ServiceNow Code Signing with Circle of Trust

The business challenge

Many organizations, regardless of industry, have become digital businesses building mission critical applications for use by their employees and customers. Organizations must take responsibility for the software they produce as it can ultimately be a financial liability as well as have legal consequences. Being a digital business comes with significant vulnerabilities in the form of cyberattacks where malware can be inserted into software and make it look legitimate.

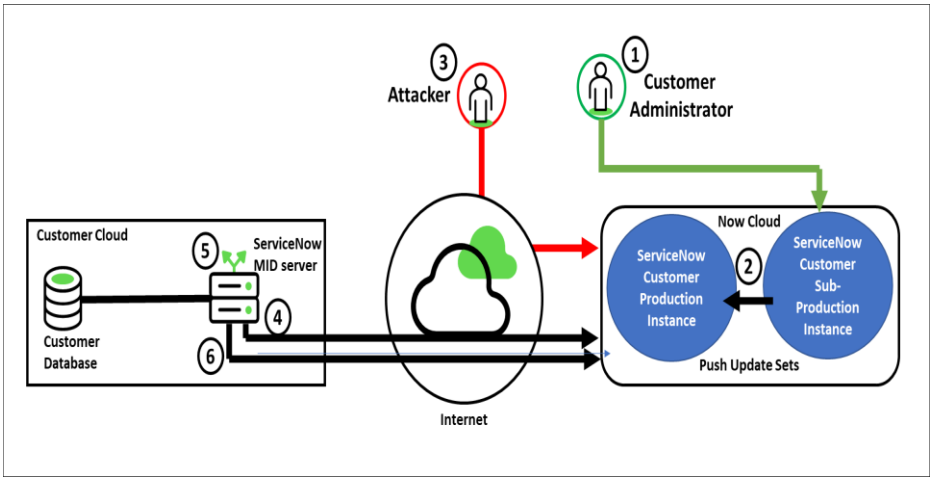
Code signing is a critical security control that provides software with an identity used to verify its authenticity. These credentials are in the form of digital certificates and private keys, both of which must be secured. Unfortunately, many organizations lack the technology and processes needed to ensure these credentials are kept secure. Additionally, a lack of visibility and oversight leaves organizations exposed to threats and attacks by bad actors.

The ServiceNow solution

ServiceNow Code Signing is a key component of the ServiceNow Vault solution. Code Signing improves security by validating sensitive application configuration data and scripts before they are used and executed on the MID Server.

Code Signing creates a digital signature for data and allows the receiving party to verify the authenticity of the sending party as well as to prove the integrity of the message by ensuring it remains untampered.

Organizations can go a step further and create a Circle of Trust (CoT) to identify authorized users who can access the Code Signing feature to prevent malicious actors from disabling or misusing code signing in the event a production instance is compromised.



ServiceNow Code Signing with Circle of Trust

Benefits

Promote trust and ensure unauthorized users cannot manipulate or insert malicious software

Maintain software integrity and prevent software from being tampered with

Ensure authenticity by making sure the receiving party can verify the sending party is the expected entity

Increase security posture and developer confidence with trusted transactions

As an example, an attacker gains access to data sources or to a specific set of records and makes a malicious change to a structured query language (SQL) statement in the customer production instance. The MID Server will find the data source request and execute the malicious SQL change. Executing malicious code can be detrimental (sometimes fatal) to the MID Server and must be avoided at all costs. By using the CoT, system administrators can mitigate vulnerabilities resulting from such a scenario.

As shown in the figure above, the Code Signing feature working in conjunction with the CoT would prevent such breach from occurring.

1. The administrator updates the data source in the sub-production instance and signs the integration records
2. The updated data is pushed from the sub-production instance to the production instance
3. At this point, the attacker tries to update the production instance with malicious statements
4. The MID Server finds the malicious data source request
5. However, it does not execute the request because no digital signature was not found
6. As a result, a message is sent back to the customer's production instance informing the customer there is a problem with the digital signature and further investigation is needed.

Code Signing provides a critical mechanism to enforce only trusted code is deployed and frees organizations from the burden of building gatekeeper components in their deployment pipelines.

Find out more

servicenow.com/products/vault.html

ServiceNow Code Signing signature configuration.

ServiceNow Code Signing certificate details

servicenow