baramundi

CHECKLISTY BARAMUNDI zapewniają zwięzłe i szczegółowe wskazówki ekspertów odnoszące się do częstych pytań i problemów. Więcej z nich można znaleźć na stronie www.baramundi.com/checklisty

7 kroków do wdrożenia i skonfigurowania BitLockera

Szyfrowanie dysków za pomocą Microsoft BitLocker zapewnia niezawodną ochronę i bezpieczeństwo wrażliwych danych firmowych. Oto 7-etapowa lista kontrolna wyjaśniająca, w jaki sposób wprowadzić i skonfigurować tę usługę tak, aby spełniała Twoje wymagania.

Sprawdź sprzęt i określ wytyczne

Sprawdź, czy urządzenia końcowe spełniają wymagania BitLockera, w tym odpowiedni układ TPM, BIOS lub wsparcie UEFI, formaty dysków czy wersje systemu Windows. Określ wytyczne dotyczące użytkowania i tego, które urządzenia, np. notebooki, muszą być szyfrowane.

Uruchomienie testowe krok po kroku

Zaplanuj stopniowe wdrażanie i testy na poszczególnych urządzeniach. Zainstaluj BitLockera na wszystkich urządzeniach dopiero po upewnieniu się, że są one kompatybilne, a użytkownicy nie będą mieli problemów z uzyskaniem do nich dostępu.

Centralna aktywacja podczas instalacji systemu operacyjnego

Najlepszym sposobem na wdrożenie BitLockera jest aktywowanie go podczas instalacji systemu operacyjnego ze scentralizowanego panelu administracyjnego. Oszczędza to czas i ułatwia zadanie.

Odblokowanie sieci

Aktywuj funkcję odblokowania sieci, aby systemy podłączone do bezpiecznej sieci firmy mogły uruchamiać się automatycznie bez konieczności wprowadzania kodu PIN. Dzięki temu system jest chroniony, a użytkownicy są bardziej zadowoleni.

Wstrzymanie BitLockera podczas wdrażania oprogramowania

Pamiętaj, aby wstrzymać lub zawiesić działanie BitLockera podczas instalowania lub aktualizowania oprogramowania, np. firmware, a także aplikacji innych firm W przeciwnym razie zautomatyzowane instalacje zawieszą się oczekując podania jego kodu PIN. Pamiętaj, aby wznowić działanie funkcji BitLocker po zakończeniu instalacji.

Centralne zapisywanie kluczy odzyskiwania

Przechowuj klucze odzyskiwania BitLockera w centralnej, bezpiecznej lokalizacji, która będzie łatwo dostępna dla upoważnionych osób z zespołu IT. Dzięki temu pracownicy będą mogli szybko odzyskać dostęp do swoich zasobów w przypadku zapomnienia hasła lub zmiany sprzętu.

Szkolenie dla użytkowników końcowych i pomocy technicznej

Powiadom wszystkich użytkowników końcowych o BitLockerze i jego zaletach. Być może trzeba będzie również poinformować ich o zmienionych procedurach logowania. Przygotuj zespół pomocy technicznej do zwiększonej ilości pytań i problemów związanych z BitLockerem.

W skrócie: Skuteczne wprowadzenie i aktywacja BitLockera znacznie zwiększa bezpieczeństwo danych firmowych. Niniejsza checklista oraz moduł baramundi Defense Control pomogą w sprawnym i niezawodnym wdrożeniu.