

Next Generation Product Authentication



Counterfeit products are now a global problem affecting brands across a range of industries. They have become a major threat to innovation, revenue and consumers. Over the last 30 years, various product authentication technologies have been developed but contained flaws in security, ease of use, or were simply not cost efficient. This whitepaper examines how next generation product authentication technology, with the inclusion of a patented security tag, creates a solution that is more secure, easier to use and integrates with other technologies.

Author: Thomas Bergmueller, thomas.bergmueller@authenticvision.com	
Authentic Vision GmbH Josef-Mayburger-Kai 114 5020 Salzburg Austria	Authentic Vision, Inc. 1005 Market St San Francisco, CA 94103 USA



CONTENTS

01

Counterfeiting A Global Issue

Counterfeit issues are growing at a rapid pace. Product piracy affects all countries and brands.

02

Motives and Consequences

Counterfeiting is attracting organized crime because of lower perceived risk when compared to other criminal activities. Outsourcing, complex supply chains as well a multitude of different distribution models makes it nearly impossible to monitor and police effectively.

03

Disadvantages of Existing Solutions

A product authentication solution's primary duty is to enable individuals in the supply chain to easily and securely authenticate products. In this respect, the current solutions fail.

04

The Industry Reality

Typically, product authentication solutions combine a QR code or other 2D representation such as a serial number, and one or more advanced security features such as a hologram or other covert technologies. These solutions detach the scan process from the real authentication.

05

Authentic Vision Security Tag

Authentic Vision's patented security tag empowers everyone in the distribution chain – manufacturers, distributors, partners, customs officials and consumers - ensuring authenticity of products without dedicated hardware or technical expertise.

06

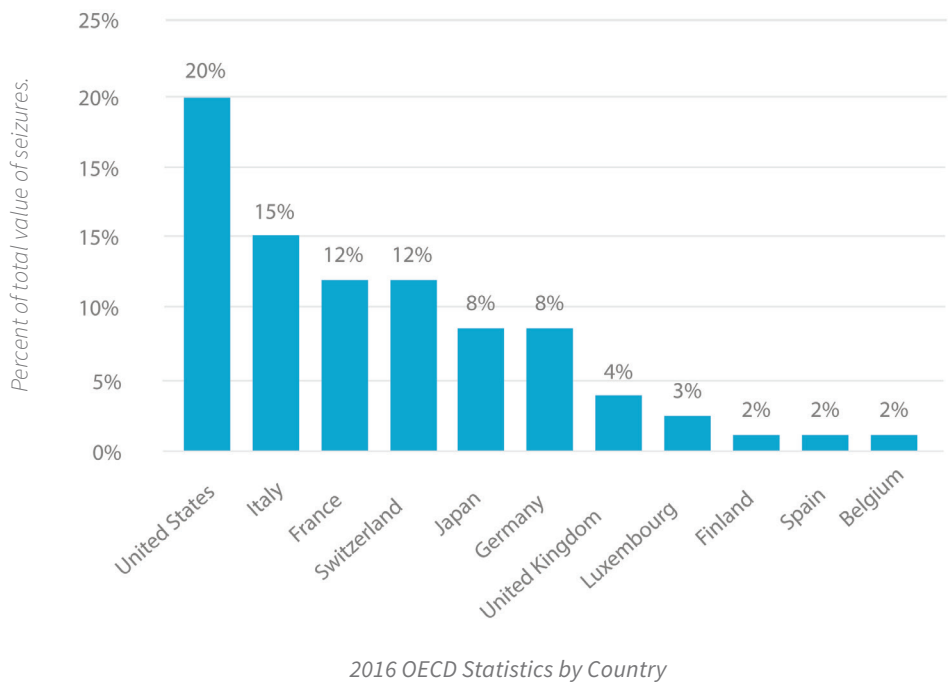
About Authentic Vision

Authentic Vision is the provider of patented security tag solutions backed by a software platform designed for regulators, brand managers, and operations professionals.

