# Case Study #1: Technology & Product Review for Endpoint Protection Solutions

## Case Scenario:

Red Clay Renovations (the “client”) has requested that your company research and recommend an Endpoint Protection Platform which will provide host-based protection for the laptop PC’s used by its construction managers and architects. These employees design and manage construction projects using a Web based project management system. The laptops are also used to access web-based corporate email servers and additional web-based applications used for internal business operations. Their laptops are running the Windows 8/8.1 operating system and cannot be upgraded to Windows 10 due to compatibility problems in a business critical, proprietary software package. The Windows 8/8.1 laptops currently use Microsoft Windows Defender and Microsoft Windows Firewall to provide host-based protection against malware, spyware, and intrusions.

The client’s IT manager wants an Endpoint Protection product that is easy to use, is deployable on individual laptops as host-based protection, and automatically updates itself (patches and virus definition files). The “automatic” updates could be a problem since the laptops are rarely connected to the company’s networks. Instead, the employees use an intermittent cellular connection to access the Internet while visiting customers and construction sites.

## Research:

1. Review the Week 1 readings.
2. Choose one of the *Endpoint Protection Platform* products from the Gartner Magic Quadrant analysis (link provided in the weekly readings). Then, research your chosen product using the vendor’s website and product information brochures. (Vendors for highly rated products will provide a copy of Gartner’s most recent Magic Quadrant report on their websites but, registration is required.)
3. Find three or more additional sources which provide reviews for (a) your chosen product or (b) information about *Endpoint Protection Platforms*.

## Write:

Write a 3 page summary of your research (“briefing paper”). At a minimum, your summary must include the following:

1. An introduction or overview for the security technology category (Endpoint Protection Platforms)
2. A review of the features, capabilities, and deficiencies for your selected vendor and product
3. Discussion of how the selected product could be used by your client to support its cybersecurity objectives by reducing risk, increasing resistance to threats/attacks, decreasing vulnerabilities, etc.
4. A closing section in which you restate your recommendation for a product (include the three most important benefits).

As you write your briefing paper, make sure that you address security issues using standard terms (e.g. 5 Pillars IA, 5 Pillars Information Security). See the resources listed under Week 1 and under Course Resources > Cybersecurity Concepts Review for definitions and terminology.

## Formatting Instructions

Use standard APA formatting for the MS Word document that you submit to your assignment folder. Formatting requirements and examples are found under Course Resources > APA Resources.

## Submit For Grading

Submit your Technology & Product Review in MS Word format (.docx or .doc file) for grading using your assignment folder. (Attach the file.)

## Additional Information

1. There is no penalty for writing more than 3 pages but, clarity and conciseness are valued. If your essay is shorter than 3 pages, you may not have sufficient content to meet the assignment requirements (see the rubric).
2. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
3. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must comply with APA 6th edition Style requirements. Failure to credit your sources will result in penalties as provided for under the university’s Academic Integrity policy.