BeyondTrust Compliance Chart

PRODUCT KEY: PPM = Privileged Password Management | EPM = Endpoint Privilege Management | SRA = Secure Remote Access

	THE REQUIREMENT	BEYONDTRUST PLATFORM			CIS	PCI	NIST	HIPAA	GDPR
		PPM	EPM	SRA					
PROTECT	Implement only one primary function per server and enable only necessary service, protocols, daemons etc. as required for the function of the system.	●	●	●	3.4, 9.1, 15.6	2.2.1-2.2.2			
	Prevent unauthorized users from obtaining access and ensure proper authentication for use	●		●	5.6, 11.4, 12.6	8.3		164.308(3) (i)	Article 5, Article 25, Article 32
	Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.			◗	11.7	2.2, 4.1, 6.2	AC-4, CA-3, CA-7, CA-9, CM-2, CM-3, CM-5, CM-6, CM-8, MA-4, SC-24, SI-4		
	Implement procedures for storing, creating, changing, and safeguarding passwords.	●		●				164.308(iii) (D)	
CONTROL	Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	●	●	●	5.1, 5.2, 5.8	2.1, 7.1-7.2, 8.1-8.3, 8.7	AC-2, AC-6, AC-17, AC-19, CA-7, IA-4, IA-5, SI-4	164.310(b), 164.310(c), 164.412 (A) (1), 164.308(3) (c), 164.312 (2) (i)	Article 5, Article 25, Article 32
	Actively manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.			◗	11.4, 11.5, 11.6, 11.7				
	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	●		●	1.1, 1.3, 1.4				
	Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	●			16.6	8.2.1, 8.2.3, 8.2.4, 8.2.5, 8.2.6		164.308 (5) (D)	
	Assign all users a unique ID before allowing them to access critical systems and data and control the addition, deletion and modification of those IDs and credentials.	●		●	3.5	8.1.1, 8.1.2, 8.1.3	AC-5	164.312 (a) (2)(i)	Article 5, Article 25, Article 32
AUDIT & ANALYZE	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.	◗			4.1, 4.2, 4.3, 4.4			164.308(1) (D)	Article 25
	Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	●		●	12.10, 13.3	10.5		164.310 (a)(1)	Article 5, Article 25, Article 32, Article 33
	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. Audit logs should specify user identification, type of event, date and time.	●	●	●	16.3, 16.8, 16.14	10.1, 10.2, 10.2.2, 10.2.3, 10.2.4, 10.3	AU-2, AU-3, AU-6, AU-7, AU-14	164.308 (5)(C)	Article 25, Article 33
	Implement procedures for monitoring log-in attempts and reporting discrepancies.	●	●	●	16.7, 16.8			164.308 (5)(C)	Article 25, Article 32
	Perform periodic evaluations to identify and evaluate evolving malware threats. Ensure all system components and software are protected from known vulnerabilities and install critical security patches within one month of release.	◗			8.1, 8.2, 8.5	5.1, 5.2, 6.2			