Counterfeiting

The Global Issue

Countries Hit Hardest by Trade of Faked Goods



Counterfeit issues are growing at a rapid pace. In 2016, the OECD published a report [1] in cooperation with the EU Intellectual Property Office (EUIPO), indicating counterfeit products sold in 2013 were worth \$431bn, totaling 2.5% of global trade in 2013. An estimated 5% of all goods imported into the European Union are fake. Product piracy affects all countries and brands. Countries with strong economies, brands and licensors are hit hardest: The EU-4 (Germany, France, Italy and the UK) totaling to 38% and the US with 20% [2].

Another detailed report published by EUIPO in 2017 [3], says counterfeit products originate from all countries in the world. China is responsible for 72% of all counterfeit products in the EU, USA and Japan. China’s questionable leading role is followed by Hong Kong and Turkey.

Motivations and Consequences

High Profitability

Europol’s OCTA report [4] finds that counterfeiting is attracting organized crime due to lower perceived risk when compared to other criminal activities. The profitability of counterfeit products, in some cases, exceeds the profitability of trafficking drugs. The International Anti-Counterfeiting Coalition (IACC) has discovered links between counterfeit profits and other organized crimes such as drug trafficking, money laundering and financing of terrorism. [5]

Easy Targets

Securing the distribution channel seems like an impossible challenge. Outsourcing, complex supply chains coupled with the range of different distribution models make it nearly impossible to monitor effectively. The counterfeiter’s goal is to sell fake product to customers and generate profit. Counterfeiters have learned to abuse the complex distribution channels by introducing fake products at every possible stage of the supply chain, from basic ingredients to final packaging. Products with higher profit margins are the preferred targets.

Brand and Distribution Channel Impact

Counterfeits affect a brand’s revenue and value. Product piracy will result in unwarranted liability costs, loss in consumer loyalty and damaged reputation. Loss in revenue and brand value restrict a brand’s ability to invest in product research, innovation and development. Additionally, pirated products erode the margins at all levels and impact legitimate distributors, resellers and partners throughout the distribution chain.

Consumer Consequence

Customers (B2B as well as B2C) are the target market for every pirated product. The potential impact and risks are many – from potential health risks due to counterfeit baby formula, pharmaceuticals and supplements to reduced service life or severe damage to industrial machines and vehicles due to forged mechanical parts. Exploding batteries in consumer electronics or malfunctioning devices because of non-compliant, incompatible cables or other components frequently create major problems for legitimate manufacturers globally.

Tax Loss, Government Involvement

OECD considered the impact of counterfeit products on tax collection [6]. While there are no reliable numbers, it is presumed that pirated products create losses in sales taxes, corporate taxes, social insurance charges, import tariffs and excise taxes, affecting all product categories, industries and countries.

Disadvantages of Existing Solutions

A product authentication solution’s primary duty is to enable individuals in the supply chain to easily and securely authenticate products. In this respect, existing technologies fail.

To get comprehensive end-to-end protection by restoring distribution channel integrity, a solution needs to empower all stakeholders to verify a product’s authenticity.



Existing product authentication solutions fail to effectively verify products throughout the distribution chain because they are:



Easy to use but not secure.

These include overt technologies such as QR codes, serial numbers or other 2D codes.



Secure but require expertise and dedicated hardware.

Covert technologies such as micro-structures, fluorescent ink, holograms or other hidden security features.



Not cost-efficient or difficult to integrate.

RFID and proprietary tags for example.

