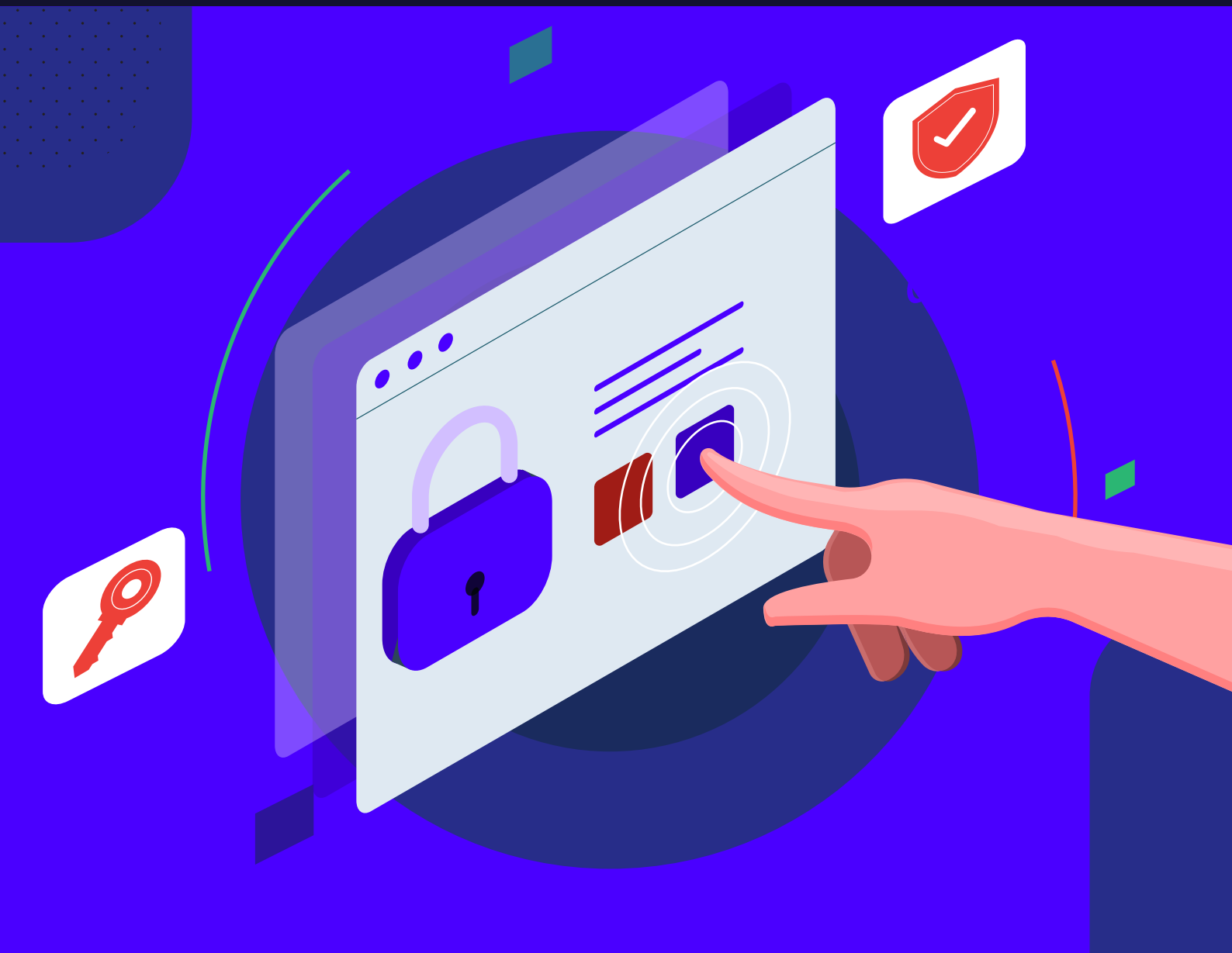
appviewx

APPVIEWX.COM

AppViewX
Smart Discovery

Discover unknown certificates and keys across heterogeneous environments for an enhanced security posture



Overview

The number of machines in the world is increasing and outnumbering the number of people who use them. The sheer number of machine identities that must be secured, including mobile, cloud, and IoT devices, makes keeping machine identities secure a

Digital certificates help identify and control who can access and operate on company networks. With the increase in number of identities in a company, it becomes extremely challenging to manage and protect certificates

Challenges Posed by Unknown Certif-icates

Most of the digital communication is now moved to secure channel and requires digital certificates. While getting a proper certificate requires time and money, technology helps create self-signed certificates for testing purposes. These self-signed certificates can be generated by anyone with great

Temporary certificates might come with third-party software. These temporary certificates are supposed to work for initial testing purposes and should be replace before being pushed into

- **Challenge**

  Creating and deploying digital certificates is easy. Whenever a certificate is needed by a microservice, anybody can deploy certificates. These unmanaged certificates pose serious threat to security

- **Solution**

  Smart Discovery of AppViewX CERT+ discovers certificates in various ways from variety of sources for holistic visibility. CERT+ is a turnkey PKI solution that includes full featured certificate lifecycle management (CLM) as well as workflow automation

- **Benefits**

  Smart Discovery provides visibility into all the certificates used in the origination. Inventory of certificates helps analyze certificates for crypto security standards as well as for expiry dates. This prevents security breaches and application outages.

