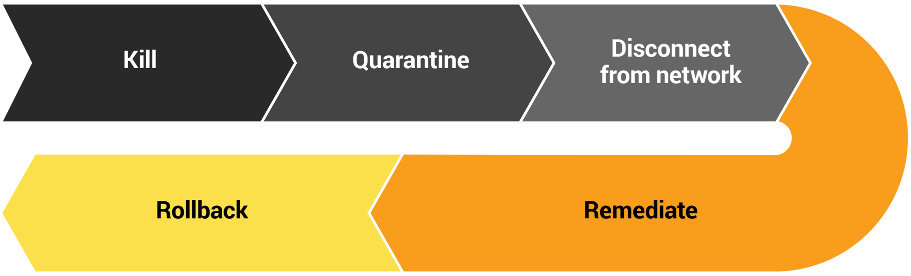
In other eBooks, we talked about the differences between traditional antivirus (AV) and endpoint detection and response (EDR) solutions. When it comes to detection and data protection, EDR encompasses a wider range of threats than traditional AV, which focuses on file-based malware threats via virus signatures. Additionally, by adapting via machine learning and focusing on endpoint behavior, EDR solutions respond better to zero-day threats than traditional AV solutions. In short, it's more comprehensive, and is *particularly* well suited for higher risk organizations that have a lot of sensitive data.

But while they say an ounce of prevention is worth a pound of cure, sometimes you still need a good cure. And with an EDR solution like SolarWinds® Endpoint Detection and Response, the cure can come faster and more effectively. In fact, the rollback capabilities of SolarWinds EDR can save you significant time dealing with cyberattacks and save your customers money in dealing with the fallout—and it's one of the key features setting it apart from an AV solution. But we're getting ahead of ourselves. We should start by talking about the different ways SolarWinds EDR deals with detected threats.

The path to rollback

One of the key elements of a good EDR solution is that it automates a good portion of the response to threats. Without an EDR solution, you must handle many of these steps manually. However, when SolarWinds EDR flags a threat, it offers five different options. Three can be classified as preventative, meaning they put a stop to damage caused by the threat. The other two options can be classified as response, meaning you can bring an endpoint back to its state prior to attack.

Let's break them down.



PREVENTATIVE

- **Kill:** This option stops the attack immediately. For example, if a malicious process starts running in the background of your computer, it can kill the process on your behalf. Or if an Excel® document launches a malicious script that starts deleting files en masse, it attempts to prevent this process from occurring. Without an EDR solution in place, you might need to catch the malicious process and manually stop it yourself.
- **Quarantine:** The quarantine option takes any executables that are a threat and moves them to a walled-off area so they can't continue causing damage or spreading across the endpoint. These files can be looked at for additional analysis in a sandboxed environment. Quarantining files is a common practice in traditional AV solutions, as well.
- **Disconnect from network:** This option allows you to disconnect an endpoint from the network. For network admins, this is particularly helpful because it limits outbound network access to the management console, thus preventing any spread of malware on the network. Cybercriminals often seek to maximize their payday. Gaining persistence across the network lets them compromise more systems and potentially steal more data. By disconnecting the endpoint from the network, you can prevent threats from causing serious damage to the wider network. Then, you can investigate what happened using the deep set of forensic tools available in the platform. This can buy you time to solve particularly thorny issues that don't have a straightforward resolution, and it can also let you understand what occurred to prevent it in the future (or make sure no other systems are affected). In short, disconnecting the network gives you numerous benefits.

RESPONSE

- **Remediate:** This option allows you to remove the damage caused by the threat. However, it isn't a full rollback, which "rewinds" to a specific point in time.
- **Rollback:** During a rollback, the affected device is restored to a saved Volume Shadow Copy Service (VSS) snapshot, which reverses any damage. In other words, it restores the endpoint to a state before the attack started doing damage. This can be particularly helpful for ransomware attacks, where it rolls the endpoint back before files were encrypted. This can help negate the need to pay the ransom. Beyond that, the rollback feature happens much faster—near instantaneously—than if you were restoring from a backup. However, EDR doesn't eliminate the need for a good, cloud-based backup solution. Ransomware is only one threat—data loss can easily occur due to software failures, hardware issues, or even natural disasters. Plus, rollback is only available on Windows®, so you'll still need a good cloud-based backup for both Mac® and Linux® machines.

