

14 მიზეზი

თუ რაბომ სჭირდებო თქვენს ორგანიზაციას  
**Endpoint Central**



სახელმძღვანელო

2024

Since 2015

## თუ ამ გამოწვევიდან თქვენს ორგანიზაციაში 3 პათგენს მაინც აწყდებით:

- 1 სხვადასხვა ლოკაციაზე არსებული IT ინფრასტრუქტურისა და კორპორაციული მობილური მოწყობილობების შეზღუდული რესურსებით აღრიცხვა და მართვა;
- 2 ერთდროულად წარმოქმნილი განსხვავებული ინციდენტების გადასაწყვეტად, სხვადასხვა ლოკაციაზე ფიზიკურად მისვლის აუცილებლობა;
- 3 ინციდენტის აღმოსაფხვრელად, თანამშრომლის საქმიანობის დროებით შეჩერების აუცილებლობა;
- 4 უსაფრთხოების გამონვევა, რაც გულისხმობს IT ინფრასტრუქტურაში პრივილეგირებული წვდომების კონტროლსა და იდენტიფიცირებას;
- 5 გემბლინგის სექტორის, კომპიუტერებსა და სერვერებში არსებული ძვირადღირებული კომპიუტერული ნაწილების ამოღების, ჩანაცვლებისა და დამატების აღრიცხვის სირთულე;
- 6 უსაფრთხოების გამონვევა, რაც გულისხმობს USB პორტებზე დაერთებული მოწყობილობების კონტროლს;
- 7 პროგრამული უზრუნველყოფის უსაფრთხოების ყველა განახლების (Patch Management- როგორც ოპერაციული სისტემის, ისე მესამე მხარის სოფტების) ავტომატურად მართვა ერთიან სივრცეში;
- 8 უსაფრთხოების გამონვევა, ინფორმაციის გაჟონვის პრევენციის კუთხით;
- 9 ბედმეტი დანახარჯების აღმოჩენის პრობლემა პროგრამული უზრუნველყოფისთვის/ლიცენზიებისთვის გაღებულ ხარჯებში;
- 10 კრიპტოგრაფიული უსაფრთხოების გაფანტული მართვა;
- 11 უსაფრთხოების გამონვევა, რაც გულისხმობს მობილური (პლანშეტები, ლეპტოპები, მობილურები) მოწყობილობების გადაადგილების კონტროლს;
- 12 მობილური მოწყობილობებისგან კომპანიის სენსიტიური ინფორმაციის გაჟონვა;
- 13 IT ინფრასტრუქტურასთან დაკავშირებული ავტომატური რეპორტირების სიმცირე;
- 14 დეპარტამენტების მიხედვით, უსაფრთხოებისა და სხვა პოლიტიკების სწრაფად შექმნა.

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

**Endpoint Central - საბოლოო წერტილების უსაფრთხოების, დისტანციური მართვის, აღრიცხვის, ავთომატიზაციის და საერთო ანგარიშების გენერირების ხელსაწყო.**

- 1 შეძლებთ ცენტრალიზებულად აღრიცხოთ და მართოთ:
  - ენდფონტები (სერვერები, ლეპტოპები, დესკტოპები, სმარტფონები და ტაბლეტები) + ორგანიზაციის კორპორაციული მობილური მოწყობილობები;
  - ყველა პროგრამული უზრუნველყოფა;
- 2 შეძლებთ სხვადასხვა ლოკაციებზე წარმოქმნილი ინციდენტებისა და კრიტიკული შემთხვევების დისტანციურად აღმოფხვრას;
- 3 შეძლებთ აღმოფხვრათ ინციდენტები დისტანციურად თანამშრომლის კომპიუტერში ისე, რომ თანამშრომელმა არ შეწყვიტოს საქმიანობა;
- 4 შეძლებთ მარტივად დააიდენტიფიციროთ და აკონტროლოთ აიტი ინფრასტრუქტურაში პრივილეგირებული წვდომები;
- 5 შეძლებთ კომპიუტერებსა და სერვერებში არსებული მნიშვნელოვანი ნაწილების ამოღების, ჩანაცვლებისა და დამატების ფაქტების აღმოჩენას ალერტებისა და გეგმიური რეპორტების საშუალებით;
- 6 შეძლებთ ცენტრალიზებულად აკონტროლოთ, თუ რა პერიფერიული მოწყობილობები (მაგ: მაუსი, მეხსიერების ბარათი) დაერთდეს ამა თუ იმ კომპიუტერზე;
- 7 შეძლებთ ერთიან სივრცეში ავტომატურად მართოთ პროგრამული უზრუნველყოფის უსაფრთხოებასთან დაკავშირებული ყველა განახლება (Patch Management);
- 8 შეძლებთ ნებისმიერი სენსიტიური ინფორმაცია დაიცვათ კომპანიის მფლობელობაში არსებული ნებისმიერი კომპიუტერიდან გაჟონვისგან (Data Leak Prevention);
- 9 შეძლებთ შეაფასოთ, თუ რამდენი ლიცენზია არის შესყიდული და რამდენი არის ორგანიზაციის მიერ გამოყენებაში, რაც შესაძლებლობას მოგცემთ ოპტიმიზაცია გაუკეთოთ ხარჯებს;