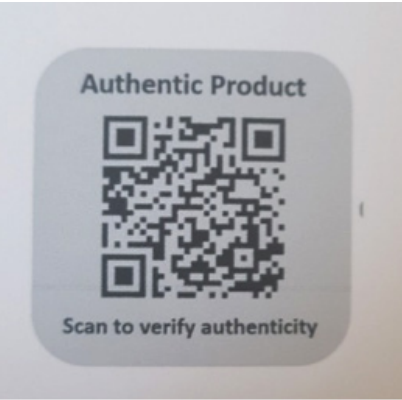
Overt Authentication

Overt serialization and authentication features are printed 2D codes such as serial numbers, QR Codes, Data Matrix Codes or other human or machine-readable representations. The main advantage of such 2D codes is their ease of use and ubiquity. A study showed 81% of consumers are familiar with QR codes, and 50% have scanned a QR code. Easily scanned by smartphones or barcode readers, 2D codes are utilized in a broad range of B2B and B2C applications.

2D codes have one major disadvantage; they are easily copied. A plain copy of a QR code replicates the full functionality of the code. Below, the QR code on the left is the original, the QR code on the right is a copy. QR code readers and apps have no way to differentiate the original from the copy. QR codes are completely unqualified for determining a product’s authenticity.



Original Tag



Photocopy provides same functionality.

Holograms

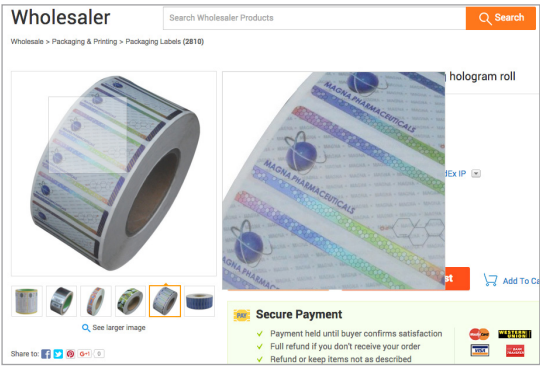
Beginning in the 1980s, holograms were integrated in many security-relevant products such as credit cards and banknotes. Holograms have complex, hard details, structures and reflection characteristics, which are hard to copy.

Despite progress in hologram technology, its function is mostly cosmetic and hardly ever used for verification. Reading instructions or watching a video gives an indication of how holograms should appear, but copycats are often sufficient to trick non-experts.



User Instructions to Authenticate Euro Banknotes

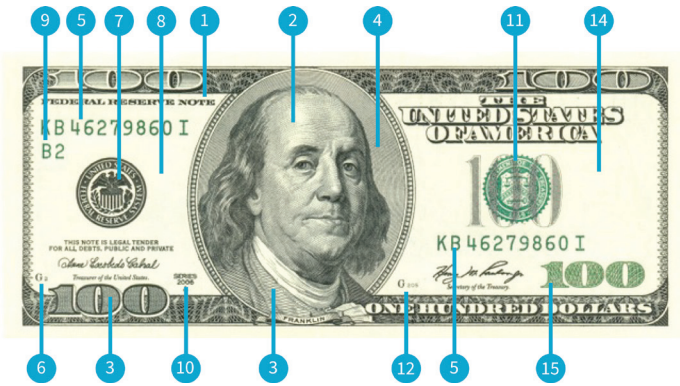
In the early days of holograms, only specialized manufacturers could produce them which guaranteed greater security and exclusivity. Today, it is possible to order branded and customized holograms of any shape, design and color, making it virtually impossible to detect a fake. To non-experts, holograms convey an unverifiable quality.



Custom Security Holograms on Alibaba

Covert Authentication
- For Experts Only

Covert security features come in many varieties. For example taggants, special security ink or pigments, reflect light in a certain wave-length. Other commonly used members of the covert feature category are micro-marks and precise structures like guilloches. While covert solutions are highly secure, their range of application is limited by the fact that, in order to be employed, these solutions require expertise, training or dedicated, expensive hardware to perform authentication. This fact reduces the user-base to experts who can perform forensic analysis and low volume checks based on test purchases, during a seizure or when requested by customs. Retailers, distributors, and customs are not able or willing to utilize covert features due to their limited accessibility and usability.



