

Zero Trust with OpenText EDOCS

[Joshua Wertheim](#)

President

Wertheim Global Solutions

Date: 2024-11-17

Version: 1.0



Contents

What is Zero Trust?.....	2
Zero Trust and Rogue Internal End-Users.....	4
Zero Trust and EDRMS.....	7
Consequences	10
Guardian Internal Information Security	14
Other Solutions.....	16
Comparison of OpenText™ eDOCS Defense and Guardian Internal Information Security	16
Overall Conclusions.....	19

What is Zero Trust?

Zero Trust is a modern cybersecurity framework that assumes no user or system, whether inside or outside an organization's network, can be trusted by default. Instead of relying on a traditional "trust but verify" approach, Zero Trust follows the principle of **"never trust, always verify."**

Key Principles of Zero Trust

1. **Least Privilege Access:** Users and systems are given the minimum access necessary to perform their tasks, reducing the risk of unauthorized access or lateral movement within a network.
2. **Continuous Verification:** Every access request is verified in real time, regardless of whether the request comes from inside or outside the organization's perimeter.
3. **Micro-Segmentation:** Networks are divided into smaller segments to minimize the scope of damage in case of a breach.
4. **Identity-Centric Security:** Emphasizes strong authentication methods (e.g., multi-factor authentication, biometrics) to ensure that only verified users and devices gain access.
5. **Assume Breach:** Organizations operate as if a breach has already occurred, ensuring robust monitoring, incident response, and containment strategies.
6. **Device and Network Trust Validation:** All endpoints (devices) and network environments are assessed for compliance before granting access.

Benefits of Zero Trust

- **Reduced Attack Surface:** Limits opportunities for attackers to move laterally within a network.
- **Improved Compliance:** Helps organizations meet stringent security and privacy regulations.
- **Enhanced Data Protection:** Safeguards sensitive data by ensuring only authorized users can access it.
- **Mitigated Insider Threats:** Identifies and blocks unusual behavior even from trusted insiders.

Zero Trust in Action

A Zero Trust framework often integrates technologies like:

- Identity and Access Management (IAM)
- Endpoint Detection and Response (EDR)
- Multi-Factor Authentication (MFA)

- Security Information and Event Management (SIEM)
- Data Loss Prevention (DLP)
- Network Access Control (NAC)

In summary, **Zero Trust** moves security from a perimeter-based model to one focused on securing users, applications, and data wherever they are. It's particularly relevant in today's cloud-driven, remote-work environment.

Zero Trust and Rogue Internal End-Users

How does zero trust help when an end user with valid credentials decides to steal confidential information that user has been granted access to in order to perform their job duties?

Zero Trust can mitigate risks associated with **insider threats**, even when the insider uses valid credentials, by focusing on **continuous monitoring, behavior analysis, and context-aware access control**. Here's how Zero Trust helps in such scenarios:

1. Continuous Monitoring and Behavioral Analytics

- **Activity Baselines:** Zero Trust solutions establish a baseline of normal user behavior, such as typical login times, accessed files, and network activity.
- **Anomaly Detection:** If an employee starts downloading unusually large volumes of data, accessing files they rarely use, or performing actions at odd times, these anomalies trigger alerts or automated actions (e.g., restricting access or flagging the activity for review).

Example: If a user with valid credentials suddenly downloads all files from a sensitive project directory, Zero Trust tools can detect this as abnormal behavior and stop the action.

2. Just-In-Time and Least Privilege Access

- **Limited Permissions:** Users are granted the minimum access necessary for their tasks, and permissions are reviewed and updated dynamically based on their job requirements.
- **Session-Specific Access:** Access can be granted on a time-limited or project-specific basis, minimizing prolonged exposure to sensitive information. This can be accomplished by setting permissions to a group rather than to individual users, and by adding a user to the group they are granted access to the information, while removing them from the group revoke their access.

Ensuring least privilege access should be **automated** to eliminate errors and inconsistencies. Instead of relying on end-users to manually set permissions, which often leads to misconfigurations or accidental exposure of sensitive materials, **rule-based automated systems** should control access dynamically based on metadata and organizational policies.

