FILECLOUD

FILECLOUD SUPPORTING THE

7 PILLARS* of ZERO TRUST

User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from applications to hypevisors, to include protection of containers and virtual machines.

Data

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network and Environmen

Segment, isolate control (physicall logically) the netv environment with granular policy ar access controls.

*National Security Agency (NSA) Cybersecurity Information Sheet: "Advancing Zero Trust Maturity Throughout the User Pillar"
https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

© 2023 FileCloud | www.filecloud.com

Zero Trust File Sharing

white paper

FileCloud supports the "Seven Pillars of Zero Trust," as defined by the Department of Defense, enabling hyper-secure collaboration within and beyond enterprise network boundaries.

What is Zero Trust File Sharing?

Zero Trust File Sharing^{SM} is FileCloud's solution for accessible collaboration and file sharing that builds on Zero Trust principles. FileCloud incorporates Zero Trust into the platform and empowers users and admins to leverage Zero Trust capabilities. The result is a Zero Trust environment suitable for enterprise and government collaboration and file sharing.

What is Zero Trust?

Zero Trust is a security framework that aims to resolve security gaps exposed by previous security models organized around the network edge or network perimeter.

Network edge: the point of connection between a device or local network and the internet.

Network perimeter: the area around a protected network environment, often defined by containment technologies like firewalls.

Security based on either the network edge or network perimeter focuses efforts on the dividing line between the network. Everything inside the network is seen as safe, and everything outside the network poses cybersecurity risks.

Access to the network was once carefully controlled through hardware and software – users could only access the network after machines were connected. This access was further secured by authentication measures (e.g., login credentials and NTFS permissions) and geographic or physical restrictions.

Therefore, once a user made it past the network perimeter, they were deemed "safe" and often had unlimited access to data contained within.

However, modern networks and devices do not operate in silos or sandboxes with perimeters that can be contained by firewalls, geography, and hardware. The boundary of the network edge has become fluid, in part due to the introduction of mobile devices, internet-of-things (IoT), and digital transformation with cloud technology.

The COVID-19 pandemic drastically accelerated implementation of cloud technology, distributed work environments, and remote applications. In the aftermath of the pandemic, organizations needed to consider the long-term security of remote work connections (bring your own device support), hybrid cloud networks, and rising rates of cyberattacks or malware exposure.

The network perimeter has eroded, and security measures that were once deemed effective are now easily circumvented. IT professionals in the public and private sector have been seeking a new model, one that enables cybersecurity without relying on a perimeter or network edge.

The Rise of Zero Trust

Zero Trust as a concept has been around since 1994, appearing in Stephen Paul Marsh's doctoral thesis, "Formalising Trust as a Computational Concept." This thesis described trust as a social concept that could be formalized as code and then embedded into computer systems.

In 2003, The Jericho Forum began discussing a concept they called "de-perimeterization," which identified vulnerabilities in perimeter-focused security. The group called for identity and access management protocols that focused on securing data rather than a network perimeter.

These protocols "define both the areas and the principles that must be observed when planning for a de-perimeterized future" and were codified in the Jericho Forum Commandments, published in 2007.

In 2009, the term "Zero Trust" as we understand it today was re-introduced by John Kindervag, a former Forrester analyst, alongside the premise "Never Trust, Always Verify" – responding to network edge-based security, which was associated with the premise: "Trust, but Verify."

The concept of Zero Trust described by Kindervag addresses enterprise cybersecurity concerns around the fallibility of the vanishing network edge. It builds on the groundwork laid by Marsh, the Jericho Forum, ongoing discussions within the IT community, and notable cyberattacks like Operation Aurora (2010) and the RSA hack (2011).

Zero Trust emphasizes securing data regardless of where it's located in a network or how the data is accessed. Implementing Zero Trust involves creating a system of "least privilege," where authorized users only have access to the data they absolutely need. Permission to access data must be actively enabled or permitted; the default status is to deny access to data.

The granular security required by Zero Trust is accomplished by curtailing access to data through **authentication, authorization, and re-verification** – not just of users, but also of their devices and even integrated applications and systems.

The user and the device must be able to prove their identity and that they have the necessary permissions to perform the requested action.

The identity of the request is authenticated and verified before granting access to the data. Both identity (authentication) and permissions (authorization) are validated at the time of the request and revalidated with any continued access.

