Security for DevOps, Without the Wait

VENAFI

Securing public access to apps requires SSL/TLS certificates from trusted authorities like GlobalSign or DigiCert.

But can you handle the wait?

// The Waiting Game to Get a Public Certificate

// No Process. No Bueno.

Big Risks, Big Delays

- Rogue certificates from unvetted authorities increase risk
- Shortcuts create vulnerabilities from poorly configured certificates
- Software releases delayed when lengthy processes bog you down

More Application Outages

- Expired certificates prevent access and cause service outages
- Unmanaged certificates can be forgotten and cause downtime
- When developers leave, knowledge of certificates they created often goes with them

// Know Your Risks

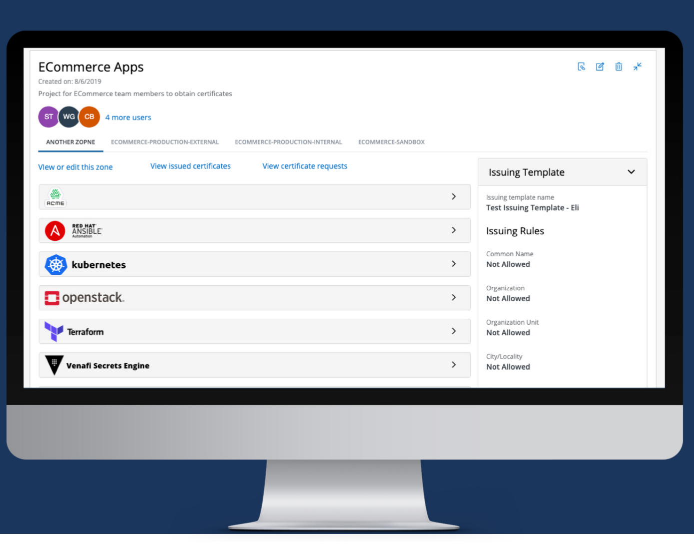
When InfoSec and DevOps Aren't Aligned, Risks Increase

DevOps teams must deliver fast. If a security process slows them down, they may take shortcuts or bypass security altogether.

Risk magnifies when DevOps teams skip issuing certificates. Machine-to-machine connections and communications can no longer be authenticated as trusted systems or encrypted.

// Connect DevOps Tools to Public CAs

With out-of-the-box integrations, developers can issue trusted certificates within CI/CD tools and workflows. This makes it easy to request certificates from leading CAs such as GlobalSign and DigiCert.



// Faster Guardrails from InfoSec

Streamlined processes from InfoSec actually help you go faster. You'll get SSL/TLS certificates in under 5 seconds with no-fuss access from the tools you already use. And InfoSec can still authorize certificate authorities and preset certificate attributes.

How's that for making everyone happy?

