

رایان سامانه آرکا

راهکارهای جامع امنیت و شبکه



مقایسه نرم افزارهای Safetica و Zecurion

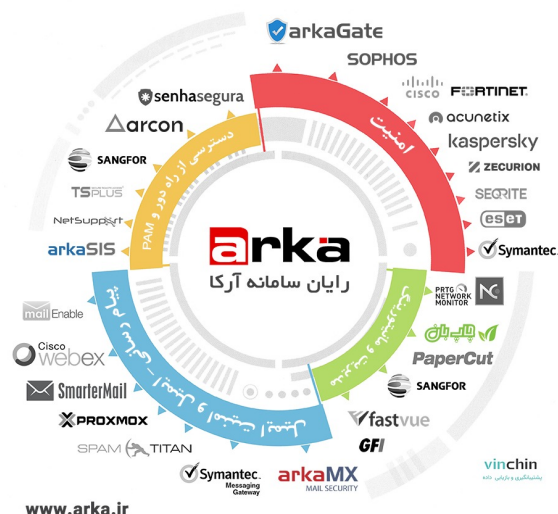
دکتر امیر حسنی کرباسی

مدیر واحد امنیت اطلاعات رایان سامانه آرکا

مدرس دانشگاه و متخصص رمزنگاری و امنیت فضای سایبری

Data Loss Prevention (DLP)

محصولات و راهکارهای رایان سامانه آرکا



مقدمه

در مباحث آتی، دو محصول Safetica و Zecurion در جداولی براساس پارامترهای زیر مقایسه شده‌اند که ما مهمترین ویژگی‌های موجود در این جداول را که Zecurion پشتیبانی می‌کند ولی Safetica پشتیبانی نمی‌کند را شرح می‌دهیم و سایر ویژگی‌ها را می‌توان از جداول مشاهده کرد. (مشاهده شد که Zecurion توانمندتر از Safetica است). پارامترها:

- ۱- روش‌های تشخیص نشت داده‌ها
- ۲- مدهای عملیاتی
- ۳- کنترل ایمیل
- ۴- کنترل اینترنت و وب
- ۵- کنترل نقاط انتهایی و کلاینت‌ها
- ۶- تجهیزاتی که پشتیبانی می‌شوند
- ۷- تحلیل اطلاعات حساس و محرمانه
- ۸- امکانات مدیریتی

- ۹- گزارش‌گیری

- ۱۰- سیستم‌های پشتیبانی کننده

چند ویژگی بارز Zecurion

۱- Digital Fingerprints

- تشخیص و ردگیری پردازش‌های محاسباتی و عملیاتی برای هر کاربر و دستگاه موجود در شبکه، اجرا می‌شود.

۲- Support Vector Machine

- یکی از روش‌های یادگیری ماشینی است که از آن برای طبقه‌بندی و رگرسیون استفاده می‌کنند.

۳- Bayes method

- تحلیل آماری با توزیع بیضی است.

۴- Control of documents containing seals or signatures

- کنترل و تحلیل اسنادی که دارای مهر و امضا هستند.

۵- Gateway interception with ICAP : integration with a proxy server

- نظارت دروازه‌های شبکه و نقاط مرزی بصورت یک واسط میانی.

۶- Mirrored mail and Mirrored traffic

- تحلیل و کنترل ترافیک و ایمیل‌های آینه‌ای با منشا متفاوت.

۷- Message modification

- کنترل دستکاری متون و نامه‌های الکترونیکی.

۸- Desktop and Mobile applications

- کنترل و تحلیل برنامه‌های کاربردی دسکتاپی و موبایلی.

۹- FTPS

	ZECURION	safetica
Detection by internal content of the document	✓	✓
Predefined templates	✓	✓
Regular expressions	✓	✓
Digital fingerprints	✓	×
Support Vector Machine	✓	×
Content analysis of attachments	✓	✓
Bayes method	✓	×
Control of documents containing seals or signatures	✓	×
Text recognition (OCR)	✓	×
Quarantine	✓	×
Hybrid content analysis	✓	✓

مدهای عملیاتی

	ZECURION	safetica
Gateway interception with ICAP integration with a proxy server	✓	×
Plugin integration for MS Exchange	✓	×
Gateway mode	✓	×
Agent interception mode	✓	✓
Mixed mode (gateway and agent)	✓	×
Receiving mirrored mail from specific mailbox	✓	×
Analysis of mirrored traffic	✓	×

کنترل ایمیل

	ZECURION	safetica
Inbound SMTP	✓	✓
Outbound SMTP	✓	✓
ESMTP support	✓	✓
Internal Microsoft Exchange mail	✓	✓
Collect mail using POP3	✓	✓
Collect mail using IMAP4	✓	✓
Message modification	✓	×

- پشتیبانی از پروتکل‌های رمزنگاری در ارسال فایل

۱۰- USB shadow copying

- کنترل بک آپ گیری پنهان در ابر یا سایر تجهیزات ذخیره‌سازی.

