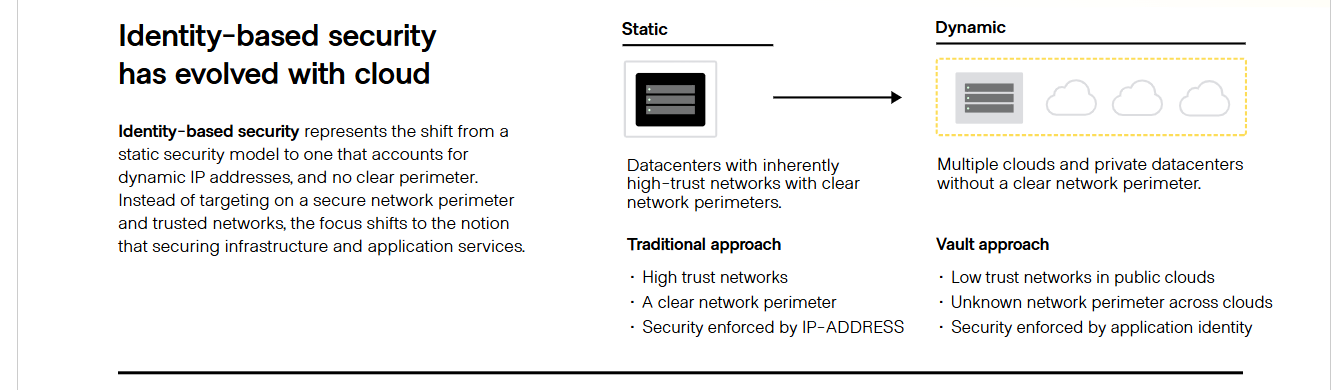
**Headline:** Public Key Infrastructure (PKI)

**Subtext (Single Line):** Centralize certificate lifecycle management to control digital certificates within your infrastructure and application stack.

**Alternative:** PKI enhances data integrity by utilizing digital signatures to verify data authenticity.



**Left Block Headline:** Enhance identity-based security with PKI.

**Left Block:** PKI strengthens identity-based security to better protect sensitive information and resources. PKI provides a robust identification verification method not subject to attacks and human errors that often come with user-password credentials. PKI-enabled digital certificates are routinely used to authenticate, digitally sign, and encrypt credit cards, passports, e-commerce websites, connected devices, and much more, shielding them from compromise or breach.

**Middle Block Headline:** PKI Automation

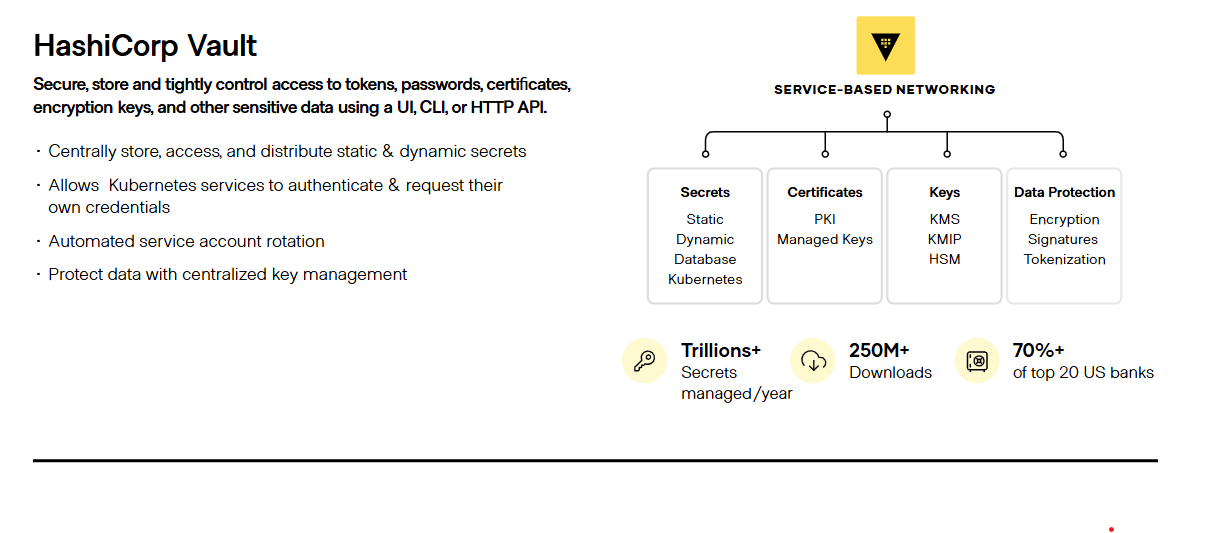
**Middle Block:** PKI automation provides significant benefits allowing organizations to manage certificates at scale, reducing the risk of security breaches and compliance issues. Key benefits include:

* Reduces human error
* Centralized management
* Scalability
* Visibility and Control

**Right Block Headline:** Zero Trust Security

**Right Block:** PKI is a crucial component of a resilient Zero Trust architecture by enabling user and device authentication through digital certificates to mitigate risks associated with weak passwords and compromised credentials. PKI improves Zero Trust Security by:

* Authenticating users and devices
* Securing communications
* Improving data integrity

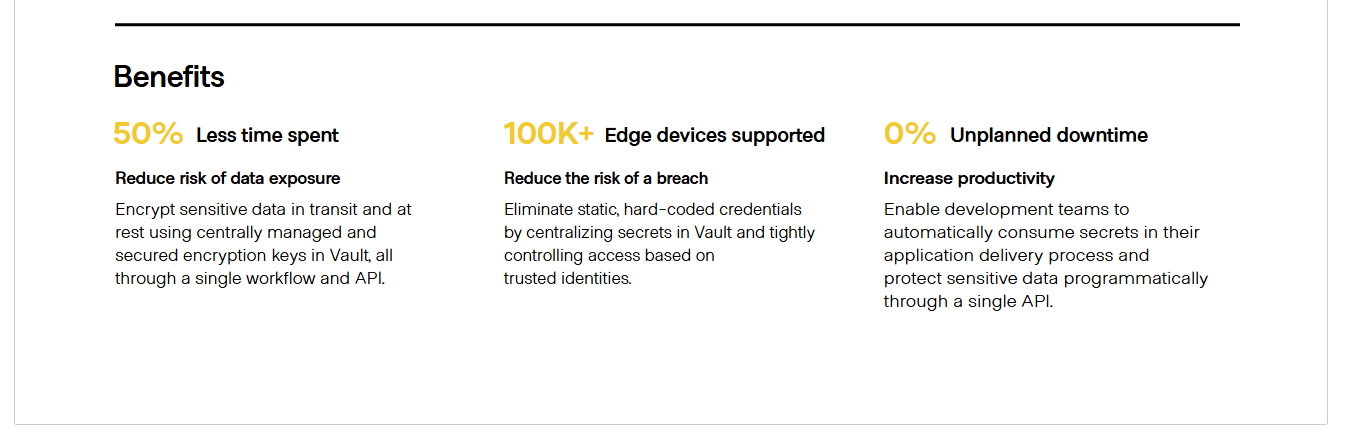


**Left Block Headline:** PKI Trends

**Left Block Sub-Headline:** The increased digitalization of enterprises and identity are driving PKI usage.

**Left Block Bullets:**

* **Internet-of-Things (IoT):** The proliferation of IOT devices along with the associated threats such as altering a device function, means that significant efforts are needed for IOT vulnerability management. PKI is expected to play a major role here since these devices will primarily rely on digital certificates for identification and authentication.
* **Cloud Adoption:** With organizations moving an increasing number of workloads to the cloud, the need for PKI credentials for cloud-based applications is going up correspondingly.
* **DevOps:** DevOps teams can automatically provision public and private SSL certificates to ensure the identity, integrity and authentication of applications, services, and infrastructure. HashiCorp Vault integrates with DevOps tools platform through RESTful APIs to reduce manual certificate management.



**Headline:** Benefits

**Left Block Headline: Centralized Certificates Management**

**Left Block Text:** Discover and manage the complete lifecycle of your certificates. Issue, renew, and revoke certificates from a single control plane.

**Middle Block Headline:** Increased Trust

**Middle Block Text:** Verifying identity is at the foundation of Public Key Infrastructure (PKI). PKI ensures authenticity and integrity of the users or devices being secured. When a user identity is verified or authenticated using PKI certificates, an organization can be assured that only authorized individuals are accessing their applications and infrastructure. Identity verification prevents unintended or malicious actors from disrupting systems or networks, therefore providing greater security and trust for organizations.

**Right Block Headline:** Data Integrity

**Right Block Text:** PKI’s digital signatures ensure data integrity, confirming it is untampered and consistent with its original signature—essential for enterprises addressing security and compliance mandates.