Example: A developer might be granted access to specific source code repositories only for the duration of their project, not indefinitely.

3. Context-Aware Access Control

- **Location and Device Checks:** Access can be restricted based on the user's location, device compliance, or other contextual factors. For example, if a user tries to access sensitive data from an unrecognized device or location, access can be denied.
 - **Granular Policies:** Policies can enforce restrictions such as "users cannot download more than 10 documents in one session" or "data cannot be exported to external storage."
-

4. Data Loss Prevention (DLP) and Encryption

- **DLP Solutions:** Zero Trust integrates with DLP tools to monitor and prevent unauthorized data exfiltration. For instance, it can block attempts to email sensitive files, copy data to USB drives, or upload it to cloud services.
 - **Encryption:** Even if the insider manages to access and steal data, encryption ensures that the stolen information is unusable without proper decryption keys.
-

5. Risk-Adaptive Responses

- **Dynamic Actions:** If suspicious activity is detected, Zero Trust systems can automatically:
 - Revoke access
 - Disable accounts
 - Notify administrators
- **User Reauthentication:** Even during an active session, users can be required to reauthenticate if their behavior changes significantly.

Example: If an HR employee accesses 100 personnel records in one session when they usually access only 5, the system can log them out and require justification for the activity.

6. Insider Threat Awareness and Training

- While technology is critical, Zero Trust also emphasizes the human element by:
 - Educating employees about security policies
 - Using AI tools to detect non-malicious insider risks, such as accidental sharing or mismanagement of sensitive information
-

Zero Trust isn't just about preventing external threats; it ensures that even users with legitimate access are continuously verified and monitored, making it harder for malicious insiders to misuse their credentials unnoticed.

Zero Trust and EDRMS

What if the user doesn't directly access the files, but accesses them through an EDRMS system?

When users interact with files through **EDRMS systems like OpenText EDOCS**, a **Zero Trust framework** remains highly effective by extending its principles and tools to monitor and secure the **application layer**.

Tracking User Activities:

EDRMS systems track and record practically every activity performed by end-users, such as file access, edits, downloads, and searches. While how this fits within GDPR privacy laws is a topic for another discussion, this activity data is crucial for detecting anomalies. It allows organizations to identify when a user exceeds normal behavioral patterns, such as accessing a high volume of sensitive documents in a short period.

1. Application-Level Monitoring and Auditing

- **Action Tracking:** Every interaction with the document management system is logged, including searches, file views, edits, downloads, and shares.
- **Behavior Analysis:** Patterns of access within the DMS are continuously monitored to detect deviations from normal usage.

Example: If a user typically accesses 5–10 documents per day and suddenly views or downloads 200 documents in a short period, the system can flag this activity as suspicious.

2. Granular Role-Based Access Control (RBAC)

- **Automated Rule Enforcement:** Permissions should be dynamically applied based on organizational rules and metadata. For example, if client information needs to be accessible only to a specific set of users, this should be **automatically enforced** every time such data is created or edited. Manual access settings should be avoided to prevent errors and ensure consistency.
- This approach enables ethical walls (or Chinese walls), often used in law firms, to protect confidential information based on predefined criteria, such as project type or client metadata. access, preventing them from downloading, exporting, or sharing files unnecessarily.

Example: A marketing user might have access to client brochures but cannot download confidential pricing models stored in the same system.

3. Just-In-Time (JIT) Access

- **Dynamic Access Grants:** Access to specific documents or folders can be granted on a time-limited or purpose-specific basis within the DMS.
- **Session Context:** Permissions can be revoked dynamically based on changes in the user's behavior, location, or other risk signals.

Example: If a user logs in from an unusual IP address, the system can restrict their access to sensitive files even though their credentials are valid.

4. Context-Aware Access Policies

- **Data Sensitivity Rules:** Different levels of scrutiny can be applied based on the sensitivity of the documents being accessed.
- **Action-Specific Triggers:** Policies can prevent bulk actions, such as mass downloads or exports, even if the user has legitimate access.

Example: The system might block attempts to download more than 10 files in one session or prohibit exporting any documents to external cloud services.