A good example of covert security can be seen in bank notes. Non-experts have a limited knowledge about the implemented security features and are unable to 100% verify a bank notes' authenticity. Often, copies look good enough to pass visual checks by amateurs.

RFID

RFID tags were developed to easily track and identify objects with contact-less RFID reader devices. Mainly used as a logistic solution, RFID was also tested for its authentication capabilities. RFID tags in the price range of USD 0.25-0.5 are not copy-proof, hence incapable of authenticating products. More sophisticated RFID tags are hardened against cloning, providing additional security but come at even higher cost. Programmable RFID tags are available online and it is simple for anyone to program a “yes, authentic” message on every tag. Proprietary RFID scan apps add another layer of security, verifying a RFID tag’s content. But, in addition to high costs, the lack of support on all mobile phones and across RFID varieties adds another barrier of adoption to RFID based authentication solutions.

The Industry Reality

Overt Codes and Secondary Verification

Evolution but No Revolution


Over the last 30 years, the industry developed a range of product authentication technologies. Typically, the solution entails a combination of a QR code or 2D representation like a serial number, and one or more advanced security feature like a hologram or covert technology. QR codes and serial numbers can be scanned or used by anyone but are easy to fake. Hence, they do not provide any proof of authenticity.

To overcome this challenge, additional, covert feature(s) or holograms enable a so called “secondary verification” which again requires training, dedicated hardware, or special expertise.

Combination of Overt Code and Secondary Authentication

Secondary authentication features are mostly created exclusively for trained brand protection experts, excluding other supply chain stakeholders like distributors, customs, retailers and customers. The 2D code (serial or QR) is completely independent from the secondary verification feature, giving a false sense of security. The serial number or QR code can be easily faked and display a “yes, authentic” result to non-experts. Real authentication remains inaccessible for non-experts.

Combined Solutions Are Failing



Covert Feature, Hologram

- Secondary Authentication for Experts
- Requires dedicated training and/or hardware

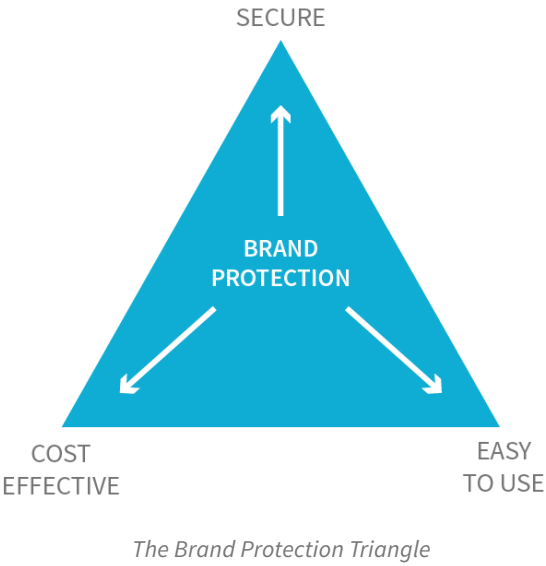
QR Code or Serial Number

- Intended for consumer connectivity
- Can be easily replicated
- Not intended for product authentication

	DISTRIBUTOR IMPORTER	BRAND PROTECTION SPECIALIST	CUSTOMS	RETAIL PARTNER	CUSTOMER
OVERT FEATURES <ul style="list-style-type: none">• 2D Codes, QR Codes, Serial No.• Interactivity, logistic• Not copy-proof, no authenticity					
COVERT FEATURES, HOLOGRAMS <ul style="list-style-type: none">• Allow secondary verification• Require expertise or hardware• Copy-proof					

Today, brands compromise

Brands considering product authentication technologies must compromise between solutions that focus on either ease of use, security or cost-effectiveness.



