Security Programs for Securing Connected Products and Systems

EXECUTIVE SUMMARY

What is the cumulative cybersecurity risk of an organization's connected products, systems, and applications (CSP)? Does everyone agree the company is addressing the right risks at the right time? Do all partners understand their roles in responding to security issues?

CSP are driving industry growth across every sector of the market due to their cost saving and product lifecycle benefits. Security challenges have evolved in this space and are more complex because security requires a different approach today–one that prioritizes not only availability, integrity, and confidentiality, but also control and safety.

In this article, Deja vu Security (Deja) outlines some of the most prevalent challenges posed by todays CSP–including lack of security integration into the development lifecycle–and provides an overview of a Deja approach to integrating security into the lifecycle. Deja can help your organization design, build, and transform its CSP security program, and provide managed security services for your company at every step of the development process.

INDUSTRY ISSUES & TRENDS

Smart CSP are driving industry growth and can reduce detection to correction cycles, anticipate manufacturing failures in advance, improve design, save money, and reduce damage to brands. But the risks are also growing, and security is getting in the way. With the onset of more CSP used in daily consumer and producer lives, vulnerabilities are everywhere.

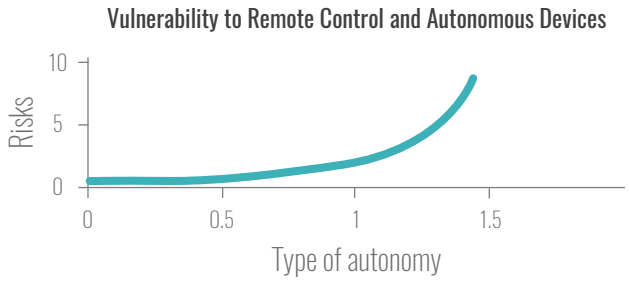
Level of autonomy	Threat rating
One-way communication	1-LOW
Two-way communication	2-MEDIUM
Remote control	5-HIGH
Full autonomy	10-CRITICAL

Table 1.1 – Level of Autonomy vs. Threat Rating

CSP AND THE SECURITY CHALLENGE

The increase in CSP brings mounting risks. In recent years, companies large and small have become susceptible to various attacks and exploits due to open vulnerabilities through their vulnerable CSP. Based on our experience with similar organizations, there are increased risks associated with CSP that send data to other CSP in accordance with their level of autonomy, leading to risks that transcend typical company risks (Table 1.1). These are heightened risks, primarily on disruptions to CSP, in turn causing system/equipment impairment, threat of physical safety, loss of R&D, and other critical issues. These have major consequences such as altered

or interrupted automated production processes, and human injury or casualty. In addition, CSP, left unsecured, may affect customer expectations and customer trust. Security concerns have evolved in complexity due to the nature of CSP and the challenges they pose. A shifting paradigm requires that product security prioritizes confidentiality, integrity, availability, control and safety.



