VeraSec Awarded U.S. Patent for Technology Binding File Integrity to File Identity

This new patent establishes the foundational intellectual property behind VeraFile and a new approach to Portable File Identity.

ASHBURN, VIRGINIA, UNITED STATES, September 29, 2026 / EINPresswire.com/ -- VeraSec Technologies LLC today announced the issuance of U.S. Patent No. 12,750,232, “Immutable Document Sealing and Authentication,” covering foundational technology behind VeraFile, the company’s platform for portable file identity and integrity.

> “The filename has been little more than a label - it can become a security control. This patent establishes foundational protection for linking the cryptographic state of a file with its identity.”
>
> *Brian Hajost*

For decades, cybersecurity has focused on protecting everything around a file: users, devices, networks, applications, repositories, and access paths.

VeraSec believes the next Zero Trust security boundary is the file itself.

VeraFile is designed to give digital files a persistent, portable identity that can be independently validated wherever they travel. Rather than relying solely on surrounding infrastructure, VeraFile creates a cryptographic relationship between file contents and file identity and carries that validation information with the file.

“The filename has traditionally been little more than a label,” said Brian Hajost, founder and CEO of VeraSec Technologies and inventor of the patented technology. “We believe it can become a security control. This patent establishes foundational protection for linking the cryptographic state of a file with its identity. VeraFile expands that concept toward a larger objective: every file should be able to prove what it is.”

Closing the File-Integrity Gap

Cryptographic hashing and PKI digital signatures remain essential security technologies, but each addresses only part of the integrity problem.

A cryptographic hash can determine whether file contents have changed, but organizations must preserve the file, the hash, and the trusted association between them. Renaming a file does not alter its conventional content hash.

PKI can establish that a digital signature is valid for signed content, but a signature ordinarily does not bind the external filename to the document, nor protect the signature from being removed.

VeraFile is designed to complement, not replace, hashing and PKI by closing their trust gaps by adding persistent file identity.

At the center of VeraFile is the Validation Integrity Key, or VIK, a compact cryptographic identifier that can bind file contents, filename, selected metadata, and validation policy into a portable, independently verifiable identity. Because the VIK travels with the file, that identity can remain verifiable across email, cloud platforms, enterprise repositories, partner organizations, archives, removable media, and AI workflows.

From Selective Protection to Ubiquitous Protection

Traditional integrity technologies are generally applied selectively because signing, certificate management, and maintaining separate hashes introduce operational friction. VeraFile is being engineered around a different objective: make integrity protection frictionless enough to protect virtually every file.

That becomes increasingly important as AI systems and machines create digital artifacts at enormous scale. Potential applications include documents, images, video, software, logs, healthcare records, legal evidence, financial information, scientific data, and AI-generated content.

VeraSec believes Portable File Identity can emerge as a new Zero Trust cybersecurity control layer - allowing trust to remain attached to digital information instead of disappearing when information crosses an infrastructure or organizational boundary.

Expanding the Intellectual Property

The newly issued patent represents the first layer of VeraSec’s intellectual-property strategy. VeraSec has also filed a continuation patent application seeking additional claims covering expanded implementations as the VeraFile architecture evolves.

The patent milestone follows recent industry recognition. In 2026, Enterprise Security Magazine recognized VeraSec and VeraFile among its Top Portable File Identity Solutions and profiled the company's approach to extending file integrity beyond traditional infrastructure boundaries.

"The bigger story is not the patent itself," Hajost said. "The bigger story is what happens if portable file identity becomes a standard property of digital information. Zero Trust changed how the industry thinks about users, devices, applications, and networks. We believe the same principle now needs to be applied to the files moving among them."

VeraSec is pursuing technology partnerships, licensing relationships, pilot programs, and strategic collaborations with enterprise software providers, cybersecurity vendors, cloud and AI companies, and government organizations.

Every file should be able to prove what it is.

About VeraSec Technologies
VeraSec Technologies LLC develops cybersecurity technologies focused on portable file identity and persistent digital integrity. Its VeraFile technology is designed to move security context from the infrastructure surrounding a file to the file itself, enabling its integrity to remain independently verifiable as data moves across systems, organizations, and trust boundaries.

Media, Licensing and Strategic Partnerships
Brian Hajost
Founder & CEO
VeraSec Technologies LLC
bhajost@verasec.net
www.verasec.net

Brian Hajost
VeraSec Technologies LLC
bhajost@verasec.net
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/946089496

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.