5. Integration with Data Loss Prevention (DLP)

- **Content Scanning:** DLP tools integrated with the DMS can scan files for sensitive content and enforce policies to prevent unauthorized sharing or exfiltration.
- **Watermarking and Tracking:** Documents downloaded or shared from the DMS can be watermarked and tracked to deter misuse and provide traceability.

Example: If a user shares a sensitive document via email, the DLP system can block the email or redact confidential portions of the file.

6. Behavioral Analytics in the EMS/DMS

- **Entity Behavior Analysis (UEBA):** An effective system can analyze user behavior within the EMS/DMS to detect patterns indicative of insider threats.
- **Automated Alerts:** Alerts can be triggered for specific suspicious activities, such as:
 - Frequent access to documents outside the user's project.
 - Repeated searches for sensitive keywords or categories.
 - Bulk actions like downloading an entire folder.

Example: If an employee with access to HR records begins accessing salary details for multiple departments without authorization, an alert can be generated for investigation.

7. Proactive Measures for EDRMS Systems

- **Restrict API Use:** Ensure that APIs for accessing DMS data are secured and monitored to prevent automated data extraction.
 - **Session Recording:** Record and analyze user actions within the DMS, providing an audit trail for all interactions.
-

8. Incident Response and Account Control

- **Automated Lockouts:** If suspicious behavior is detected, the user's access to the DMS can be immediately disabled while an investigation is conducted.
- **Forensic Analysis:** Detailed logs and analytics from the DMS provide evidence for investigations, allowing security teams to determine the extent of the threat.

Example: Account disablement when a user with access to sensitive legal documents begins accessing unrelated high-profile case files in bulk.

Why Zero Trust is Still Effective

By enforcing Zero Trust principles **at the application level** and integrating with tools like Guardian, organizations can:

- Detect and prevent misuse of access rights within EDRMS systems.
- Limit the scope of data exposure even for authorized users.
- Provide visibility and accountability for every user action within the DMS.

This layered approach ensures that insider threats are contained, even when users work within highly structured EDRMS systems.

Consequences

What could happen when an organization does not implement continuous monitoring and behavior analytics?

When an organization does not implement **continuous monitoring** and **behavior analytics**, several risks and vulnerabilities emerge, particularly in addressing insider threats and advanced cyberattacks. Here's what could happen:

1. Increased Risk of Insider Threats

Without continuous monitoring, malicious or negligent insiders can exploit their access for long periods without detection.

- **Data Exfiltration:** Employees could steal sensitive data (e.g., intellectual property, client lists) using valid credentials, with no one noticing until the damage is done.
- **Sabotage:** Disgruntled employees could deliberately damage or alter critical files or systems, impacting business operations.
- **Unintentional Misuse:** Employees might accidentally share sensitive data, misconfigure access settings, or violate compliance policies without awareness.

Example: An employee downloads sensitive customer data for personal use. Without monitoring, this activity may only be discovered after customers report fraud or data breaches.

2. Delayed Detection of Cybersecurity Breaches

If behavior analytics are not in place, an organization might remain unaware of breaches for weeks or months, allowing attackers to maintain persistence and escalate their privileges.

- **Lateral Movement:** Attackers who gain access to one system can move laterally through the network, exploiting other systems and accounts undetected.
- **Data Breaches:** Sensitive data can be exfiltrated in small increments over time, evading traditional detection methods.
- **Advanced Persistent Threats (APTs):** Attackers can establish a foothold in the network and remain undetected for extended periods.

Example: A phishing attack results in stolen credentials. The attacker uses them to log in, impersonate the employee, and access sensitive financial data. Without behavioral monitoring, this unauthorized activity might blend in with normal operations.

3. Regulatory Non-Compliance

Many industries require organizations to implement continuous monitoring and data protection mechanisms to comply with regulations like GDPR, HIPAA, CCPA, or SOX.

- **Fines and Penalties:** Failing to detect or report unauthorized access to sensitive data can result in hefty fines and penalties.
- **Loss of Certifications:** Non-compliance can lead to the loss of certifications, such as ISO 27001 or PCI DSS, affecting the organization's ability to operate in certain markets.