Benefits of Zero Trust

Implementing Zero Trust isn't just a matter of sealing cybersecurity gaps and vulnerabilities exposed by outmoded strategies organized around the network perimeter. **Zero Trust is about optimizing enterprise networks and all their varied connections to create a modern, productive, and secure environment.**

At its core, Zero Trust is a responsive and adaptive cybersecurity strategy that has the potential to revolutionize how we all interact with data – it protects data not just from cyberattacks but also from insider threats, which serve as a significant source of network breaches.

> ***"26% of data breaches are caused by insider incidents, most of which are malicious."***
> - Joseph Blankenship, Research Director at Forrester. 2022 Forrester Security & Risk Conference (Keynote Panel: *Insider Risk Reduction Requires Two Parts Culture, One Part Security*)

By implementing Zero Trust in network architecture, enterprises and organizations can:

- Strengthen enterprise security postures.
- Embrace cloud workload technology and work-from-anywhere policies.
- Reduce attack surface and minimize data exposure/exfiltration.
- Mitigate damage from insider threats and external attacks.
- Ease pain points associated with identify verification and access.

The adaptive nature of Zero Trust also means that advances in artificial intelligence, machine learning, and real-time network access telemetry can be incorporated to automate processes of identity and access management.

Zero Trust as a strategy is not only appropriate but essential to continue working in our data-driven, globally connected world. Ironically, Zero Trust stands to improve our trust in major institutions, including governments and enterprises, by creating secure environments that safeguard our information as consumers, citizens, and contributors – whether that's as an employee, contractor, vendor, consultant, or stakeholder.

US Federal Government Embraces Zero Trust

Since Kindervag's reintroduction, private sector solution providers have applied the term "Zero Trust" to a variety of new tools and applications.

These interpretations of Zero Trust addressed pieces of the cybersecurity puzzle, but there was no unified consensus over Zero Trust as a comprehensive strategy applied in real time to real world use cases.

In recent years, major governments and institutions have provided clarity to the concept by creating holistic roadmaps of Zero Trust hardening initiatives and policy guides.

Notably, the US federal government has established a Zero Trust architecture strategy that outlines how the federal government will enact Zero Trust principles throughout agency infrastructure.

Zero Trust Adoption Timeline

2018

CISA formed as a branch in the Department of Homeland Security to focus on the government's official cybersecurity posture.

2020

NIST Special Publication 800-207, "Zero Trust Architecture," was released.

2021 (May)

An Executive Order was issued, mandating investment and restructuring of federal information security systems.

2021 (September)

CISA issued a Zero Trust Maturity Model to offer guidance on implementing Zero Trust within federal infrastructure across agencies.

2022

The Department of Defense (DoD) released their Zero Trust Strategy and Roadmap for implementation by FY 2027.

2023

The National Security Agency (NSA) published the Cybersecurity Information Sheet (CSI), "Advancing Zero Trust Maturity Throughout the User Pillar."

The Executive Order “on Improving the Nation’s Cybersecurity” explicitly included references to a Zero Trust framework. CISA advisories have also urged government and private sector organizations to begin developing Zero Trust security strategies and have published guidance on how to implement Zero Trust through their Zero Trust Maturity Model.

The DoD Zero Trust Strategy and Roadmap established base level and advanced Zero Trust maturity targets across seven pillars:

- User
- Devices
- Data
- Visibility & Analytics
- Network & Environment
- Automation & Orchestration
- Application & Workload

NIST SP 800-207, “Zero Trust Architecture,” established a definitive understanding for Zero Trust as a framework within the US federal government:

“Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.”

NIST SP 800-207 goes on to define how this approach impacts security considerations around data or resources within IT infrastructure:

"Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource."

Key principles of Zero Trust have also been outlined by the NSA CSI, “Advancing Zero Trust Maturity Throughout the User Pillar.”

These principles are referred to as “Tenets of Zero Trust.”

Zero Trust Tenets

Assume a Hostile Environment:

There are malicious personas both inside and outside the environment. All users, devices, applications, environments, and all other NPEs are treated as untrusted.

Never Trust, Always Verify:

Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.

Apply Unified Analytics

Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics, and log each transaction.

Presume Breach:

There are hundreds of thousands of attempted cybersecurity attacks against DoD environments every day. Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes.

Scrutinize Explicitly:

All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources. Access to resources is conditional and access can dynamically change based on action and confidence levels resulting from those actions.

