ISO/IEC 27001:2005

THE CHERRY GROUP

CIS

IP-guard

განიხილეთ კომპანიის მონაცემთა დაცვისა და მონიტორინგის ახალი ტექნოლოგია

ინფორმაციული უსაფრთხოება

ინსაიდერები - უდიდესი საფრთხე თქვენი ორგანიზაციისათვის

ინსაიდერების მიერ მიყენებული ზიანი მრავალი სახისაა. მან შესაძლოა ხანგრძლივი პერიოდით დააზარალოს თქვენი კომპანია.

კონტროლის უმაღლესი ხარისხი IP-guard-ის საშუალებით

IP-guard წარმოადგენს უნივერსალურ პროდუქტს, რომელიც უზრუნველყოფს ორგანიზაციის შიდა ინფორმაციული უსაფრთ-ხოების მართვას. IP-guard დაიცავს თქვენს კონფიდენციალურ მონაცემებსა და ინტელექტუალურ საკუთრებას. იგი თავიდან აგაცილებთ კომპანიიდან ინფორმაციის "გაჟონვას".

IP-guard ეფექტურად მართავს ინსაიდერულ საფრთხეებს

IP-guard ეხმარება ხელმძღვანელობას უკანონო ქმედების აღმოჩენასა და ბლოკირებაში. იგი აკონტროლებს შიდა ქსელურ კომუნიკაციას ისეთი მოქმედებების აღსაკვეთად, როგორიცაა მნიშვნელოვანი ინფორმაციის გაცვლა, ქსელური თამაშები, ჩათი, ტორენტ ჩამოტვირთვები და ა.შ. უსაფრთხოების პოლიტიკის დარღვევის შემთხვევაში ხელმძღვანელობა/ადმინისტრატორები დაუყოვნებლივ იღებენ შეტყობინებას.

IP-guard დეტალურად აღრიცხავს და აკონტროლებს:

- თანამშრომლების მიერ პროგრამული აპლიკაციებით განხორციელებულ ნებისმიერ მანიპულაციას
- ვებ ბრაუზერებში მუშაობის ისტორიას, ჩამოტვირთვებს
- მყისიერი შეტყობინების გაგზავნის აგენტებს (მესინჯერებს)
- ინფორმაციის ბეჭდვას, გაცვლას ან შენახვას სპეციალურ გარე მოწყობილობებზე (CD, USB, პორტი, მოდემი და სხვა).

IP-guard ადაპტირდება ნებისმიერ ქსელურ სტრუქტურასთან; აქვს დისტანციური კონტროლის შესაძლებლობა.

IP-guard-ის დიზაინი შეესაბამება საერთაშორისო სტანდარტებს (ISO/IEC 27001: 2005). იგი წარმატებით დაინერგა მსოფლიოს წამყვან წარმატებულ ორგანიზაციებში.

IP-guard-ის მოდულები

IP-guard-ში ინტეგრირებულია სხვადასხვა მოდული. მათი საშუალებით შესაძლებელია ინფორმაციული უსაფრთხოების მონიტორინგი და მიუღებელი ქმედებების გამოვლენა რეალურ დროში. მიღებული ინფორმაცია კონსოლიდირებული რეპორტინგის საშუალებით მიეწოდება ხელმძღვანელობას. თქვენ შეგიძლიათ შეარჩიოთ მხოლოდ თქვენი ორგანიზაციი-სათვის აუცილებელი მოდულები.

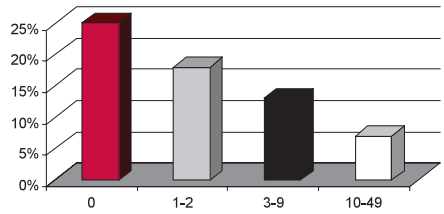
ფაქტები არ ტყუიან

„სერიოზული დარღვევათა 70% ინსაიდერების ინიციატივის შედეგია"

IDC Worldwide Security Products and services, 2008

თქვენს კომპანიაში უკანასკნელი 12 თვის განმავლობაში უსაფრთხოების დარღვევის რამდენი შემთხვევა მოხდა?