۱۱- Encrypting files when writing to USB or other contents

- اسنادی که در سازمان ایجاد و نگهداری می‌شوند، فقط در سیستم های سازمان قابلیت خوانایی دارند و در خارج از سازمان بصورت رمزشده هستند که کلیدهای رمزگذاری در فواصل معین، آپدیت می‌شوند.

۱۲- screenshots

- کنترل قدرتمند روی اسکرین‌شات‌ها.

۱۳- Network storage scanning and Real-time storage scanning

- پایش بلادرنگ تجهیزات ذخیره‌سازی شبکه.

۱۴- User connections and emotional diagrams

- نمودارهای تعاملی و گرافیکی از رفتار و ارتباطات کارکنان.

۱۵- Export reports

- گزارش گیری و تهیه گزارش در فرمت های مختلف.

مقایسه امکانات و ویژگی‌های Safetica و Zecurion

در جداول

روش‌های تشخیص نشت داده‌ها

کنترل اینترنت و وب

	ZECURION	safetica
Keylogger	✓	✓
Clipboard control	✓	✓
Uninstall password for endpoint	✓	✗
Files Removal action in Discovery module	✓	✗
MS Office documents properties attributes verification	✓	✗
TITUS tags verification in MS Office documents properties attributes	✓	✗

	ZECURION	safetica
HTTP inbound traffic	✓	✓
Outgoing HTTP traffic	✓	✓
MS Lync	chat, attachments, clipboards text, and voice	✗
ICQ	✓	✗
Viber	✓	✗
Webmail	✓	✓
WhatsApp desktop application	✓	✗
Telegram desktop application	✓	✗
Social networks	✓	✓
FTP	✓	✓
FTP5	✓	✗

تجهیزاتی که پشتیبانی می‌شوند

	ZECURION	safetica
Pre-configured lists of typical classes and types of connected devices	✓	✓
USB	✓	✓
LPT / COM	✓	✓
CD / DVD	✓	✓
External and internal HDD	✓	✓
Ethernet	✓	✓
Clipboard	✓	✓
RDP forwarded devices	✓	✓
Bluetooth / Wi-Fi	✓	✓
Virtual devices	✓	✓

	ZECURION	safetica
HTTPS traffic	✓	✓
Yahoo! Messenger	✓	✓
Google Hangout	✓	✗
Skype	chat, attachments, clipboards text and voice	✗
Jabber	✓	✓
WhatsApp	✓	✓
Telegram	✓	✓

تحلیل اطلاعات حساس و محرمانه

	ZECURION	safetica
Network storage scanning	✓	✗
Scan local storage	✓	✓
Scan databases	✓	✓
Scan MS SharePoint	✓	✓
Scan MS Exchange	✓	✓
Real-time storage scanning	✓	✗
Scheduled Scan	✓	✓
Security administrator notification of storage policy violations	✓	✓
Alert users about violation of information security policies	✓	✓
Moving / deleting files	✓	✗

کنترل نقاط انتهایی و کلاینت‌ها

	ZECURION	safetica
Agent stand-alone mode without access to the server	✓	✓
Blocking leakage via USB and other devices	✓	✓
Block leakage through printing using content analysis	✓	✓
USB read only mode	✓	✓
USB shadow copying	✓	✗
Shadow copy file size limit	✓	✓
Manage settings and volume of the local storage of logs and shadow copies on Endpoints	✓	✓
Application startup control	✓	✗
Encrypting files when writing to USB	✓	✗
Content analysis based encryption	✓	✗
Access control for encryption keys by user / group of users	✓	✗

امکانات مدیریتی

	ZECURION	safetica
Management through own console	✓	✓
Single management console	✓	✓
Single incidents console	✓	✓
Setting alerts	✓	✓
Web console management	✓	✓
Deploy and upgrade through domain policies	✓	✓
Deploy and upgrade through own server / console	✓	✓
Separation of administrator roles	✓	✓

	ZECURION	safetica
Re-generation of encryption keys	✓	✗
Save encryption key history	✓	✗
Making screenshots	✓	✓
OCR for screenshots	✓	✗
Set screenshots for list of users	✓	✓
Set screenshots with periodicity	✓	✓
Saving screenshots in different file formats	✓	✓
Saving grayscale screenshots	✓	✗
Hiding agent presence	✓	✓
Protection against agent disable	✓	✓
Record sound through the built-in microphone or connected headset	✓	✗

گزارش‌گیری

نارضایتی‌های موجود از Safetica در Gartner



Vinny K

Cyber Security Architect
Mid-Market (51-1000 emp.)

Validated Reviewer ✓

Review source: Organic

What do you dislike?

The Web categorization is not good. We should work on that.

نارضایتی‌های موجود از Safetica در Gartner



Karel P

Head of IT & Member of Management Board
Mid-Market (51-1000 emp.)

Validated Reviewer ✓

Review source: Organic

What do you dislike?

The product has too wideness menu and therefore acts as complex.

نارضایتی‌های موجود از Safetica در Gartner



Mücahid A

Senior Technical Consultant
Small-Business (50 or fewer emp.)