*National Security Agency (NSA) Cybersecurity Information Sheet: "Advancing Zero Trust Maturity Throughout the User Pillar"
https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

Enterprise Implementation of Zero Trust File Sharing

File sharing and collaboration are critical processes for workforce productivity, regardless of industry. Yet these processes can be corrupted to expose and exfiltrate data; entire systems can be brought down by ransomware and data loss, where malicious actors gain access through something as simple as a phishing scam.

Enterprises need strong security; yet the more security hurdles they put in place, the more users pay (in terms of productivity and morale) to access necessary information. This cost multiplies throughout the enterprise, creating a cascade of degraded efficiency.

Users need easy, intuitive access to files and collaboration tools; admins and CISO's need to ensure access is restricted only to those who are authenticated and authorized.

Zero Trust is the solution enterprises and governments are turning to in ever greater numbers to solve this paradox, not for its strength as a barrier between "insiders" and "threats," but for its adaptive (and strict) approach to protect data at the source.

If implemented correctly, Zero Trust can even support secure collaboration and make file sharing easier. The Zero Trust rollout by the US federal government offers a roadmap for other state and local governments and for the private sector.

The pressures enterprises face from sophisticated cyberattacks provide further incentive to lock down data and implement a system of least privilege, while preserving ease of access for authenticated and authorized users. The Zero Trust model demonstrates that cybersecurity does not have to involve a trade-off though between security and appropriate access.

FileCloud Supporting the 7 Pillars of Zero Trust

Enterprises and public-sector organizations can jump-start their Zero Trust implementation with FileCloud, a hyper-secure file sharing and sync solution with:

- Zero Trust principles built-in
- Flexible deployment options (on-premises, cloud, hybrid)
- Intuitive UI for user collaboration and storage
- Centralized controls for admins
- Compliance-friendly tools to support regional, global, and industry regulations

FileCloud offers an industry-first solution that incorporates functionalities critical to a Zero Trust framework defined by the DoD. These functionalities can be mapped across the Zero Trust pillars:

FILECLOUD SUPPORTING THE

7 PILLARS* of ZERO TRUST

User

Continually authenticate, access, and monitor user activity patterns to govern users’ access and privileges while protecting and securing all interactions.

Devices

Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from applications to hypevisors, to include protection of containers and virtual machines.

Data

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network and Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

Automation & Orchestration

Automate security response based on defined processes and security polices enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Visibility & Analytics

Analyze events, activities and behaviours to derive context and apply AI/ML to achieve a highly personalised model that improves detection and reaction time in making real-time access decisions.

*National Security Agency (NSA) Cybersecurity Information Sheet: "Advancing Zero Trust Maturity Throughout the User Pillar"
https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

User

Zero Trust Objective:
Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

FileCloud Implementation:
FileCloud can integrate with a variety of identity and access management solutions, including Active Directories (AD) and Lightweight Directory Access Protocol (LDAP) as well as best-in-class authentication standards such as Security Assertion Markup Language (SAML), Single Sign-On (SSO), and multi-factor authentication (MFA). These integrations serve to streamline and automate the user authentication process to grant access to FileCloud.

Once the user is authenticated, FileCloud can automate permissions to restrict access only to the necessary data, in line with the Zero Trust principle of least privilege. This can be accomplished via role-based access controls (RBAC), workflow-based authentication, or policy-based authentication. Policies offer granular permission levels to enforce not just which users can see what data, but also how they are permitted to engage with the data.

Admins have broad and deep oversight when it comes to FileCloud monitoring. They can leverage built-in reports or create custom reports to monitor specific file and user activity in the FileCloud environment. They can also pull audit logs for a comprehensive review of file and user activity. These audit logs are unchangeable and can be exported as CSV files for internal review or external audit processes.

Additionally, admins can set up notifications based on certain user activity, which will trigger an alert and prompt action. Admins can also enable reCAPTCHA to distinguish between human and automated access to the system.

- AD/LDAP integration
- SAML & SSO integration
- MFA support (email, SMS, TOTP, Duo Security, etc.)
- RBAC "just enough access"
- Workflow-based authentication, access management, and re-validation
- Policy-based authentication, access management, and re-validation
- Fine-grained user policy control for file sharing and access
- Audit records to monitor user activity patterns
- Granular permissions for better access control
- ReCAPTCHA to distinguish between human and automated access to the system

Devices

Zero Trust Objective:

Understand the health and status of devices to inform risk decisions. Real-time inspection, assessment, and patching informs every access request.

