

# 9 მიზეზი

თუ რაბომ სჭირდება თქვენს ორგანიზაციას  
**PAM360**



სახელმძღვანელო

2024

Since 2015

## თუ ამ გამოწვევებიდან თქვენს ორგანიზაციაში 3 მათგანს მაინც აწყდებით:

- 1 ორგანიზაციის ინფრასტრუქტურაზე დაუცველი წვდომების გაცემა;
- 2 ორგანიზაციის ინფრასტრუქტურაზე დაუცველი წვდომების აღმოჩენა;
- 3 ორგანიზაციის ინფრასტრუქტურაზე დროებითი წვდომის მიმდინარეობის მენეჯმენტი (მაგ: დროის ლიმიტის, ექსუნთების, პაროლების კონტროლი);
- 4 გაცემული დროებითი წვდომების მიმდინარეობის მონიტორინგი;
- 5 გაცემული დროებითი წვდომების მიმდინარეობის ჩანაწერების არარსებობა;
- 6 სხვადასხვა ვებ-გვერდზე გადახდის სისტემების უსაფრთხოდ ინტეგრირების სირთულე;
- 7 მომხმარებლის ქცევების უჩვეულო ცვლილებების პროაქტიური აღმოჩენა, გაცემული დროებითი წვდომის მიმდინარეობისას;
- 8 კრიპტოგრაფიული უსაფრთხოების სერტიფიკატების მენეჯმენტის სირთულე;
- 9 ნულოვანი ნდობის პოლიტიკის გატარების სირთულე.

**მაშინ, კომპანია სინთაქსი PAM360-ის საშუალებით, არსებული გამოწვევების გადაჭრის გზებს გთავაზობთ.**

## **PAM360 (Privileged Access Management)**

**სრული პრივილეგირებული წვდომების უსაფრთხოების გადაწყვეტილება, რომელიც ეხმარება IT ბუნდებას, განახორციელოს მკაცრი მენეჯმენტი იმ წვდომის გზებზე, რომელიც კრიტიკულ კორპორატიულ აქტივებზე წვდომას მოიაზრებს.**

- 1 შეძლებთ ორგანიზაციის ინფრასტრუქტურაზე გასცეთ დაცული წვდომები (მაგალითად, PAM360-ის დახმარებით, გარეშე პირს მისცეთ დაცული, არაპირდაპირი წვდომა თქვენს მონაცემთა ბაზის სერვერზე);
- 2 შეძლებთ ორგანიზაციის ინფრასტრუქტურაზე დაუცველი წვდომების აღმოჩენას (მაგალითად, შეიძლება აღმოაჩინოთ ადმინ ექსპუნთები აქტივ დირექტორიაში, ლინუქს სერვერზე და ა.შ.);
- 3 შეძლებთ გასცეთ დროებითი წვდომები (მაგალითად, გარეშე კონტრაქტორს მისცეთ უსაფრთხო დისტანციური პრივილეგირებული წვდომა 1 ან მეტი დღით)
- 4 შეძლებთ აკონტროლოთ დროებითი წვდომების გაცემისას, რემოუთ სესიის დროს, მომხმარებლის მიერ განხორციელებული ქმედებები;
- 5 თქვენ გექნებათ ყველა გაცემული წვდომების სესიების ჩანაწერები;
- 6 შეძლებთ უსაფრთხოდ გააზიაროთ API სექრეტები, რომელიც საშუალებას მისცემს თქვენს პარტნიორებს, უსაფრთხოდ მოახდინონ თავიანთ პლატფორმაზე მიწოდებული სერვისების ინტეგრაცია;
- 7 შეძლებთ სისტემისგან მიიღოთ ინფორმაცია, პრივილეგირებული მომხმარებლის არასტანდარტული ქცევის შესახებ (მაგალითად, მომხმარებელმა შესვლა სცადა თქვენს მონაცემთა ბაზაზე უჩვეულო დროს);
- 8 შეძლებთ ორგანიზებულად მართოთ სხვადასხვა ვენდორისა და თქვენი პირადი კრიპტოგრაფიული უსაფრთხოების სერტიფიკატები;
- 9 შეძლებთ ნულოვანი ნდობის პოლიტიკის გატარებას (მაგალითად, თქვენს თანამშრომელს მისცეთ ლინუქს სერვერზე კონკრეტული ბრძანებების განხორციელების უფლება და ა.შ.).

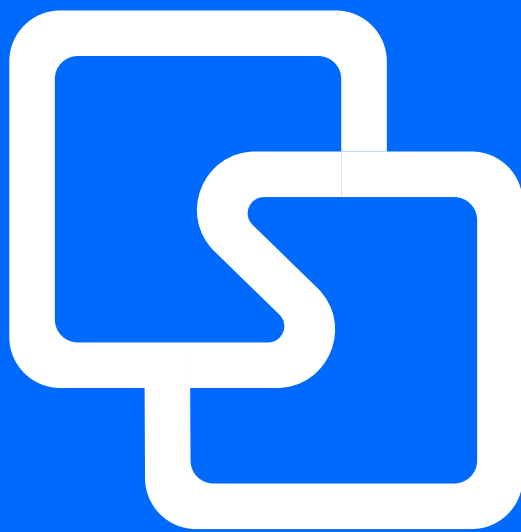
## შეჯამება

ManageEngine PAM360 არის პრივილეგირებული წვდომის უსაფრთხოების გადაწყვეტილება, რომელიც საშუალებას აძლევს ბიზნესს, ამოიციონ და თავიდან აიცილონ ნებისმიერი უმართავი, უკონტროლო და უცნობი პრივილეგირებული წვდომის გზები კრიტიკულ აქტივებზე.

PAM360 უზრუნველყოფს ცენტრალურ კონტროლს პრივილეგირებულ ანგარიშებზე, მიუხედავად იმისა, ეს ექაუნთი ღრუბლობლოვან სისტემაშია, თუ ადგილობრივ სერვერზე.

ამგვარად, PAM360 წარმოადგენს პრივილეგირებული წვდომების უსაფრთხოების გადაწყვეტილებას, რომელიც უზრუნველყოფს IT გუნდებს მხარდაჭერით, რათა მათ განახორციელონ მკაცრი მენეჯმენტი სხვადასხვა სახის წვდომებზე, რომელიც კრიტიკულ კორპორატიულ აქტივებზე წვდომას მოიაზრებს.





**დამატებითი ინფორმაციის მისაღებად  
დაგვიკავშირდით**

**E-mail: [sales@syntax.ge](mailto:sales@syntax.ge)**

**Phone: (032) 2 88 00 99**

**[WWW.SYNTAX.GE](http://WWW.SYNTAX.GE)**