**Discussion Question: Architectures**

For this module's discussion board assignment, select **one** of the following to discuss:

* While IaaS, PaaS, and SaaS are all widely accepted, what are some of the security issues associated with each? Can those issues be mitigated? If so, how?
* Describe how SECaaS works. Would it make sense to use this type of service? Why or why not?
* More often than not, you won't be creating an entire system from the ground up. Typically you are building functionality to integrate into existing systems. While your new application might be fairly secure, what needs to be done before integration to ensure maximum security for the entire system?

***Before you submit your thread, put your name in the subject line.***

As we have all learned, security is a vital aspect that should be ingrained into all programming. If seeking additional or outside security practices to ensure secure software instead of in-house, then SECaaS can be a viable option. SECaaS, also known as Security-as-a-Service, is a “cloud-based” way to outsource cybersecurity (Fortinet, n.d.). According to Fortinet, SECaaS can provide “data protection, VoIP security, database security, and general network security.”

A benefit of SECaaS is that it can be more cost-efficient than hiring an onsite security specialist. It can also be beneficial since it gets companies in touch with experts, which can be handy when internal employees lack cybersecurity experience (Fortinet, n.d.). The software development world is constantly evolving; with that, what defines secure software can change. So, as time progresses, subscribing to SECaaS can grant access to the latest security updates (Fortinet, n.d.). If there is only one in-house security person, they may not be as informed as the experts dedicated to providing security as a service (Fortinet, n.d.). Another bonus of this service is that fewer internal resources are spent on security and can focus on other tasks (Fortinet, n.d.).

Based on the information provided, using SECaaS as a service makes sense. The reason I think this is because not every company is going to have the means to support a proper security department. If this is the case, outsourcing seems to be the best idea since security should be a major priority in protecting the company’s and any of its customers’ data.

**Reference**

Fortinet. (n.d.). *Security-as-a-Service (SECaaS)*. Fortinet. Retrieved April 1, 2025, from https://www.fortinet.com/resources/cyberglossary/security-as-a-service

**Assignment Requirements and Grading:**

1. An initial post of approximately 250 words is due by **Thursday, 11:59 p.m., CT**.
2. For the initial post to be considered substantive, it should be at least 250 words in length and fully cover the topics being presented. Single sentence definitions or responses will not be awarded points.
3. Submit your post by clicking on the **Assignment Link** above, then **Create Thread**. You must create a thread in order to view your peers' posts. Tip: Create your post in a Word document and then copy and paste your work into the thread.
4. A minimum of three (3) responses, **to the original threads of other students**, of 100-200 words each are due by **Sunday, 11:59 p.m., CT**.
5. To view the rubric grading criteria, click on the following link: [Discussion Board Grading Rubric.](https://content.bellevue.edu/cst/csd/rubricdbv3.pdf)

**(50 points)**