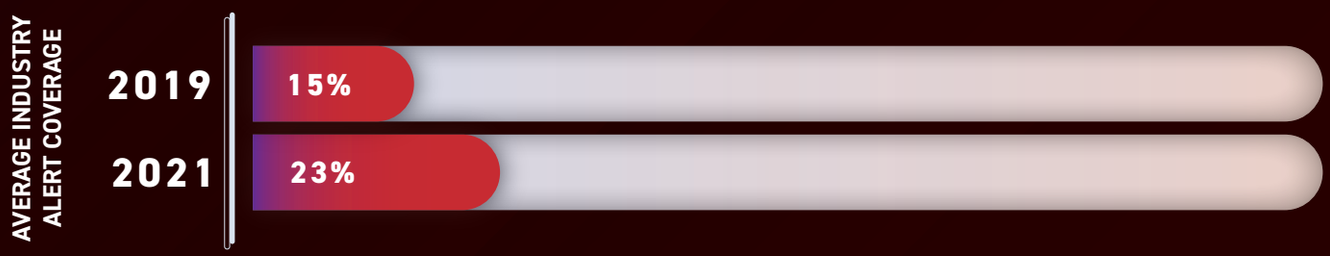
RANSOMWARE DETECTION CHECKLIST

Ransomware is simply a strategy for adversaries to make money. A strategy that's working so well that ransomware attacks doubled in frequency in 2021, according to the Verizon Data Breach Investigations Report, and ransom demands reached an astounding $70 million (source: Ransomware Task Force).

The increasing threat and impact of ransomware is not going to subside until we develop better strategies for detection and prevention. According to NetSPI data, the average industry alert coverage in 2021 was 23% — an 8% increase over 2019.

While ransomware detection coverage is getting better, there is a lot of room for improvement. To get started, here are nine steps to follow to improve your ransomware detection capabilities.



- **Ensure data sources are available to provide your security operations teams and/or partner with enough information to develop detections for common malicious behavior.**
  This should include file modification events, registry modification events, process creation events, image load events, network connection events, Windows endpoint security event logs, command line event logs, PowerShell event logs, Netflow/Pcap data, and security event data from third party software or devices.
- **Review telemetry flows on a regular basis to ensure they're still functioning as expected. You can't act on the data you can't see.**
- **Ensure your security operations team and/or partner have the capability to tune or create new detections.**
  NetSPI found that most endpoint detection and response and security information and event management (SIEM) solutions only identify around 15% of the most common TTPs used by real world attackers out of the box. This is why it is important that you carefully read your MSSP contracts – many organizations are not getting the coverage they thought they were.
- **Ensure that alert levels trigger response for high-risk behavior associated with high fidelity detections.**
- **Deploy or configure monitoring for high-risk command execution related to scheduled tasks, service manipulation, and LOLBAS (living off the land binaries, scripts, and libraries) execution.**
  It's important to monitor these patterns as they can be the result of encrypting files on scale during ransomware attacks.
  Note: This could potentially be done using existing performance monitoring tools.
- **Monitor for the deletion of shadow copies.**
- **Monitor for modifications to SafeBoot and similar restore capabilities.**
- **Ensure security tool tampering logs are enabled and forwarded to the SIEM.**
- **Monitor for high file I/O and CPU utilization on individual systems and the average across the network.**

Ready to measure the effectiveness of your ransomware detections against real tactics, techniques, and procedures (TTPs)? Learn more about NetSPI's Breach and Attack Simulation assessments and request a demo.