(CIO Magazine/PwC Survey)

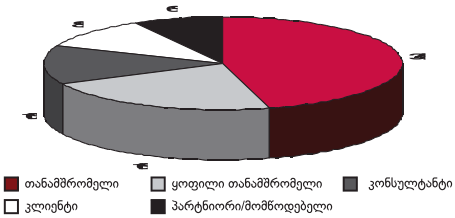


„გამოკითხულ თანამშრომელთა 85%-მა განაცხადა, რომ სამსახურიდან დათხოვნის შემთხვევაში თან წაიღებდნენ კომპანიის კონფიდენციალურ ინფორმაციას"

Cyber-Ark, 2009

თქვენი აზრით, ვინ წარმოადგენს უსაფრთხოების დარღვევის წყაროს?

(CIO Magazine/PwC survey)



„რესპონდენტთა 97%-ს მიაჩნია, რომ ინფორმაციის გაჟონვის ყველაზე სავარაუდო მიზეზია ინსაიდერის ან პარტნიორის გაუფრთხილებელი ქმედება, ან ინსაიდერის წინასწარ განზრახული მოქმედება"

Ponemon Institute, 2009

IP Guard-ის მოდული	აღწერილობა
მართვის საბაზო მოდული	- მართვის საბაზისო საშუალებები - ძებნის ძლიერი მექანიზმი - იმპორტ/ექსპორტის ფუნქციონალობა
პროგრამული აპლიკაციების მართვა	- არაავტორიზებული აპლიკაციების გამოყენების აღკვეთა - აპლიკაციების დეტალური ლოგ-ფაილები - პროგრამულ სისტემებში უსაფრთხოების დარღვევის დაფიქსირება და მყისიერი შეტყობინება
დოკუმენტების მართვა	- ყველა ოპერაციის დეტალური ლოგირება - ცვლილებაშეტანილი ფაილების ავტომატურად შენახვა
შეტყობინებათა მყისიერი გაცვლის მართვა	- ყველა ცნობილი ინტერნეტ-პეიჯერის (Skype, ICQ, MSN) მონიტორინგი - საუბრის ჩანაწერის და გადაგზავნილი ფაილების შენახვა
ელ.ფოსტის მართვა	- ყველა სახის ელ.ფოსტის (POP/SMTP mail / Outlook / Notes / webmail) მონიტორინგი, ლოგირება და ძებნის ძლიერი მექანიზმი
ბეჭდვის მართვა	- პრინტერის გამოყენების კონტროლი - ამობეჭდილი ფაილების შენახვა
ეკრანის მართვა	- მრავალრიცხოვანი ეკრანების პარალელური მონიტორინგი - ეკრანის ისტორიის ჩაწერა ვიდეო ფაილის სახით
ინტერნეტში წვდომის მართვა	- ვებ რესურსებზე წვდომის კონტროლი - ინტერნეტში წარმოებული ყველა მოქმედების ლოგირება
ინფორმაციის შესანახი მოწყობილობების მართვა	- გარე შესანახი მოწყობილობების ავტორიზაცია/შიფრაცია - ავტორიზებული წვდომა დაშიფრულ მონაცემებზე
აპარატურის მართვა	- სრული ინვენტარიზაცია - პროგრამულ-აპარატურული უზრუნველყოფის მართვა - Windows-ის ავტომატურად განახლება
გამტარუნარიანობის (Bandwidth) მართვა	- ქსელში ნებისმიერი არასათანადო ქმედების გამოვლენა - ტრაფიკის კონტროლი - ჩამოტვირთვების სიჩქარის ლიმიტირება
აპარატურის მართვა	- აპარატურასთან წვდომის კონტროლი რეალურ დროში
ქსელის მართვა	- ქსელზე არასანქცირებული მიერთების კონტროლი - ქსელის რესურსებზე (კომპიუტერები, პორტები) არაავტორიზებული/ უკანონო წვდომის ბლოკირება
დისტანციური მართვა	- ფილიალებში მიმდინარე პროცესების კონტროლი - ძლიერი რეპორტინგი

IP-guard - ყველაზე მოქნილი და რენტაბელური გადაწყვეტილება ინსაიდერული რისკების მართვისათვის

www.cherrygroupcis.com

The Cherry Group CIS Ltd

E-mail: info@cherrygroupcis.com

www.cherrygroupcis.com

ექსკლუზიური დისტრიბუტორი:

BIT
BUSINESS INTELLIGENCE TECHNOLOGIES

ჩიქოვანის 16
თბილისი, საქართველო
ტელ.: 18 53 53
ელ-ფოსტა: bit@bit.ge
www.bit.ge