FileCloud Implementation:

With a Zero Trust strategy, users and devices are no longer inherently connected, which calls for security protocols to address devices independently from user-based policies and solutions.

In FileCloud, admins can access a comprehensive device inventory with health and status details pertaining to each connected device. This centralized oversight and management enables admins to enforce configuration policies on devices connected to the system.

Admins can also remotely wipe data from devices or block device access. This is particularly useful to secure enterprise data if a device is reported as lost or stolen or when an employee leaves the enterprise. Admins can also automate approval or denial of device connection attempts via workflows or policies.

For admins or enterprises already working with a Mobile Device Management (MDM) solution, FileCloud offers integration support through its API-driven interface.

- Device inventory with near real-time health/ status of device
- Device blocking and remote wipe
- Centralized device management
- Device approval via workflow and policy enforcement
- Support for external MDM providers
- Mobile device security status
- Centralized device management

Applications and Workloads

Zero Trust Objective:

Secure everything from applications to hypervisors, to include protection of containers and virtual machines.

FileCloud Implementation:

FileCloud's deployment flexibility ensures the solution can be configured and segmented as needed to isolate and secure application and workload data.

Built-in antivirus scanning and Data Leak Prevention (DLP) solutions also help prevent the introduction of threats into the system or the inappropriate exfiltration of data, whether attempted by a user, application, or workload.

The API extensibility of FileCloud also provides options for enterprises to integrate with third-party ICAP, CASB, or DLP solutions.

- Private cloud configuration
- Isolated network/air-gapped support
- Antivirus/malware scanning
- DLP
- ICAP & CASB integration

Data

Zero Trust Objective:

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

FileCloud Implementation:

Data is the most valuable asset an enterprise can have, and securing data (regardless of its location) is the heart of a Zero Trust strategy. With FileCloud, data can be secured at rest with AES encryption and in transit with SSL or TLS protocols. FileCloud can also be run in “FIPS mode” with certification for encryption standards that comply with FIPS 140-2.

FileCloud also support AWS Server-Side Encryption with Customer-Provided Keys (SSE-CPK) and Server-Side Encryption with Key Management Services (SSE-KMS). These solutions offer an additional level of encryption for data stored in containers or servers integrated with FileCloud.

Encryption is only one of many functionalities FileCloud offers to secure data. Another major element is file access control, which can be levied by admins and users. Folder-level permissions support folder, sub-folder, and file-level permissions to achieve a granular hierarchy of access. FileCloud also supports NTFS permissions integration – admins will not have to replicate permissions that have already been configured for network shares.

Furthermore, admins can set custom DLP rules based on metadata or other file attributes to limit and manage file access and sharing. Alternatively, they can create global, user, or group policies that enforce access and sharing rules for specific files and folders.

These policies can be automated through workflows, for instance to require approval before a file is shared. This supports admin oversight and management over shares within the system.

To achieve better visibility over data (thus supporting better management and security), admins can utilize built-in metadata sets or create custom sets to tag data within the system.
These tags help locate personally identifiable information (PII) or other sensitive or confidential data in FileCloud.

Metadata combined with OCR text recognition are key elements of FileCloud’s Smart Content Classification, which scans uploaded files and applies appropriate metadata automatically. This functionality can be used in tandem with DLP (Smart DLP) and policies. Classifying data reduces risks associated with orphan data and lightens the administrative burden associated with securing data by automating metadata application and creating policies, DLP rules, and other security measures triggered by metadata.

Data (continued...)

When it comes to sharing files, FileCloud supports users (and admins) in maintaining control over data and ensuring data access is restricted to authorized users and intended recipients. Users in FileCloud can share files or folders with granular permissions (read, write, download, upload, share). They can also send a share link as either public or private, leverage password-protection, limit the number of downloads, and even set an expiration date.

Digital Rights Management (DRM) takes this control over data sharing a step further. Share links are shared in a secure document container, which can be controlled by the user even after distribution. Users can restrict the field of vision within the opened document and even revoke access to the data entirely (meaning the recipient will no longer be able to open it). The container also enables users to disallow downloads and screen captures.

Notably, FileCloud also offers industry-first Zero Trust File SharingSM. By sharing data via encrypted (AES 256-bit) ZIP file with password-protection, users can ensure that data can only be decrypted by individuals with the Zero Trust password. The password is never stored in FileCloud, in line with the Zero Trust tenant of presuming a breach is inevitable; highly sensitive or confidential data remains secure. Share permissions can be set to read only (preview, view, and download) or read-write (view, download, upload, delete).