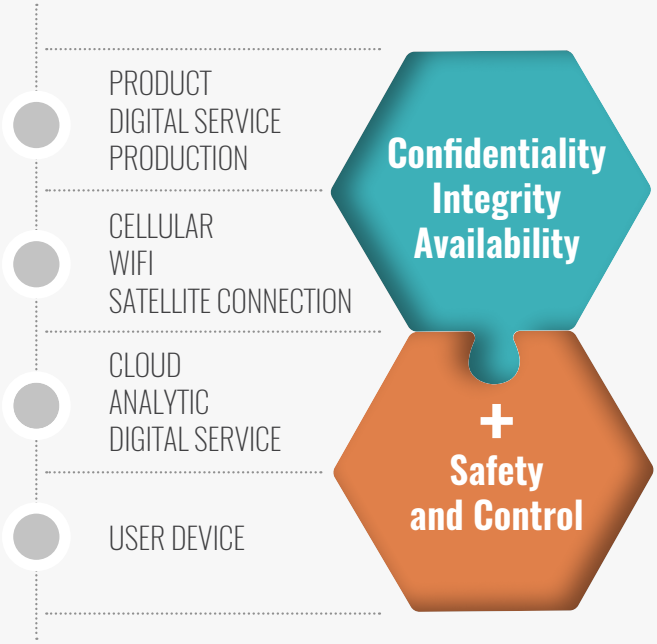


Image 1.1 – Security Concern's need for CIA + SC

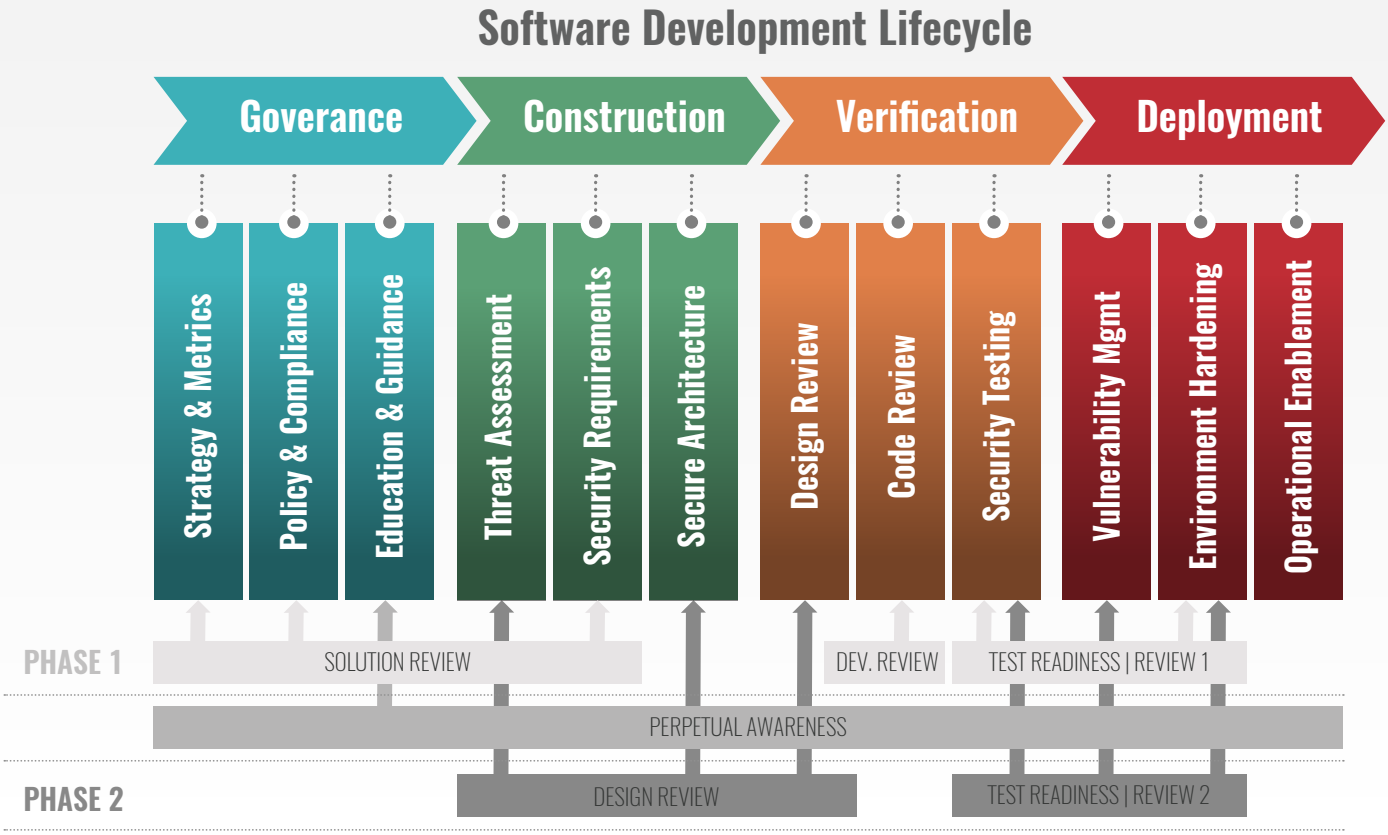
TOP 5 CHALLENGES POSED BY CSP

In an evolving technology landscape driven by CSP, organizations face a myriad of challenges related to incorporating security within the development and post-development phases of CSP. Based on our experience with delivering cybersecurity services to organizations across a variety of industry sectors, we have compiled a list of top 5 CSP security challenges faced by our clients as follows:

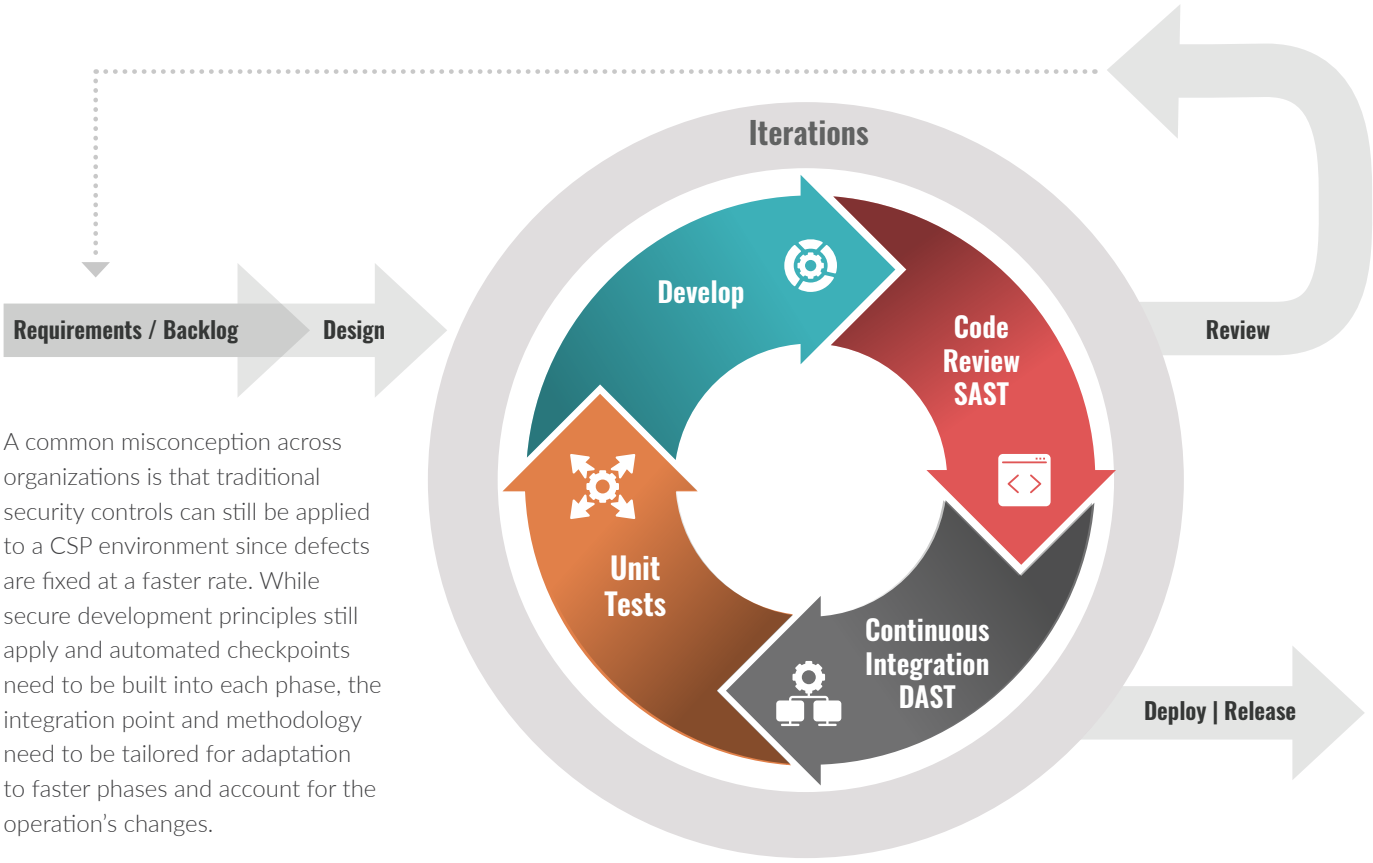
Common challenge	Preferred state
Lack of security integration into the CSP development lifecycle	Integrate security with existing engineering practices, from the requirements phase to maintenance via standards enablement
Unknown CSP inventory and uneven deployment of security tools to CSP engineering	Integrate security with existing engineering practices, from the requirements phase to maintenance via standards enablement
Ineffective CSP testing	Operationalize a client's "toolbelt" of tests to include SAST, DAST, IAST, fuzz testing, etc., in order to identify different vulnerabilities throughout the development lifecycle
Ad-hoc compliance-based CSP security testing is performed	Centralize CSP security testing based on the risk profile of the CSP
Lack of buy-in or resistance to security initiatives from engineering and business groups	Make CSP security a strategic collaboration between security, business, and engineering to manage overall CSP development

