YUBICO YubiHSM 2 v2.4 USB-Sicherheitsschlüssel

Artikelnummer	999892065
Gewicht	1kg
Länge	1mm
Breite	1mm
Höhe	1mm

Produktbeschreibung

YUBICO YubiHSM 2 v2.4 USB-Sicherheitsschlüssel

Produktbeschreibung:

Schutz für kryptografische Schlüssel
mit dem kleinsten Hardware-Sicherheitsmodul (HSM)
der WeltDas YubiHSM 2 ist erhältlich als
FIPS 140-2 Level-3 validierte /
zertifizierte Lösung sowie als Nicht-FIPS
zertifizierte Lösung.
Beide Produktlinien haben aber die gleichen Funktionen.
Beide Lösungen gewährleisten kompromisslose
kryptografische HardwareSicherheit für Anwendungen,
Server und und Computergeräte YubiHSM 2 YubiHSM
2 FIPS zu einem Bruchteil der Kosten und Größe
von traditionellen HSMs. In Software gespeicherte
kryptografische Schlüssel sind gegenüber
Bedrohungen anfällig. Die Kosten der weltweiten
Cyberkriminalität werden sich im Jahr 2021
voraussichtlich auf 6 Billionen US-Dollar belaufen,
ein Anstieg von 3 Billionen US-Dollar im Jahr 20151 .
Die Speicherung kryptografischer Schlüssel
für Server in Software wird immer anfälliger
für immer ausgefeiltere Angriffe.
Der Diebstahl kryptografischer Schlüssel
von einem Server kann ein katastrophales Datenleck
zur Folge haben.
Wenn beispielsweise ein privater Schlüssel
von einer Zertifizierungsstelle kompromittiert wurde,
kann ein Angreifer eine Phishing Site online nehmen,
die sich als Ihre Website ausgibt. ,Das YubiHSM
2 und das YubiHSM 2 FIPS setzen einen neuen Maßstab
für effektive SchlüsselsicherheitSichern
Sie die Speicherung von kryptografischen Schlüsseln

und Operationen für Anwendungen,
Server und Computer in Hardware und eliminieren
Sie gleichzeitig die Kosten und die Komplexität
traditioneller Hardware-Sicherheitsmodule (HSMs).
Die HSM-Lösungen von Yubico sind manipulationssicher
und bieten einen kostengünstigen,
hochsicheren ROI in tragbaren &lsquo,Nano&rsquo,-Formfaktor,
der einen flexiblen Einsatz auf verschiedenen
Geräten und Standorten möglich macht.
Mit dem YubiHSM 2 und YubiHSM 2 FIPS können
Unternehmen verhindern,
dass kryptografische Schlüssel von Angreifern,
Malware und böswilligen Insidern kopiert werden.
Unternehmen können mit Hilfe des Open Source
SDKs schnell eigene Lö,sungen entwickeln oder
vorhandende Systeme einfach integrieren.Sicherer
Hardware-Schutz fü,r Kryptografische Schlü,sselIn
Software gespeicherte kryptografische Schlü,ssel
kö,nnen kopiert werden und sind anfä,llig
fü,r versehentliche Weitergabe und den Diebstahl
aus der Ferne.
Ohne strenge Kontrolle ist es fü,r Administratoren
oder bö,swillige Insider ein Leichtes Schlü,ssel
auf USB-Sticks zu sichern,
sie per FTP zu ü,bertragen oder sie mit anderen
ü,ber einen Cloud-Speicherdienst zu teilen.
Auß,erdem kö,nnen raffinierte Angreifer
so Admin-Zugriff erlangen oder Trojaner-Malware
einsetzen die sich auf Servern ,installiert,
nach kryptografischen Schlü,sseln sucht und
diese dann zum Verkauf auf Dark-Web-Seiten wie
Alphabay kopiert.
YubiHSM2 und YubiHSM2 FIPS ermö,glichen eine
sichere Schlü,sselspeicherung und Betrieb,
indem sie das versehentliche Kopieren und Verteilen
von von Schlü,sseln und verhindern den Diebstahl
von gespeicherten Schlü,sseln aus der Ferne.
? Sichere Schlü,sselspeicherung und -operationen
auf manipulationssicherer Hardware,
mit Audit-Protokollierung. ? Umfangreiche kryptografische
Funktionen einschließ,lich Hashing,
Key Wrapping, asymmetrisches Signieren, Entschlü,sselung,
Attestierung und mehr.Innovatives Design fü,r
flexiblen EinsatzHerkö,mmliche rackmontierte
und kartenbasierte HSMs sind fü,r viele Organisationen
nicht praktikabel fü,r viele Unternehmen nicht praktikabel,
da die Grö,ß,e und Komplexitä,t der HSMs.
Hinzu kommt, Serverschrä,nke mit Metallgittertü,ren,
um den Zugang zu sichern. Serverschrä,nke
mit Metallgittertü,ren zur Sicherung des Zugangs
was den verfü,gbaren Platz einschrä,nkt.
Mit den HSM-Lö,sungen von Yubico kö,nnen
Unternehmen problemlos Server,
Anwendungen, Datenbanken, Fließ,bä,nder,
IoT-Gerä,te Kryptowä,hrungsbö,rsen
und mehr mit einem tragbaren &lsquo,Nano Formfaktor,
der einen schnellen und flexiblen Einsatz in verschiedenen
Umgebungen Der YubiHSM 2 oder YubiHSM 2 FIPS passt