Leading CAs
Use CAs your organization trusts

Secure Algorithms
Use InfoSec-approved encryption algorithms

Open Source
Connect your toolchain to certificate issuance

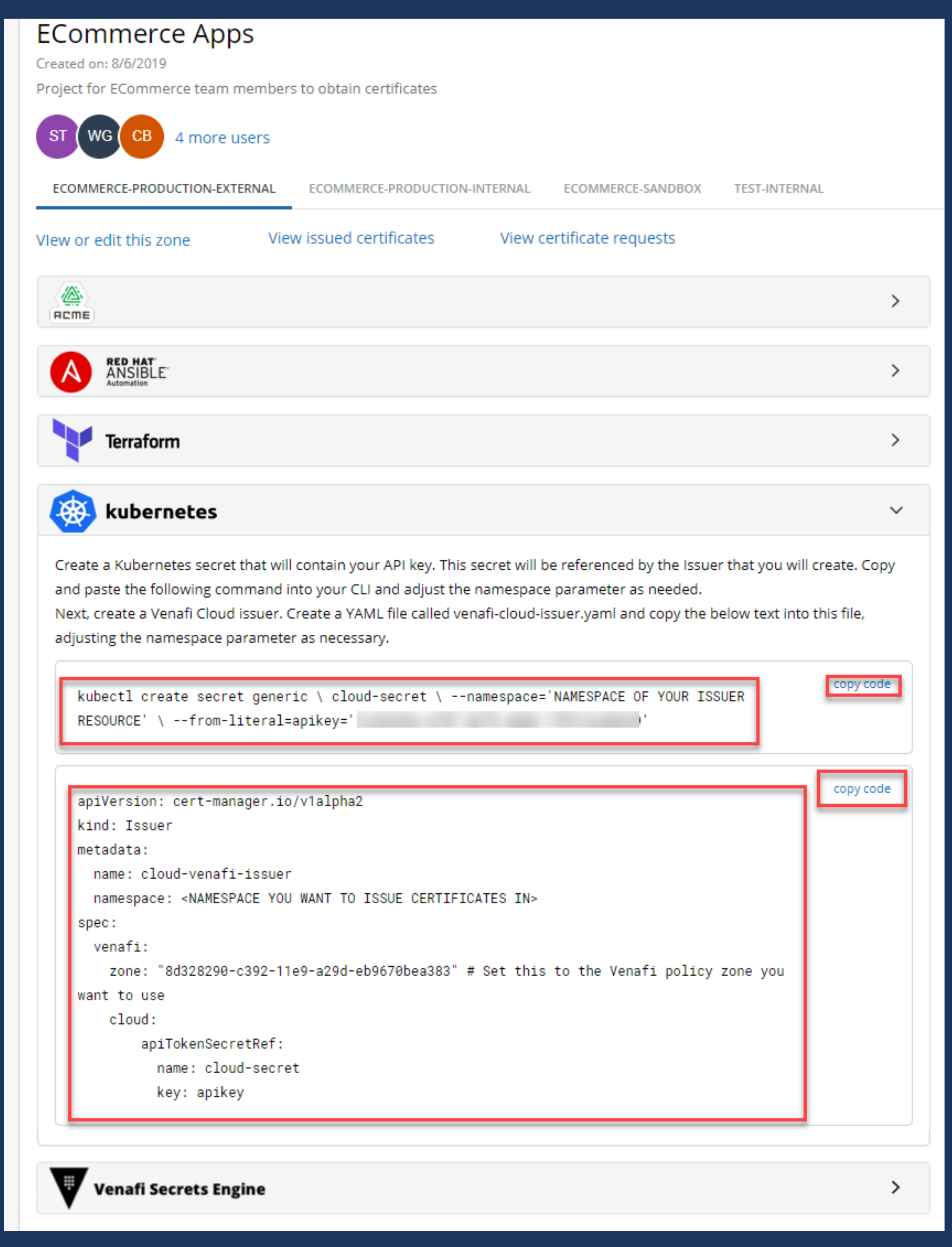
// No Wait. No Bog. Just DevOps.

A new product from Venafi is being introduced in December 2019 to secure DevOps applications. Developers get easy access to certificates. And InfoSec can still set policy and monitor issuance.

Sign up now for an invitation to try it.

How Does It Work? Developers Use a 3-Step Process

+ Select Your Tool



+ Configure Integration

```
kubectl create secret generic \ cloud-secret \ --
namespace='NAMESPACE OF YOUR ISSUER RESOURCE' \ --from-
literal=apikey='[illegible]'
```

+ Get Certificates

- Approved CA
- Enforced Policy
- Secure Encryption
- Auditability

// Request Your Invite for Early Access

Get an invite to receive full access and free certificates from our built-in CA.

Click here or visit https://www.venafi.com/secure-DevOps-without-the-wait

Featured Integrations

kubernetes · JETSTACK · HashiCorp Terraform · HashiCorp Vault · openstack · ANSIBLE · docker · SALTSTACK

See **https://github.com/venafi** for other out-of-the-box integrations & tools.

About Venafi
Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.
venafi.com