Example: A healthcare organization fails to monitor access to patient records. If a breach occurs, the organization may face HIPAA penalties and lawsuits.

4. Missed Early Warning Signs

Behavior analytics often detect early warning signs of malicious activity, such as unusual login patterns or data access behaviors. Without these tools, such signs may go unnoticed.

- **Unusual Login Locations:** A legitimate user's credentials are used from an unexpected geographic location, which could indicate account compromise.
- **Abnormal Access Patterns:** A user who typically accesses 10 files per day suddenly downloads 500 files in one session, but no alert is generated.
- **Privilege Escalation Attempts:** Unauthorized attempts to access higher-level systems or administrative accounts might not be flagged.

Example: An insider begins systematically downloading large volumes of data over several weeks. Without monitoring, these downloads are treated as routine activity.

5. Financial and Reputational Loss

The financial and reputational damage resulting from undetected threats can be catastrophic.

- **Revenue Loss:** Breaches can result in downtime, lost customers, and legal expenses.
- **Customer Trust Erosion:** Clients may lose confidence in the organization's ability to safeguard their data.
- **Market Share Decline:** Competitors may exploit the fallout from security incidents to capture disillusioned customers.

Example: An undetected breach leads to the theft of sensitive customer data. The breach becomes public months later, prompting lawsuits, customer attrition, and a drop in stock value.

6. Inefficient Incident Response

Without monitoring and analytics, security teams lack the visibility needed to respond quickly and effectively to incidents.

- **Delayed Containment:** Threat actors have more time to escalate their activities before being detected.
- **Lack of Forensic Data:** Without detailed logs, it becomes challenging to investigate incidents, identify root causes, and determine the scope of impact.

Example: After a ransomware attack, the organization cannot determine how the attacker gained access, leaving vulnerabilities unaddressed and risking repeat incidents.

7. Overreliance on Perimeter Security

Organizations that lack behavioral analytics often rely solely on perimeter defenses (e.g., firewalls, VPNs), which are insufficient in today's threat landscape.

- **Credential-Based Attacks:** Perimeter defenses cannot detect when attackers use stolen credentials to blend in as legitimate users.
- **Cloud and Remote Work Vulnerabilities:** Modern environments blur traditional network boundaries, making perimeter-based approaches outdated.

Example: An attacker gains access to a cloud-based document management system. Since the attack does not breach the perimeter, it goes unnoticed for months.

8. Higher Costs for Post-Incident Recovery

The longer a threat goes undetected, the costlier it becomes to recover.

- **Data Restoration:** Recovering lost or corrupted data can be expensive and time-consuming.
- **Legal Expenses:** Lawsuits, regulatory fines, and breach notifications add to the financial burden.
- **Reputation Repair:** Rebuilding trust with customers and stakeholders requires significant investment.

Example: A retail company incurs millions in legal and operational expenses after failing to detect a data breach that exposed customer credit card information.

Conclusion

Without **continuous monitoring** and **behavior analytics**, organizations expose themselves to greater risks from insider threats, external attacks, and regulatory penalties. Proactive monitoring is essential to detect and mitigate threats in real time, reduce incident impact, and maintain trust in today's complex and interconnected environments.

Guardian Internal Information Security

Guardian stands out not only for its robust capabilities in **continuous monitoring, behavior analysis, and context-aware access control**, but also for its **cost-effectiveness** and **ease of implementation** compared to other solutions. Here's what makes Guardian uniquely qualified:

1. Continuous Monitoring

- Guardian provides **real-time monitoring** of user activity, focusing on identifying unusual patterns, potential misuse, or insider threats.
 - Unlike broader toolsets that require significant configuration and integration, Guardian is optimized for **immediate deployment**, offering actionable insights with minimal setup.
-

2. Behavior Analysis

- Utilizing **User and Entity Behavior Analytics (UEBA)**, Guardian establishes a baseline of normal user behavior and detects anomalies that could indicate malicious or negligent activity.
 - This proactive approach helps mitigate risks such as unauthorized data access, mass downloads, or unusual file activity.
-

3. Context-Aware Access Control

- Guardian dynamically adjusts access permissions based on **real-time factors** like user behavior, roles, and activity context.
 - This ensures sensitive data is only accessible to authorized users under the right conditions, reducing the likelihood of misuse.
-

