YOUR EVALUATION CHECKLIST FOR

KEYFACTOR

PKI & Certificate Management Tools

Find the right tool to manage keys and digital certificates across your enterprise.

Discovery & Inventory

REQUIRED FEATURES

- ☐ Real-time synchronization with internal and public CAs
- ☐ Distributed discovery of SSL/TLS certificates across segmented networks
- ☐ Low-level discovery of key and certificate stores on devices and in the cloud
- ☐ Inventory and management of root of trust (RoT) certificates
- ☐ Discovery of certificates issued by EMM/MDM and IaaS providers

QUESTIONS TO ASK

- Is the solution able to discover certificates across all devices and CAs, regardless of how they were issued?
- How does the solution allow you to deploy and configure network scans to optimize network utilization?
- Does the product integrate with all of your target web servers, load balancers, firewalls, and other systems?
- Does the product offer agent-based and agentless discovery methods?

EVALUATION CRITERIA

- Assess the scope and flexibility of certificate discovery mechanisms
- Assess the impact on existing network and firewall configurations
- List of supported CAs, servers, network appliances and cloud services

Monitoring & Reporting

REQUIRED FEATURES

- ☐ Centralized dashboard to view all certificates from a single pane
- ☐ Fully customizable certificate groups and metadata
- ☐ Automatic notifications for non-compliant or expiring certificates
- ☐ Revocation monitoring for OCSP and CRL expiration
- ☐ Exportable audit logs and integration with SIEM tools

QUESTIONS TO ASK

- Does the vendor provide useful out-of-the-box reports?
- What is the process to schedule expiration alerts and periodic reports for respective certificate owners?
- Does the dashboard provide interactive visuals and drill-down functions?
- Is it possible to search and revoke certificates directly from the console?

EVALUATION CRITERIA

- Review sample dashboards and reports
- Screenshot or demo of custom metadata and groups
- List of supported export formats for audit logs and SIEM integrations

Lifecycle Automation

REQUIRED FEATURES

- ☐ Ability to assign certificate owners and define request/approval workflows
- ☐ Self-service interface(s) for end-user certificate enrollment
- ☐ Automatic renewal and provisioning of certificates to end-devices
- ☐ Ability to add, remove or change CAs without service disruptions
- ☐ Support for lifecycle management of SSH keys and symmetric keys

QUESTIONS TO ASK

- Can the solution manage certificates already issued in my environment?
- Does the solution provide partial or end-to-end automation (i.e. request intake, issuance, provisioning, installation, binding)?
- Does the product use a push or pull model to perform certificate lifecycle tasks? What happens if a device is temporarily unreachable?
- In the event of CA or algorithm compromise, what is the process to replace all affected keys and certificates?

EVALUATION CRITERIA

- Evaluate ease of use for self-service request and approval workflows
- Assess automation capabilities – how much is automated vs manual steps
- List of integrations with ITSM tools for workflows and incident reporting

Ecosystem Integration

REQUIRED FEATURES

- ☐ Integrations with container orchestration frameworks, external key vaults, service meshes, and CI/CD tools
- ☐ Support for IoT and mobile device platforms
- ☐ Support for industry-standard protocols such as SCEP, ACME and others
- ☐ REST API for integration with existing applications and systems

QUESTIONS TO ASK

- How does the product integrate with infrastructure and cloud tools, such as HashiCorp Vault, Kubernetes, Docker Engine and others?
- How does the product integrate with IoT and mobile devices?
- How will “out of the box” integrations work in my production environment?
- Does the product support the level of scale and performance required for Cloud and DevOps integrations?
- Does the vendor provide an open framework for developers to build and deploy custom integrations quickly?

EVALUATION CRITERIA

- Proof of concept (POC) for business-critical integrations
- List of supported out-of-the-box and custom integration capabilities

Policy & Governance

REQUIRED FEATURES

- ☐ Role-based access leveraging users and groups from identity providers
- ☐ Support for on-device and server-side private key generation
- ☐ In-depth auditability of all certificate- and user-related activities
- ☐ Native integrations with privileged access management (PAM) and HSMs

QUESTIONS TO ASK

- Does the solution allow you to configure private key storage and retention policies – including on-device key generation (ODKG)?
- Does the solution allow you to push custom policies, such as device whitelisting or SAN enforcement?
- How does the system allow customers to audit specific events such as configuration changes, user activities or certificate-related events?

EVALUATION CRITERIA

- Assess access controls, policy and governance capabilities
- Review detailed auditing capabilities
- List of supported PAM/ secrets vaults and HSM providers

Cloud-Hosted PKI as-a-Service

REQUIRED FEATURES

- ☐ Dedicated offline root CA hosted in a highly secure facility
- ☐ Single-tenant, cloud-hosted CA and revocation infrastructure
- ☐ Built-in HSMs for key protection on root and issuing CAs
- ☐ High availability (HA) and disaster recovery (DR)
- ☐ 24/7 service monitoring by trained and dedicated PKI experts

QUESTIONS TO ASK

- Does the vendor offer the option of fully managed or hosted PKI combined with certificate management?
- Is it a dedicated or shared infrastructure deployment?
- What arrangements are included for physical security, access controls, disaster recovery, and high availability?
- Does the vendor allow customers to retain control of root CA keys and recovery materials?
- How experienced is the PKI operations and support team?

EVALUATION CRITERIA

- Service Level Agreements (SLAs)
- SOC 2 Type II compliance
- Certificate Policy and Certificate Practice Statement (CP/CPS)

Architecture & Deployment

REQUIRED FEATURES

- ☐ Modular, distributed and highly scalable solution architecture
- ☐ Consistent certificate discovery and orchestration framework across all CAs
- ☐ Ability to deploy the product on-prem, in the cloud, or as-a-service
- ☐ Ability to implement the product without re-issuing certificates

QUESTIONS TO ASK

- How long does it take for the product to be fully operational?
- How difficult and time-consuming is it to run the solution?
- What additional hardware and software and network enhancements are required to implement the product?
- How many certificate transactions per second can the architecture handle in high-scale environments?

EVALUATION CRITERIA

- Average time to deploy or time to value
- Required infrastructure and certificate workflow changes
- Proof of performance in high-volume certificate deployments

Customer Support & Pricing

REQUIRED FEATURES

- ☐ 24/7 technical support with guaranteed response times
- ☐ Dedicated customer success and solution delivery teams
- ☐ No hidden infrastructure costs (hosted PKI)
- ☐ No per-certificate fees (certificate management)

QUESTIONS TO ASK

- What are the technical support options, policies and procedures?
- Does the vendor have a dedicated delivery and implementation team to ensure proper deployment?
- Does the vendor provide basic training and regular health checks?
- Does the customer incur additional costs if the number of certificates under management grows?
- What results are other customers experiencing?

EVALUATION CRITERIA

- Service Level Agreements (SLAs)
- Available references and reviews
- Customer satisfaction and retention rates

KEYFACTOR

Keyfactor empowers enterprises of all sizes to prevent the breaches, outages and failed audits from digital certificates and keys that impact your brand loyalty and bottom line. Powered by the industry's only PKI as-a-service platform, IT and infosec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale.

▶ www.keyfactor.com
▶ +1.216.785.2990