However, many times because of a slip in the process, these temporary certificates make their way into an organization's infrastructure without the knowledge of the team managing these certificates. At times certificates are deployed by application owners that the centralized security groups or public key infrastructure (PKI) admins might not be aware of or have an inventory of. While rogue, unknown and unmanaged certificates often lead to unplanned application outages, they also serve as easy targets for hackers.

Even for known certificates, many times the hardest part of mitigating a certificate related issue is not identifying the certificate, but it is often locating it on-time. When a certificate is distributed across multi-cloud, heterogeneous environments, it is necessary to capture information such as locations, owners, associated applications, expiry dates, and signatures, diligently to eliminate breaches.

AppViewX Solution Features & Benefits

Gain complete visibility into your certificate infrastructure, and minimize the risk of outages

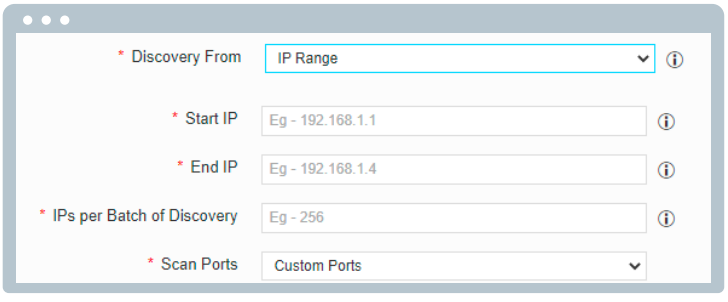
AppViewX CERT+ is a turn-key solution for all PKI needs of an organization. CERT+ discovers certificates from various devices and applications across hybrid-cloud or multi-cloud environments. Unauthenticated network scan as well as authenticated scan of devices, certificate authority (CA) accounts and cloud accounts are used to discover as many certificates as possible. Appropriate knobs are available to balance discovery time and pressure on the network.

Certificate Discovery

AppViewX's smart discovery can help you perform a certificate discovery by two modes – unauthenticated and authenticated.

Unauthenticated Network Scan

As the name suggests, this type of discovery doesn't require any authentication information of network devices. The scan runs on an IP range, a subnet or an URL to identify the certificates being respond on the various IP-Port combinations in the network.



In addition to the certificate information on an IP-Port, CERT+ also identifies the device or application in which the certificate is being used. This discovery process is customized with total pause-resume control to optimize network utilization.

Authenticated Device Scan

Some devices or applications keep certificates with them and present them in specific conditions. Such certificates are difficult to find via network scan. For such certificates, configuration of network devices (load balancer, firewall, web server etc.) is scanned using the authentication credentials of the devices.

Authenticated Cloud Account Scan

Appropriate authentication and authorization into cloud account not only provides access to all the resources using the certificates but also to the internal certificate store. This allows the discovery of most certificates used in that cloud

Authenticated Scan of CA Accounts

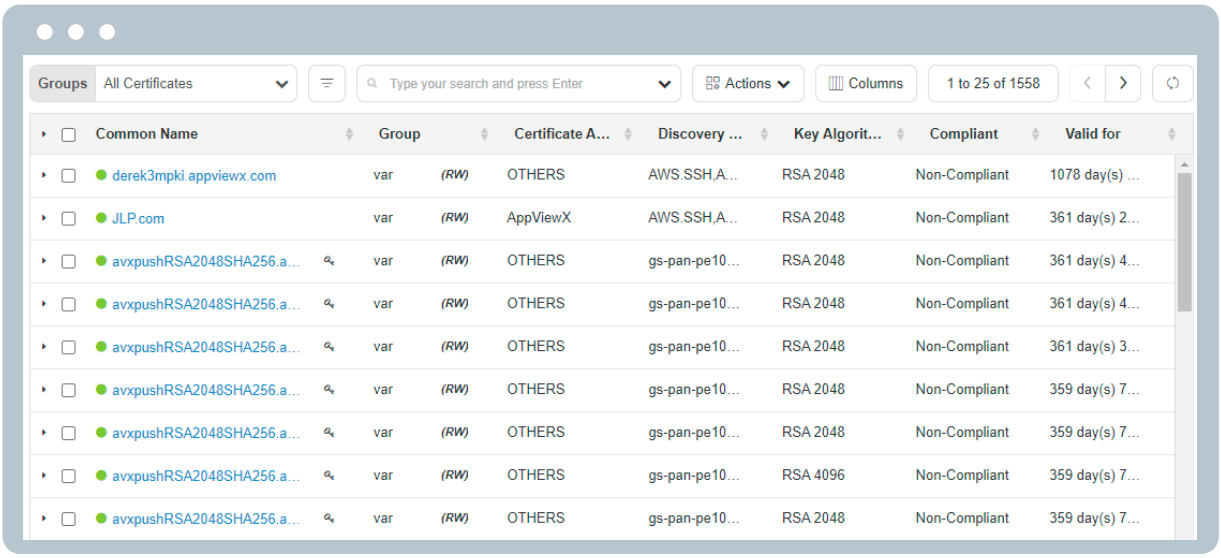
CA accounts are another source of finding the certificates issued for the organizations. However, mapping these certificates to the devices and applications still remains manual efforts unless these certificates are discovered