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

- 10 შეძლებთ ერთი კონსოლიდან მართოთ კომპანიის კომპიუტერების კრიპტოგრაფიული უსაფრთხოება, რაც შესაძლებლობას მოგცემთ დაიცვათ სენსიტიური ინფორმაცია გარეშე პირებისგან (Bit Locker);
- 11 შეძლებთ აკონტროლოთ ორგანიზაციის მფლობელობაში არსებული მობილური მოწყობილობების (პლანშეტები, ლეპტოპები, მობილურები), გადაადგილება (MDM-Location Based Actions);
- 12 შეძლებთ აკონტროლოთ ორგანიზაციის მფლობელობაში არსებული მობილური მოწყობილობების (პლანშეტები, ლეპტოპები, მობილურები), ნვდომის უფლებები (MDM-Conditional Access);
- 13 შეძლებთ აიტი ინფრასტრუქტურასთან დაკავშირებული ავტომატიზირებული და მრავალფეროვანი რეპორტების გენერირებას;
- 14 შეძლებთ დეპარტამენტების მიხედვით უსაფრთხოებისა და სხვა პოლიტიკის სწრაფად შექმნასა და გავრცელებას.

## **Endpoint Central - შედეგები:**

- ავტომატური პაჩ მენეჯმენტი;
- პროგრამული უზრუნველყოფის დისტანციური ინსტალაცია;
- იმიჯინგი და OS დეფლოიშმენტი;
- მობილური მოწყობილობების მენეჯმენტი;
- USB მოწყობილობების მენეჯმენტი;
- აპლიკაციების კონტროლი (white list; black list);
- აქტივებისა და ლიცენზიების მართვა;
- დისტანციური მართვა;
- Tool - ები: სისტემის ხელსაწყოები, განცხადება, ჩატი და სისტემის მენეჯერი;
- კონფიგურაციები: 30+ კონფიგურაცია Windows-ის, Mac-ის, Linux - ისთვის და სხვა;
- აუდიტი და რეპორტიინგი.

## შეჯამება

ManageEngine Endpoint Central მოიცავს MDM (Mobile Device Management) გადაწყვეტილებას, რომელიც ერთიანი კონსოლიდან მართავს და იცავს მობილურ მოწყობილობებს, აპლიკაციებსა და მონაცემებს.

ManageEngine Endpoint Central მართავს დაახლოებით 25,000+ ორგანიზაციის 200 მილიონ საბოლოო მოწყობილობას.

ManageEngine MDM გადაწყვეტილება აკონტროლებს მობილური მოწყობილობების აპლიკაციებს, მონაცემებს და უსაფრთხოებას, ისე რომ თანამშრომლებმა შეძლონ მოწყობილობებზე უპრობლემოდ მუშაობა.

MDM საშუალებას გაძლევთ ერთი კონსოლიდან მონიტორინგი გაუწიოთ, მართოთ და დაიცვათ თქვენს ორგანიზაციაში არსებული კორპორაციული და არა კორპორაციული მობილური მოწყობილობები, ამასთან, დააგენერიროთ ავტომატური რეპორტები სასურველი სიხშირით.

85%+ მომხმარებელი ყოველწლიურად ანახლებს ლიცენზიას, რაც თავისთავად ასახავს სინტაქსის კმაყოფილი მომხმარებლის რაოდენობას, რომელიც ენდობა ManageEngine-სა და Endpoint Central-ის შესაძლებლობებს. შესაბამისად, Endpoint Central-ი წარმოადგენს უსაფრთხოების სანდო სისტემას.



**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)**