INTEGRATING SECURITY INTO CSP

In order to properly identify and mitigate these vulnerabilities, one must understand the environment and technologies that underlie them. Each component has a disparate development methodology, making it essential that the security program be holistic in nature. The final CSP is typically a combination of internally developed and externally sourced components, making it essential to ensure security of the underlying components from the supply chain.

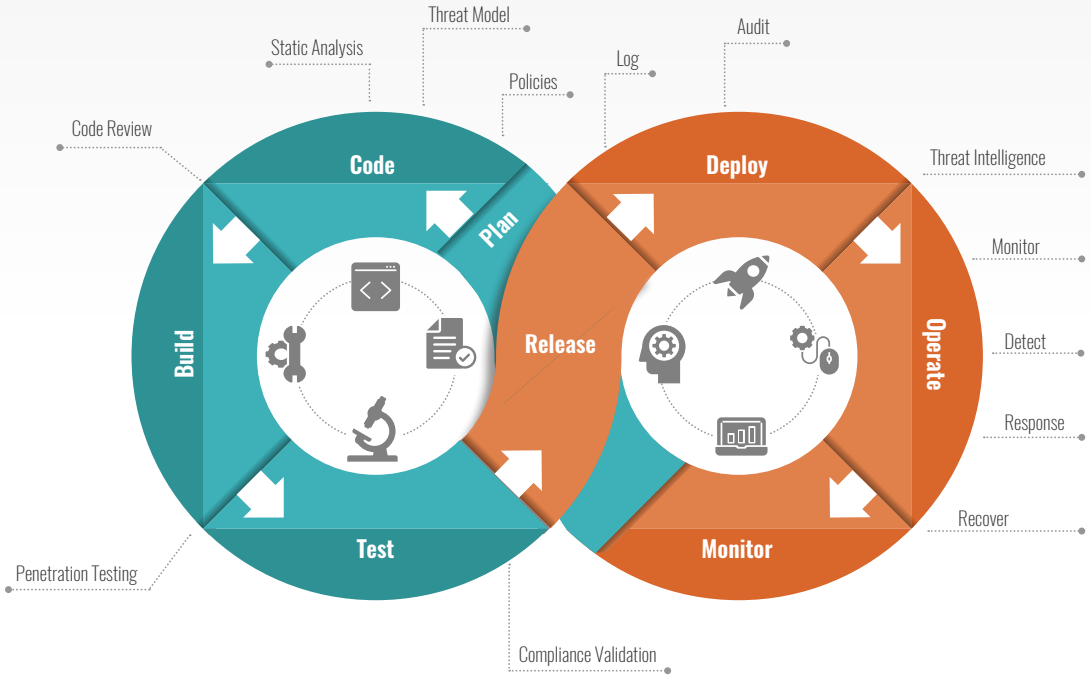


Securing CSPs entails starting an inventory and risk profile, development of policies and procedures around CSPs, security testing, and monitoring. Securing analytics and control backend requires effective practices in software security, continuous monitoring, vulnerability identification and management, and denial of service protection. Finally, securing the operating product involves development of deployment guidance, intellectual property protection, threat intelligence, and incident response capabilities.