Import of Reports from 3rd-party Security Scanner

CERT+ can take input of 3rd-party security scanner like Qualys Certificate View, and list certificates from it. This eliminates the requirement of running multiple

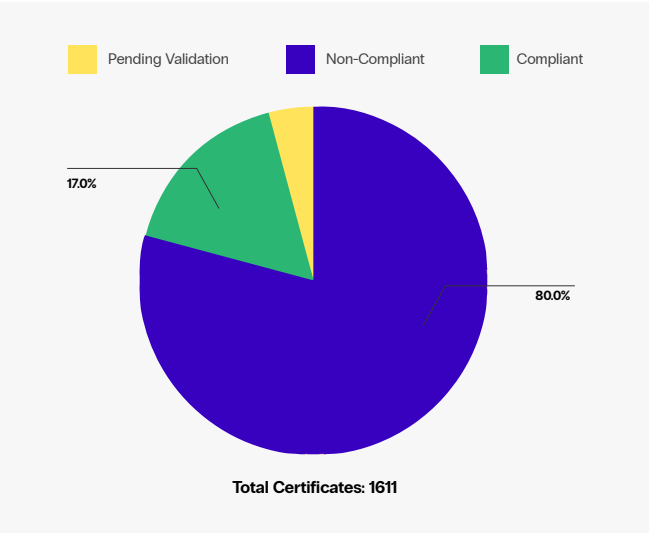
Central Certificate Inventory

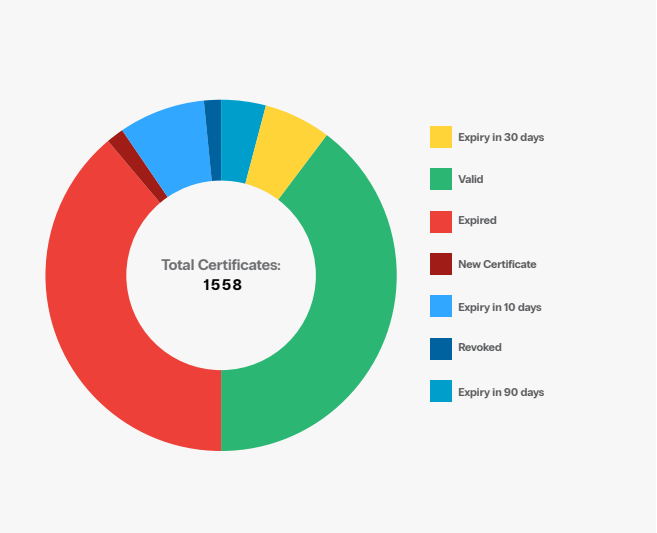
All certificates distributed into various devices and applications across hybrid-cloud or multi-cloud environments come under central inventory. Users can enrich each certificate information with custom information to organize and identify them easily. These certificates can be grouped for administrative



Analytics of Crypto Standards

CERT+ provides analytics about the security standards (e.g. key size, hashing algorithm, cipher strength, allowed TLS protocols etc.) being used in the PKI. The certificates using poor standards are easily identified. Crypto agility provided by CERT+ helps enhancing the security of the PKI without much effort.





Certificate Expiry Analysis & Alerts

CERT+ periodically alerts about the certificates nearing expiration, so that they can be renewed and sudden outage of application can be avoided. CERT+ also provides end-to-end automation for certificate renewal from CA and its provisioning for target device/application.

Solution Consumption Models

CERT+ can either be consumed as a service or CERT+ software can be deployed in the enterprise network. Features, capabilities and benefits of CERT+ remain the same irrespective of how it is being consumed.

SaaS – Operated by AppViewX

Available as a service, the cloud-based CERT+ is fully managed and monitored by AppViewX. Customers can directly get an account on SaaS CERT+ and start using it. For connecting to non-public corporate network segments without poking a hole into corporate firewall, AppViewX Cloud Connector is to be installed in the private network.

On-Prem – Operated by Customer

CERT+ software may also be deployed within a customer's environment in hypervisor based virtual machines (VMs) or private clouds at data centers or public clouds like AWS, GCP and Microsoft Azure etc. CERT+ can be installed on any virtual machine instance running CentOS or RHEL operating system. As CERT+ is a Kubernetes based application, it can also be installed in a managed Kubernetes environment like EKS, AKS, GKE, RedHat Openshift, Rancher etc.

Security simplified with AppViewX

Trusted by one out of every five Fortune 100 companies, AppViewX CERT+ powered by enterprise-grade automation, helps with smart discovery, visibility into security standards and centralized management of certificates and keys across hybrid multi-cloud environments.

Scan QR code to learn more about how AppViewX can be your partner of choice in your cyber security journey

https://www.appviewx.com