- At-rest encryption for local storage (AES 128 or 256-bit encryption)
- In-transit encryption via SSL/TLS protocols
- FIPS certification for encryption standards of data at rest and in transit
- Support for Server-Side Encryption with Customer-Provided Keys (SSE-CPK) and Server-Side Encryption with Key Management Services (SSE-KMS).
- File access controls:
    - Folder-level permission support
    - NTFS permission support
    - Custom DLP rules
    - Policy-based rules for access and sharing
    - Workflow-based rules for access and sharing
- Metadata-based tagging support
- OCR support for automatic data classification and tagging
- DRM support: revoke permission any time after sharing, limit downloads, and disallow screen captures
- Zero Trust File Sharing^{SM}: Secure encrypted (AES 256-bit) folder support with customer provided password (password is never stored in FileCloud)

Network and Environment

Zero Trust Objective:

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

FileCloud Implementation:

FileCloud is a flexible enterprise and government solution that supports a variety of deployments, including on-premises, cloud, and hybrid. For cloud deployments, FileCloud can be configured to operate as a private cloud or as an isolated, air-gapped network (no interact connections required to function). This means that FileCloud can perform even within NIPR, SIPR, and JWICS.

FileCloud also supports multitenancy, which enables multiple sites to be run as separate tenants and databases, while maintaining centralized control.

DLP rules can also be used to control the network environment and restrict login attempts based on access attributes such as IP address, subnets, or even country.

- Air-gapped network support (e.g., NIPR, SIPR, JWICS)
- Multi-tenancy (segmented sites and databases)
- DLP rules

Automation and Orchestration

Zero Trust Objective:
Automate security response based on defined processes and security polices enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

FileCloud Implementation:
FileCloud's hyper-security comes not simply from the variety of security features built into the platform, but also from how these features overlap and reinforce each other, with minimal administrative oversight once enabled.

For example, admins can create custom DLP rules that are triggered by user or file attributes such as metadata. These DLP rules are designed to prevent both access and data exfiltration. With Smart Classification enabled, even the application of metadata feeding into DLP rules can be automated.

FileCloud can also be configured with access policies based on allow and disallow lists for IP addresses, and workflow automation can be implemented to block devices or users.

- Custom DLP rules to block access based on attributes/metadata
- Automated metadata tagging with Smart Content Classification
- Workflow automation to automate device blocking
- Allow and disallow lists to support IP-based access

Visibility and Analytics

Zero Trust Objective:
Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

FileCloud Implementation:
Admins are empowered in FileCloud with a powerful admin console and dashboard that can be customized to meet the needs and demands of the administrative role.

Admins have access to complete message logs (both incoming and outgoing), which can be archived and searched. SIEM integration in FileCloud supports the admin ability to send logs using LEEF/CEF format to Splunk for analysis.

Admins can also collect information via reports; FileCloud offers built-in reports that can be run at any time, or admins can create custom reports to capture specific information. Additionally, the comprehensive audit log captures significant details relating to who (user) did what (activity) to which data (file/folder affected) how (device access) and where (IP address). Reports and audit logs can be exported for internal or external review.

- Complete message logging (incoming and outgoing), archival, and search capability.
- SIEM integration
- Built-in and custom reports
- Comprehensive audit log

Conclusion

Zero Trust is a cybersecurity model that embraces the changes that have impacted IT infrastructure over the past two decades, including cloud transformation and work-from-anywhere technologies. It acknowledges the need to exchange information to collaborate effectively, as well as the web of connections (extending within and beyond the traditional network perimeter) that are often required for collaboration to take place.