problemlos in einen USB Steckplatz und liegt fast bü,ndig,
um physikalische Sicherheits Gehä,usen. ?
Der &lsquo,Nano&rsquo,-Formfaktor ermö,glicht
eine flexible Bereitstellung und Nutzung ü,ber
Gerä,te und Standorte hinweg ? Vollstä,ndig
verdeckter Einsatz des USB-A-Ports ? Netzwerkfreigabe
zur Nutzung durch Anwendungen auf anderen ServernNiedrige Kosten,
hoher Sicherheits-ROIIn Software gespeicherte
kryptografische Schlü,ssel sind anfä,llig
fü,r Hacker und Malware-Angriffe.
Alternativ kö,nnen herkö,mmliche HSMs
kostspielig in der Bereitstellung sein.
Mit den HSM-Lö,sungen von Yubico erhalten
Unternehmen eine hohe kryptografische Sicherheit
und einen Betrieb ohne dem traditionellen HSM-Preisschild. ,Schnelle Integration,
einfache VerwaltungMit dem YubiHSM 2 SDK kö,nnen
Entwickler schnell die Unterstü,tzung fü,r
die FIPS- oder Nicht-FIPS-Version des HSM in Unternehmensprodukte
und -anwendungen integrieren,
mit Funktionen wie Generieren und Importieren
von Schlü,sseln,
Signieren und Verifizieren sowie Verschlü,sselung
und Entschlü,sselung.
Entwickler kö,nnen diese Funktionen auch Funktionen
ü,ber den Industriestandard PKCS#11 zugä,nglich
machen.Abdeckung aktueller und zukü,nftiger
Anwendungsfä,lleSicherer Umtausch von Kryptowä,hrungen:
Der Kryptowä,hrungsmarkt verzeichnet ein rasantes
Wachstum und erreicht 2018 voraussichtlich einen
Marktwert in Hö,he von 1 Milliarde US-Dollar.
Dieses enorme Wachstum ist auch mit zahlreichen
Assets verbunden,
die vor Sicherheitsrisiken geschü,tzt werden mü,ssen.
Bei mehreren Kryptowä,hrungsbö,rsen ist
es zu Datenlecks gekommen.Diese Datenlecks nehmen
stets zu und hä,tten allesamt mö,glicherweise
mit einem Best Practice-Sicherheitsansatz unter
Beteiligung eines Hardwaresicherheitsmoduls verhindert
werden kö,nnen.
Mit dem YubiHSM 2-SDK kö,nnen Entwickler von
Lö,sungen fü,r Kryptowä,hrungsbö,rsen
das HSM schnell integrieren,
um kryptografische Schlü,ssel und sensible
Finanzdaten zu schü,tzen.Sichere Internet
of Things-(IoT-)Umgebungen: Das Internet der Dinge
(Internet of Things,
IoT) ist ebenfalls ein schnell wachsender Markt,
in dem Systeme oft in gefä,hrdeten Umgebungen
betrieben werden.
Dabei ist die Sicherung kryptografischer Schlü,ssel
noch wichtiger,
da Unternehmen sensible Informationen schü,tzen mü,ssen.
Kryptografische Schlü,ssel werden in zahlreichen
IoT-Anwendungen mit nur unzureichenden Sicherheitsmaß,nahmen verwendet.
Das ist teilweise darauf zurü,ckzufü,hren,
dass der Schutz kryptografischer Schlü,ssel
und die Registrierung von Zertifikaten bei IoT-Gateways
oder -Proxys bisher kompliziert waren ,und

