

40 Cybersecurity Questions to Ask Your Security Vendor (And Your Team) Before Buying

Whether you're looking at pure cloud, hybrid cloud, or traditional physical security systems, make sure your setup remains strong long-term with these 40 cybersecurity questions.



Category	Question	Yes	No	Notes
Network Security & Encryption	Are the vendor's systems configured to use the Zero Trust model?	<input type="checkbox"/>	<input type="checkbox"/>	
	Is the data encrypted both in transit and at rest? If so, which ciphers does the vendor use?	<input type="checkbox"/>	<input type="checkbox"/>	
	Do devices on the system make outbound connections only? If not, what types of inbound connections are necessary to use the platform?	<input type="checkbox"/>	<input type="checkbox"/>	
Updates & Patch Management	Are backend services continuously and automatically updated with the latest security patches?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor provide patches and upgrades on a regular cadence? If so, what is the frequency?	<input type="checkbox"/>	<input type="checkbox"/>	
Compliance & Testing	Is the vendor SOC 2 Type I and Type II compliant?	<input type="checkbox"/>	<input type="checkbox"/>	
	Is the vendor FY2019 NDAA compliant?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor perform quarterly penetration testing? If not, how frequently do they perform penetration tests?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor offer a Bug Bounty program?	<input type="checkbox"/>	<input type="checkbox"/>	
Industry-Specific Regulatory Compliance (if relevant)	Is the vendor FedRAMP authorized?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor help you maintain HIPAA compliance?	<input type="checkbox"/>	<input type="checkbox"/>	
	Can the vendor consider or sign BAA agreements?	<input type="checkbox"/>	<input type="checkbox"/>	
	Can the vendor help you meet PCI requirements?	<input type="checkbox"/>	<input type="checkbox"/>	



Category	Question	Yes	No	Notes
Authentication & Access	Does the vendor support multi-factor authentication?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor offer self-serve SSO/SAML/SCIM protocols?	<input type="checkbox"/>	<input type="checkbox"/>	
	What is the physical location in which the data is stored? (Where are the servers located?)	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor use industry-leading cloud service providers like AWS or Microsoft Azure? If not, which cloud service provider does the vendor use?	<input type="checkbox"/>	<input type="checkbox"/>	
	Do the vendor's data center locations comply with GDPR?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor allow you to set users' session durations?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor allow you to create and assign user groups, each with specific permissions?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor's system have a default or base username and password that cannot be changed?	<input type="checkbox"/>	<input type="checkbox"/>	
Data Management & Privacy	Does the vendor's system have a default or base username and password that cannot be changed?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor refrain from monetizing customers' private data?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor have easily accessible policies on data retention and deletion? What are they?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor's solution require any collection of personal data (PII)?	<input type="checkbox"/>	<input type="checkbox"/>	
Vendor Management & Supply Chain Security	Does the vendor offer configuration management tools?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor offer enhanced audit logging?	<input type="checkbox"/>	<input type="checkbox"/>	
	Will the vendor detail its external, third-party dependencies? If so, what are they?	<input type="checkbox"/>	<input type="checkbox"/>	



Category	Question	Yes	No	Notes
Service Features & Infrastructure	Does the solution allow you to enable, disable, or permanently remove select features for compliance, security, or privacy purposes?	<input type="checkbox"/>	<input type="checkbox"/>	
	If the solution is multi-tenant, can the vendor detail how customer data is segregated?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor offer 24x7 support?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor have a disaster recovery procedure?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does the vendor have a change control process?	<input type="checkbox"/>	<input type="checkbox"/>	
	Do the devices require a direct ethernet connection?	<input type="checkbox"/>	<input type="checkbox"/>	
	Will the vendor tell you how many customers have deployed their solution? If so, how many?	<input type="checkbox"/>	<input type="checkbox"/>	
Your Company's Internal Processes	Does the vendor have bandwidth requirements? If so, what are they?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does your company give privacy and data protection training to your employees on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>	
	Do your employees have the ability to access internal data? If so, what controls are in place?	<input type="checkbox"/>	<input type="checkbox"/>	
	Do you have tightened controls around your supply-chain and manufacturing parts? What are they?	<input type="checkbox"/>	<input type="checkbox"/>	
	How do you manage and control access to encryption keys? Who within your organization has access to these keys?	<input type="checkbox"/>	<input type="checkbox"/>	
	Does your company use sub-processors or subcontractors?	<input type="checkbox"/>	<input type="checkbox"/>	