Authentic Vision

Security Tag Solution

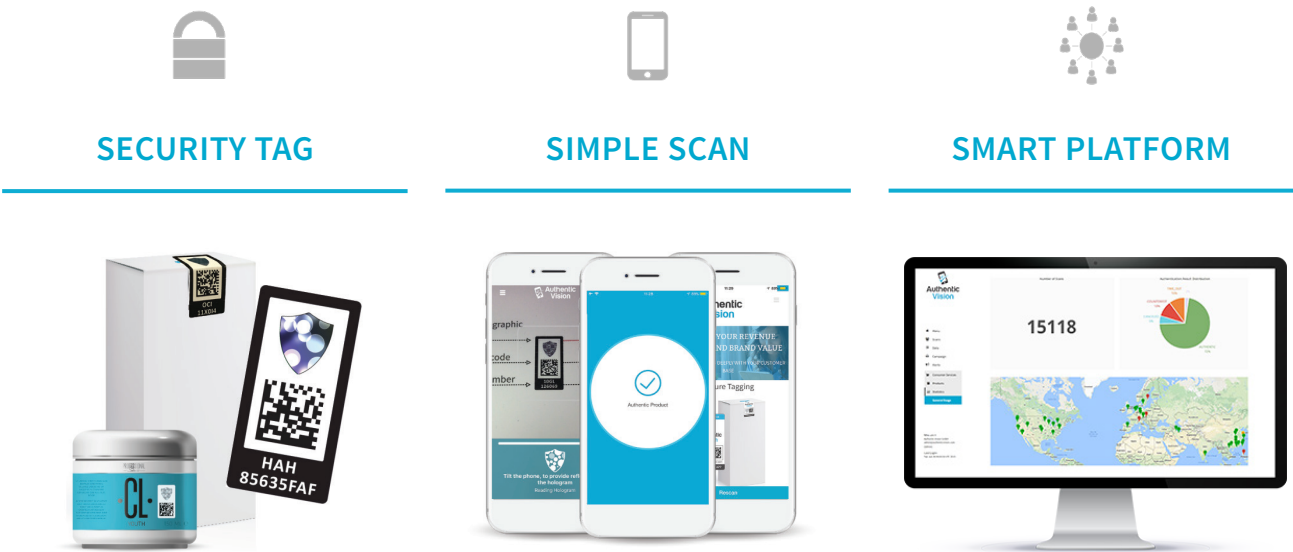
With the weaknesses of the current approaches and the ever increasing global counterfeit problem there is a real need for companies to carefully examine their product authentication options and select a solution that is fully secure, easy to use and cost effective. To identify a solution that meets these criteria, here are six questions a company should ask during its specification and selection process:

How easy is the solution to integrate into the company's product design, operations, distribution, and risk management systems?

To answer this question, the company must first consider the security tag that gets embedded in the product packaging. Executives will need to assess whether the tag can be reproduced by counterfeiters. They also must review how easy the tag is to produce and whether the company will create each one internally or outsource production.

Next, the company must determine how easy the tag will be to use in the field, including whether special equipment or training would be needed for using the tag system to authenticate each unit of product.

Last, the administrative tracking system must provide a robust set of real time information about the status of the company's products in the field. At the same time, this online reporting system must be intuitive for users.



