Malwarebytes

TECH BRIEF

# Reimaging vs. Automated Remediation

## Improving Efficiency in Incident Response Processes

Organizations cannot prevent every attack on the endpoints, so it's critical to have strong capabilities to detect and remediate attacks after they penetrate your defenses. Minimizing dwell time is an area where organizations need to focus on to advance their incident response processes.

### What's the Trend in Remediation Times?

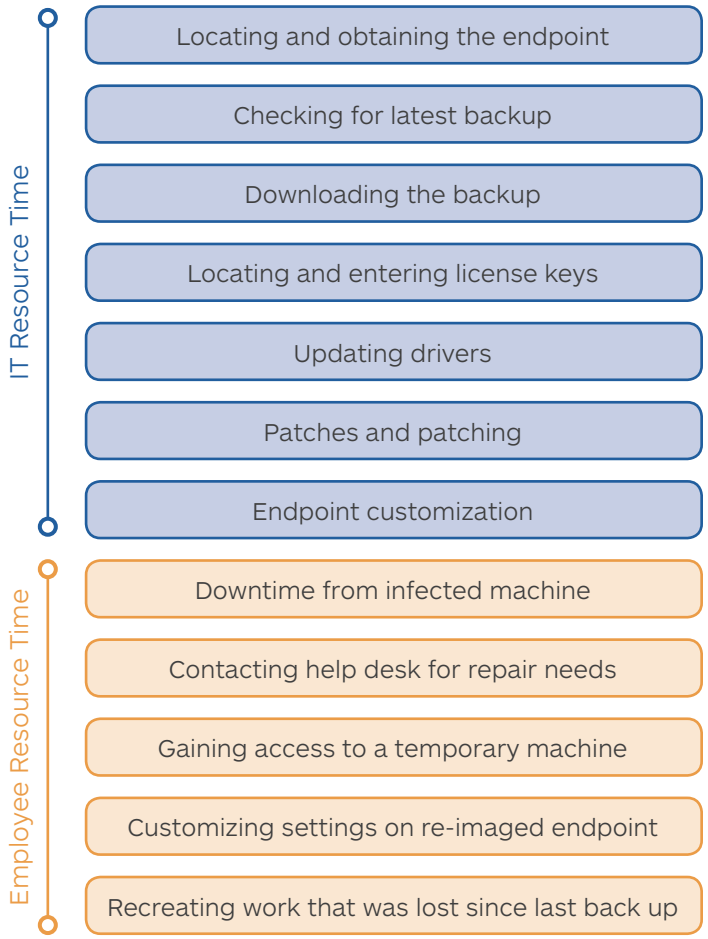
According to incident response (IR) teams, malware is the root cause of 68% of the incidents they investigate.[i] But how long does it take to recover from these attacks? In 2017, 28% of IR teams reported the time from detection to remediation was 6 to 24 hours and 23% required a minimum of 1 to 5 hours to recover.[ii] This is seen as an important improvement compared to the previous year. In 2016, the majority of IR teams needed a lengthy 2 to 7 days, and only 13% could complete remediation within 6 to 24 hours.[iii]

Automation tools are a key contributing factor behind increased response time efficiency. In fact, 25% of incident responders list full automation of detection, remediation, and follow-up workflows in their 12-month plan for incident response improvements.[iv]

### Legacy Reimaging IR Process

IR automation requires parting ways with the traditional re-imaging processes. While reimaging an infected endpoint has a long legacy as the de facto standard, it's fraught with time inefficiencies and inherent risks.

This adds up to hours of restoring endpoints and lost productivity caused by employees. There's also a high likelihood of lost work caused by the time between the last clean backup and the time of infection. The net result of this is a loss of employee productivity and ultimately money.



## Automation Tools Drive IR Efficiency

Now more than ever organizations need to shift from reactive to automated incident response processes in the face of limited resources and constant barrage of advanced threats.

IR teams need to establish a plan to adopt automated endpoint remediation that effectively rips malware out by the roots. The solution needs to deliver thorough remediation to the endpoint that seamlessly restores it to its pre-infection state. The Malwarebytes solution will proactively hunt for recently reported indicators of compromise (IOCs) to search for other compromised systems.

Automated remediation solves the severe shortcomings of reimaging and greatly increases response time efficiency. When properly executed, your automated remediation solution will remove all traces of malicious code while leaving legitimate files untouched, and it is fast.

The advantages of automated remediation over reimaging:

- Delivers automated, accurate, and thorough remediation
- Bridges operational silos
- Reduces malware dwell time
- Closes gap in personnel and skills shortage
- Eliminates cost and complexity of managing incident response
- Eliminates workstation and employee downtime
- Restores all employee work

## INCIDENT RESPONSE

Malwarebytes Incident Response delivers accurate and thorough remediation that optimizes your incident response efficiency and effectiveness. This automated approach helps advance your security model and bridges operational silos.

Most remediation solutions only remediate active malware components—this doesn't provide complete remediation. Malwarebytes Linking Engine applies a propriety approach that also detects and removes dynamic and related artifacts. The Malwarebytes engine applies associated sequencing to ensure malware persistence mechanisms are removed in such a way that disinfection is permanent. Our advanced remediation methodology provides organizations with expedient malware identification and thorough removal.

Malwarebytes empowers your IR team to run scheduled scans that proactively hunt for recently reported IOCs across the company. The Malwarebytes solution makes it easy to adopt an assume-the-compromise process to ensure your remediation includes searches for lateral movement and disinfection of all impacted endpoints.

[i] SANS Institute. "The 2017 SANS Incident Response Survey." June 2017.
[ii] SANS Institute. "The 2017 SANS Incident Response Survey." June 2017.
[iii] SANS Institute. "The 2016 SANS Incident Response Survey." June 2016.
[iv] SANS Institute. "The 2017 SANS Incident Response Survey." June 2017.

### LEARN MORE

To learn more about Malwarebytes Incident Response visit: malwarebytes.com/business

malwarebytes.com 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.