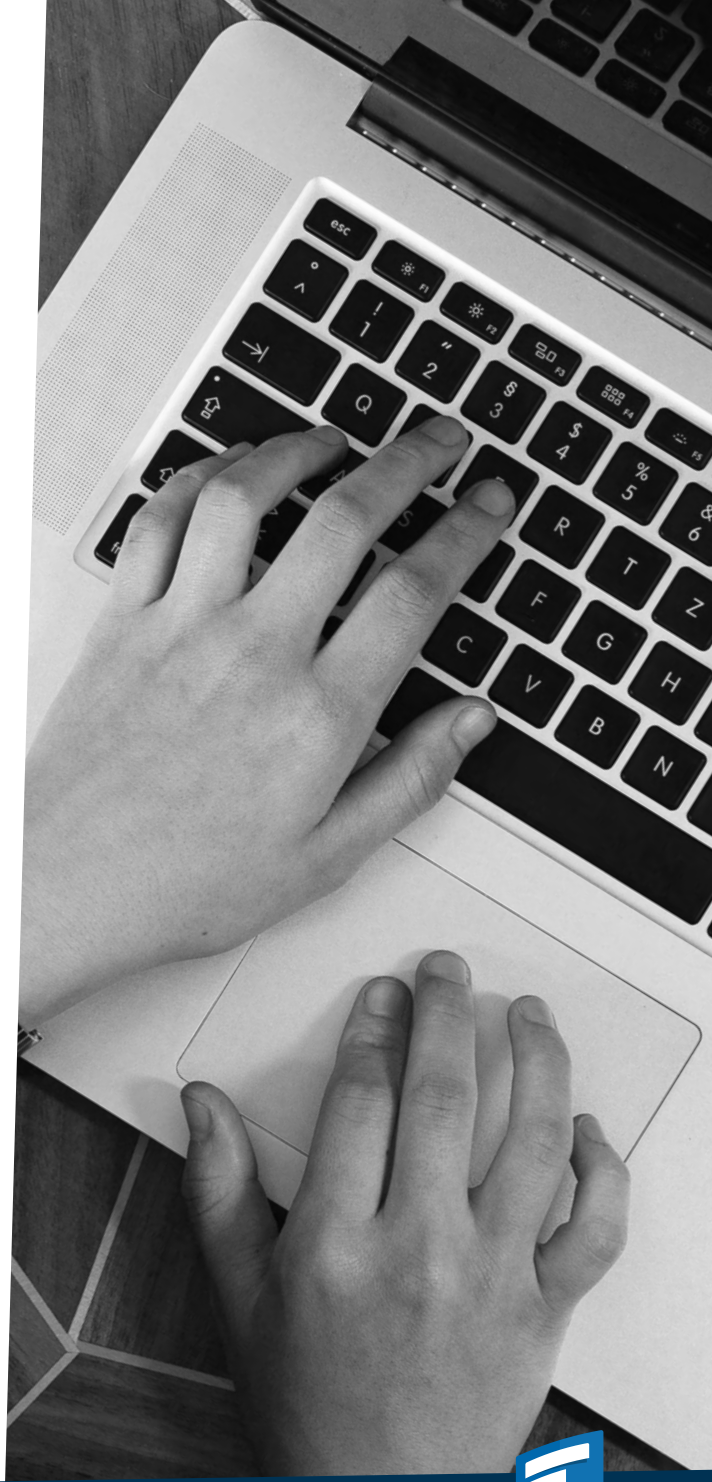
Building from this understanding, Zero Trust offers a consistent method to control and secure data flowing through these varied connections, regardless of whether that connection is person-to-person, person-to-system, or system-to-system. Principles of least privilege reduce the attack surface, with authentication, authorization, and validation processes protecting data at the source.

Zero Trust gives enterprises and organizations the means to:

- ✓ Optimize systems and processes.
- ✓ Ease user and admin pain points.
- ✓ Build confidence in their brand.

FileCloud offers a comprehensive solution to bring Zero Trust within reach, whether by integrating with existing systems or launching a brand-new environment.

FREE TRIAL



Resources for Further Reading

Mary K. Pratt. "History and Evolution of Zero Trust Security."

- *TechTarget. Published 12 Oct 2022. Accessed 25 Apr 2023.*

Ganesh N Kumar. "History of Zero Trust Security."

- *Infraon. Published 16 Nov 2021. Accessed 25 Apr 2023.*

Kapil Raina. "Zero Trust Security Explained: Principles of the Zero Trust Model."

- *Crowdstrike*. Published 17 Apr 2023. Accessed 25 Apr 2023.

Mark Loveless. "The Evolution of Zero Trust."

GitLab. Published 1 Apr 2021. Accessed 25 Apr 2023.

C.J. Haughey. "What Is Zero Trust? A Complete Guide for Security Professionals."

- *SecurityIntelligence. Published 30 Sep 2021.*

About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.

1M+	3000+	100+	90+
USERS	ENTERPRISES	RESELLERS	COUNTRIES

13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

CONTACT US

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES

REUTERS

US Army Corps of Engineers

NASA

COLUMBUS REGIONAL HEALTH

TOYOTA

Deloitte.

Copyright Notice

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.