Validated Reviewer ✓

Verified Current User ✓

Review source: Organic

What do you dislike?

Safetica error codes are not very pleasant.

نارضایتی‌های موجود از Safetica در Gartner



Pavel J

External IT Consultant
Mid-Market (51-1000 emp.)

Validated Reviewer ✓

Review source: Organic

What do you dislike?

DLP sometimes referred to incorrect documents.

ZECURION safetica

Graphic Reports	✓	✓
Tabular reports	✓	✓
List of messages in a table with the ability to view their contents	✓	✓
User connections diagrams	✓	✗
User emotional status diagram	✓	✗
User Behavior Analytics based on composite everyday indicator (incidents, files, traffic volume etc.)	✓	✓
User profile card	✓	✓
Export reports and rows to PDF, XLSX, CSV, PST file formats	✓	✗
Export reports and rows to expropriated HTML file	✓	✗

سیستم‌های پشتیبانی کننده

ZECURION safetica

Administrators logging	✓	✓
OS requirements by server components	Windows Server 2008 R2 and later	Windows Server 2008 R2 or later, Quad-core processor 2.4 Ghz+, 2Gb RAM, 3Gb disk space
OS support by endpoints	Windows 7, Windows Server 2008 R2 and later; Linux	Windows 7 32/64-bit or later, Dual-core processor 2.4 Ghz+, 2Gb of disk space
Supported databases	Microsoft SQL, PostgreSQL	Microsoft SQL
AD integration	✓	✓

مقایسه‌ی دو محصول از دید موسسات بین‌المللی ارزیابی و مشاوره‌ای Gartner و CyberPal

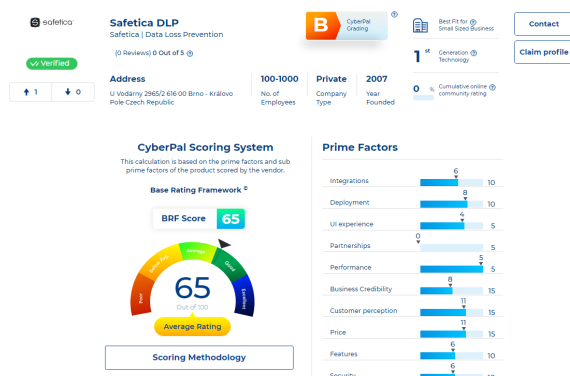
ارزیابی توسط Gartner و CyberPal

• در مقایسه با Safetica می‌خواهیم به گزارشات Gartner و CyberPal اشاره کنیم که از بهترین و بزرگترین موسسات بین‌المللی مشاوره‌ای و ارزیابی تجهیزات و راهکارهای محصولات ICT هستند.

• در گزارشات Gartner به ۴ مورد از نارضایتی‌های خریداران Safetica برخورد کردیم که آنها را همین‌جا بیان می‌کنیم و برای جزئیات بیشتر می‌توان به لینک زیر رجوع کرد: (البته موارد رضایت‌مندی را نیز بیان کرده‌اند).

• <https://www.g2.com/products/safetica/reviews#details>

• ولی در خصوص Zecurion به موارد نارضایتی برخورد نکردیم.



رتبه بندی CyberPal

• در ارزیابی های CyberPal، رضایت مندی بیشتری نسبت به Zecurion را مشاهده کردیم و گفته شده است که Zecurion امکانات بیشتری را فراهم می کند و Zecurion امتیاز بیشتری را در بین خریداران از آن خود کرده است.

• این آمار را هم اکنون بیان می کنیم ولی جهت اطلاعات بیشتر می توان به لینک های زیر رجوع کرد:

- <https://cyberpal.io/solutions/zecurion-dlp>
- <https://cyberpal.io/solutions/safetica-dlp?undefined>

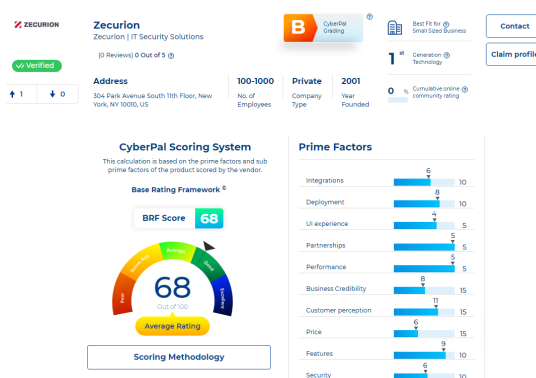
رایان سامانه آرکا- نماینده رسمی Zecurion و Safetica در ایران

تهران، خیابان شهید بهشتی، خیابان پاکستان، کوچه چهارم، پلاک ۱۱، طبقه چهارم، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی: ۱۵۳۱۶۴۵۹۱۸
www.arka.ir | info@arka.ir

arka
رایان سامانه آرکا

کلیه حقوق مادی و معنوی محفوظ و متعلق به شرکت رایان سامانه آرکا می باشد.

Zecurion در CyberPal با امتیاز ۶۸



Safetica در CyberPal با امتیاز ۶۵