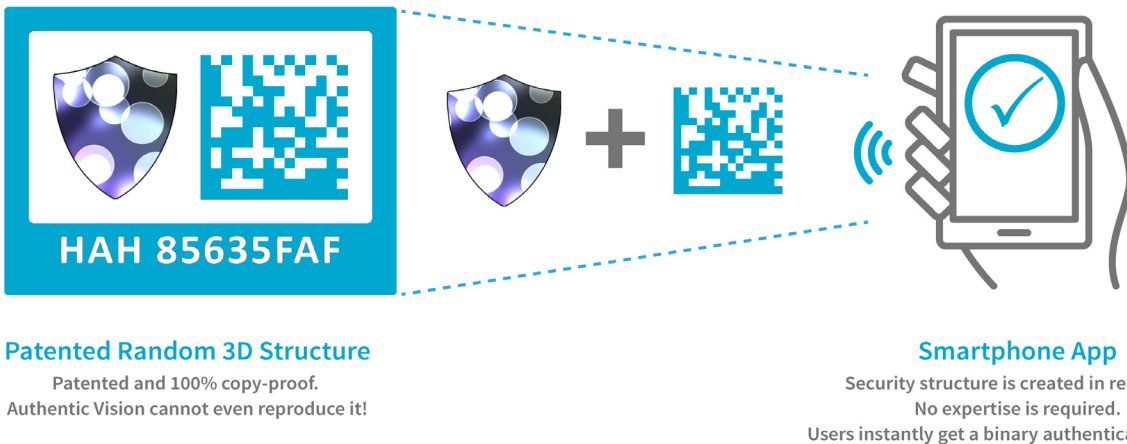
What is the technology behind the Security Tag?

Technology to create a unique security tag exists today, containing random structures that are so secure that they could not be reproduced.



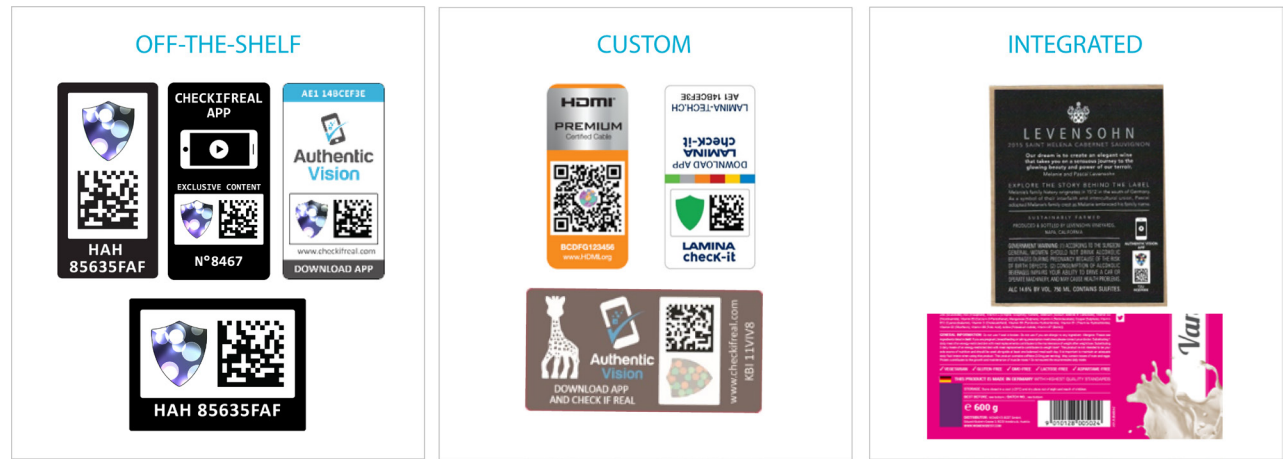
Can the tag be easily scanned?

For maximum effectiveness, the system should not require proprietary equipment or user training. An easy-to-use authentication system would involve an app that could be deployed via any common smart phone. A user's phone would then be set up to read the serial number and authenticate the tag in real time, making the other secondary verification solutions obsolete. Technology should make sure there is not a reliance on visual, human verification. Additionally, developer resources such as a software development kit, should be available to allow for integration into a company's or brand's own app.



How easily can the solution be produced and integrated into the product design and packaging?