traditionelle HSMs zu groß,
und sperrig fü,r bestimmte IoT-Umgebungen
wie vernetzte Autos sind.
Mit dem OpenSource-SDK kö,nnen Entwickler
von IoT-Anwendungen das tragbare YubiHSM 2 oder
YubiHSM 2 FIPS schnell integrieren,
um kryptografische Schlü,ssel zu schü,tzen
und die feindliche Ü,bernahme kritischer IoT-Umgebungen
zu verhindern.Sichere Cloud-Services: Hohe Sicherheit
fü,r Cloud-Umgebungen ist unerlä,sslich,
da Organisationen sicherstellen mü,ssen, dass
ihre Daten in der Cloud geschü,tzt werden.
Das HSM kann in einem Rechenzentrum bereitgestellt
und als Komponente einer Cloud-Infrastruktur eingesetzt werden.
Unternehmen kö,nnen sich entspannt zurü,cklehnen,
wenn ihr Cloud-Serviceanbieter das YubiHSM 2 im
Rahmen seines Angebots verwendet.Sichere Microsoft
Active Directory-Zertifikatdienste: Das HSM kann
kryptografische Schlü,ssel fü,r die Microsoft-basierte
PKI-Implementierung eines Unternehmens sicher
bereitstellen.
Das HSM fü,r Microsoft Active Directory Zertifikatsservices
schü,tzt dabei nicht nur die privaten Schlü,ssel
der Zertifizierungsstelle,
sondern auch alle Signatur- und Verifizierungvorgä,nge
die den privaten Schlü,ssel nutzen.ZusammenfassungMit
dem YubiHSM 2 und YubiHSM 2 FIPS kö,nnen Unternehmen
aller Grö,ß,enordnungen die Sicherheit
kryptografischer Schlü,ssel im gesamten Lebenszyklus verbessern,
Risiken mindern und die Einhaltung gesetzlicher
Vorschriften sicherstellen.
Mit dem als Open-Source-SDK verfü,gbaren YubiHSM
SDK 2.0 kö,nnen Unternehmen Unterstü,tzung
fü,r das YubiHSM 2 einfach und schnell in
zahlreiche Plattformen und Systeme integrieren,
und zwar fü,r aktuelle und zukü,nftige
Anwendungsfä,lle mit hö,chsten Sicherheitsanforderungen.
Technische Details:

Allgemeines
Typ
Schloss / Zutrittskontrolle

Produkteigenschaften

Farbkategorie	Gold, Schwarz
Zubehörkategorie	Sicherheitsprodukte für Computer, Desktop-Computer und Serverzubehör
Gewicht	1 g
Service und Support - Typ	1 Jahr Garantie

Weitere Bilder