These five steps occur in a sequence. As an administrator, you set how you want EDR to respond to a threat. If you choose to implement any of the above as a first action (i.e., you quarantine a threat), EDR will also implement any actions available prior to that—in this case, it will apply "kill" as well.

The nuts and bolts of rollback

Automated rollback obviously has a lot of potential. It can allow you to quickly get customers up and running in an instant and save them a lot of money from paying ransoms. So how does it work?

The key technology behind rollback is VSS. This feature from Microsoft® Windows Operating Systems can maintain multiple copies of volumes or computer files, even while they're in use.

How does this work? It's roughly akin to taking a digital photo, which has a time and date stamp. VSS is no different—it creates a digital image of the entire system at a specific interval and time, and stores it so it can be used to overwrite a corrupted endpoint. VSS gives the end user a mirror image of their system pre-attack. It's a powerful technology put to even more powerful use in rollback.

Interestingly, VSS doesn't cause as much resource drain on a computer as you might think. VSS is highly efficient by moving files to temporary locations in an incremental fashion. So it only moves files that have changed since the last snapshot. This obviously saves significant amounts of time compared to taking a full system snapshot each time.

VSS was introduced in Microsoft Windows XP®/Server 2003, and has been available in every version of Windows since. SolarWinds EDR allows for rollback in agents for Windows Vista®/Windows Server® 2008 R2 and onward.

ℹ Unfortunately, since Mac and Linux do not use VSS, we cannot currently support rollback functionality for macOS® or Linux-based systems.

Why rollback?

So why is it so important to have a rollback feature? Simple—one click can infect an entire network. Just one click on a bad email could lead to a ransomware download that spreads throughout a network, encrypting files and locking machines until it's almost impossible to operate.

Consider just the following:

- Businesses hit by ransomware attacks experienced an average of 16.2 days at the end of 2019[1]
- Experts predict that one business will fall victim every 11 seconds to a ransomware attack by 2021[2]
- They also predict that ransomware damages could cost $20 billion in damages worldwide by 2021[3]

The fiscal consequences of a successful ransomware attack can devastate a business. Being able to quickly detect ransomware helps you stop them from spreading, then rolling back an endpoint quickly prevents the costs of downtime from piling up. Plus, IT providers can demonstrate their value to customers by showing that they stopped an attack and restored an endpoint with almost no interruption to the end user.

EDR solutions do cost a little more than AV solutions on the front end. However, it's important to consider what you gain in functionality—from detection to automated responses and rollback—when factoring in the cost. The upfront price could easily justify itself when compared to the cost of a successful attack.

There's a place in organizations for both AV and EDR, depending on use cases. But if you fall into the latter camp for the reasons mentioned earlier in the eBook, consider what costs more to both your end users and your team—a bit more per seat for EDR or four to six hours to reimage an infected endpoint. That cost increases exponentially if you support a large organization and must reimage multiple endpoints that were infected. And don't forget—downtime is the most critical cost of all. When employees aren't working, productivity and profits follow a parallel path. EDR can help negate this.

[1] "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Coveware. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate (Accessed September 2020).

[2] "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021," Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed September 2020).

[3] Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021," Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Accessed September 2020).

Rollback in action

Cyberthreats can cause serious damages to a business, and ransomware, in particular, can wreak havoc on the bottom line. Yet, despite the challenges they bring, defeating them doesn't have to be overwhelming. SolarWinds EDR can help you roll back an endpoint after an attack in almost no time. With SolarWinds EDR in your corner, you can offer your customers better protection and greater peace of mind.

SOLARWINDS N-CENTRAL WITH INTEGRATED EDR

With SolarWinds EDR integrated in N-central®, you can offer your customers enhanced threat detection, monitoring, and fast remediation using SolarWinds EDR from the same solution you use to monitor and manage the rest of their IT infrastructure. N-central also offers multiple other security layers alongside EDR including AV, allowing you to choose the solution you need for each customer or user.

Plus, SolarWinds N-central can help you increase your operational efficiency with multiple built-in automation features including a drag-and-drop editor that lets you build full automation workflows without needing to write a line of code (or learn a scripting language).

Learn more today about the SolarWinds EDR integration within SolarWinds N-central: solarwindsmsp.com/products/rmm/endpoint-detection-and-response

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information.