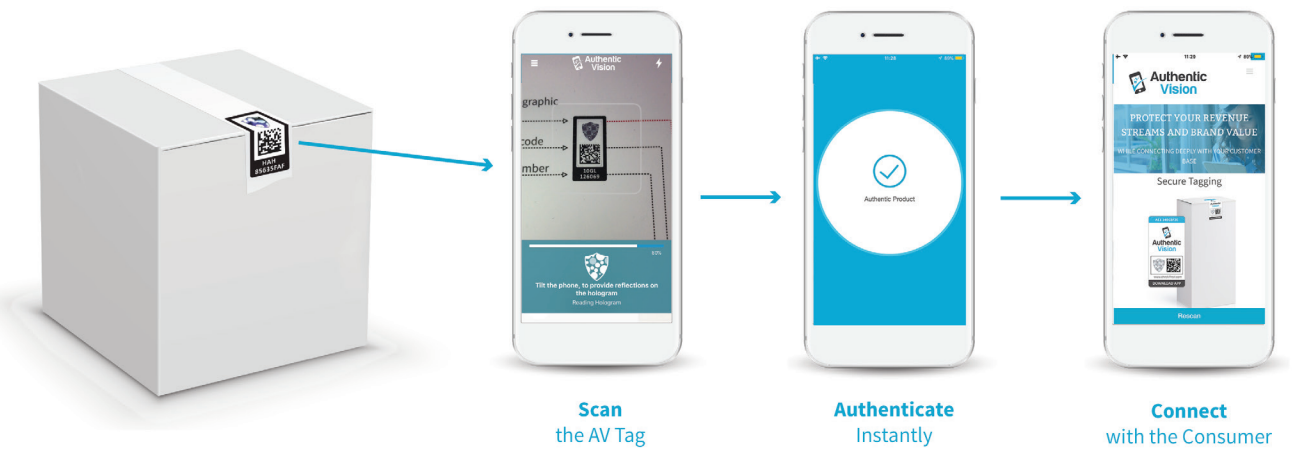
The best solutions today support ready-to-use off the shelf label solutions that can be produced by a large number of professional secure printers. The company should be able to customize the tags in design, size, shape and messaging so they can be integrated into existing labels, closures, boxes, seals, and even the product itself.



Flexible Tagging and Integration

Does the solution leverage the Internet of Things and deliver value-added services?

Easily scanned by every user, a security tag should serve dual purposes, maintaining brand integrity and enabling product interactivity. The best solution should securely connect brands, products and users including a secure communication channel, enabling a broad range of interactive services, including customizable product and license information, digital process workflows, audit and tracking processes, customer engagement and marketing, content redemption and product related CRM services. On top of these interactive capabilities, open a 2-way communication channel, enabling brands to directly push messages to customers.



After scanning the tag and receiving an authentication result, Authentic Vision's app enables secured value-added services like product and channel information, customer services or consumer loyalty and marketing programs.

Arrange a Demo?

We are always ready to help with securing your products and brand value. If you're ready, we would love to hear your story.

Contact our team to get the conversation started and learn about how Authentic Vision secures your products with a simple scan.



About Authentic Vision

Authentic Vision [AV] is the provider of patented security tag solutions backed by a software platform designed for brand managers, product development and operations professionals. Unlike QR codes and holograms, each AV security tag is unique, containing random 3D structures generated in real-time to ensure greater brand integrity and less risk for knock-off products. AV's security tag makes the competitor's secondary verification solutions obsolete.

Authentic Vision GmbH

Josef-Mayburger-Kai 114
5020 Salzburg
Austria

Authentic Vision, Inc.

1005 Market St
San Francisco, CA 94103
USA

www.authenticvision.com

Sources:

- [1] OECD & EUIPO, "Global trade in fake goods worth nearly half a trillion dollars a year," 2016.
- [2] OECD: 2016, "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact," 2016.
- [3] EUIPO, "Counterfeit goods in the EU: Extent of the problem, 2017 Situation Report," 2017.
- [4] Europol, "EU Organized Crime Threat Assessment," 2011.
- [5] International Ant-Counterfeiting Coalition, "The Negative Consequences of International Intellectual Property Theft: Economic Harm, Threats to the Public Health and Safety, and Links to Organized Crime and Terrorist Organizations," 2007.
- [6] OECD, "The Economic Impact of Counterfeiting and Piracy," 2007.