A common misconception across organizations is that traditional security controls can still be applied to a CSP environment since defects are fixed at a faster rate. While secure development principles still apply and automated checkpoints need to be built into each phase, the integration point and methodology need to be tailored for adaptation to faster phases and account for the operation's changes.

Deja's approach to connected products is unique because it covers the entire product development lifecycle. Maturing risk management is achieved by integrating an advanced risk identification processes into the development lifecycle, and the threat and vulnerability management processes. When implemented correctly, software security effectively manages the total cost of development and strategically aligns information security with business partners. Our approach can be applied to organizations regardless of their development methodologies or whether they build in-house or use vendors.



HOW CAN DEJA CONSULT AND INNOVATE?

1. Assess and design a CSP security program:

Deja can assess the current product security program maturity, develop a future roadmap, and assess the implementation of a CSP solution.

2. Build and transform a comprehensive CSP security program:

Deja can design a secure CSP development process and integrate it with engineering teams to determine secure requirements, design, development, and testing. Our team can also design and operate a CSP security governance committee to drive the security program, perform proof of concept for security technologies and build architecture to support adoption.

3. Provide managed security services:

Deja can operate security services during the development of the CSPs. Moving to a managed service will allow flexibility to scale the team as new CSP integration and maintenance strategies change, while also increasing quality of existing services to align with senior management initiatives.

ABOUT DEJA VU SECURITY

Deja vu Security is a leader in cybersecurity and risk mitigation for global technology companies, founded on two guiding principles: Over time, all companies will become technology companies, and effective cybersecurity is the foundation of trust for technology companies.

The transition to cloud infrastructure, as well as cadence changes in feature and product updates, have created near-infinite connections between company products and potential bad actors. To help Fortune 50 companies manage risk in this context, Deja has developed programs and processes to ensure the integrity of clients' software and hardware, and to assist in envisioning, deploying, and scaling security programs that address pressing business needs.

WHERE TO GO FROM HERE?

Whether you're looking to build a cybersecurity program from the ground up, or simply looking to strengthen your existing processes, here are some fundamental steps we recommend to help you focus on people, processes, and technology:

- Before you can protect it, you first must acknowledge the nature and type of sensitive data that you have, such as customer payment information, patient health records, personal financial information, and intellectual property.
- You can't protect sensitive information if you don't know where it is. Therefore, identify where sensitive data exists in your environment and build controls around the processes that store, process, or transmit it.
- Create and maintain an inventory of your hardware and software devices. This will enable you to determine which devices in your environment must be updated or patched when critical vulnerabilities are announced.
- Develop and implement a plan to train employees and users on cybersecurity best practices. Ultimately, protection of sensitive data comes down to the end users who are handling it. They must know and understand their responsibilities for protecting sensitive data and interacting securely with the company's computer systems. Additionally, employees must be trained to recognize and report phishing attacks and baiting, and should be well-versed in password management to protect your systems and data.
- Implement multi-factor authentication for external network access to company systems. In most cases, access to sensitive systems and data is protected by only a password. Experience has shown that user-selected passwords are typically easily guessed or can be obtained via a simple e-mail phishing attack.
- Find a trusted partner who can help you. Limited time and staffing are the most common challenges businesses face when it comes to effective cybersecurity. Having a third-party assistance in building or enhancing your cybersecurity program is key to getting an objective validation that your cybersecurity program is effective and that your sensitive data is as secure as possible.

Authored by:
Shahnawaz Sabuwala - Principal Consultant
Akshay Aggarwal - Founder & Executive Chairman