4. Cost-Effectiveness

- **Pricing starts at \$6,000 USD plus annual maintenance of approximately 22% of the published price**, making Guardian a much more affordable option than large-scale monitoring solutions like OpenText ArcSight or others.
 - By focusing specifically on user activity and behavior analysis, Guardian eliminates the need for costly additional modules or system-wide licenses that broader platforms often require.
-

5. Simplicity of Implementation and Maintenance

- As a **standalone application**, Guardian is **much simpler to implement and maintain** than integrated solutions bundled within larger toolsets.
 - This independence allows Guardian to function effectively without requiring heavy customization, complex integrations, or ongoing maintenance associated with EDRMS monitoring suites.
 - IT teams can deploy Guardian faster, reducing operational overhead and allowing for quick ROI.
-

Why Choose Guardian?

With its focus on targeted functionality, affordability, and ease of use, Guardian is the ideal solution for organizations seeking:

- **Comprehensive monitoring and analysis** without the complexity of enterprise-level toolsets.
- A solution tailored to address **insider threats** and **context-sensitive access control** at a fraction of the cost.
- **Streamlined implementation** that minimizes disruptions and maximizes efficiency.

Guardian's ability to deliver high-value security outcomes at a competitive price point, combined with its simplicity, positions it as a uniquely qualified tool to meet modern security demands effectively.

Other Solutions

Besides Guardian Internal Information Security, what solutions that perform continuous monitoring and behavior analysis exist for OpenText EDOCS?

Continuous monitoring and behavior analysis are essential for maintaining the security and efficiency of OpenText EDOCS. Besides Guardian Internal Information Security, the only other solution is OpenText eDOCS Defense

Comparison of OpenText™ eDOCS Defense and Guardian Internal Information Security

Feature/Functionality	OpenText™ eDOCS Defense	OpenText™ Internal Information Security
Primary Purpose	Enhances security within eDOCS by providing document-level encryption and activity monitoring.	Monitors user activities in real-time within eDOCS to detect and prevent internal security breaches.
Activity Monitoring	Offers real-time monitoring of user activities to detect unusual behavior patterns.	Provides continuous, real-time monitoring of user actions, such as document access and downloads.
Anomaly Detection	Detects anomalies based on activity counts , such as an unusually high number of accesses or downloads.	Uses a Predictive Analysis Engine to identify anomalies by comparing user behavior against established baselines and predictive patterns.
Identifying Phishing Attempts	Identifies potential phishing activity by flagging anomalous actions performed with valid user credentials, such as unusual access locations or abnormal file activity.	Detects phishing-related anomalies using its Predictive Analysis Engine, flagging suspicious activity like bulk access, geographic inconsistencies, or atypical usage patterns.
Identifying Insider Threats	Flags excessive document downloads, unusual search patterns, or access outside typical times, which may	Monitors insider activity for behavioral deviations, such as unexpected bulk downloads, file transfers, or improper access to confidential information,

Feature/Functionality	OpenText™ eDOCS Defense	OpenText™ Internal Information Security
	indicate an insider exfiltrating data.	automatically alerting or disabling accounts as needed.
Instant Notifications	Sends alerts to administrators upon detecting suspicious activities.	Sends immediate notifications via email or text when user activities exceed established thresholds.
Account Disabling	Can lock out users when a breach is detected to prevent further unauthorized access.	Has the capability to automatically disable user accounts upon detecting violations of security policies.
Document Encryption	Provides encryption at rest for documents within the eDOCS repository.	Does not offer document encryption features.
Integration with eDOCS	Seamlessly integrates as a module within the eDOCS environment.	Integrates directly with eDOCS DM to monitor repository usage.
Customization	Allows configuration of monitoring rules and encryption settings.	Enables setting of specific rules and thresholds for monitoring user activities.
Reporting and Auditing	Maintains logs of all alerts and activities for audit purposes.	Generates reports on user activities and security incidents for compliance and auditing.
How Anomalies Are Identified	Activity Counts: Flags anomalies based on thresholds like excessive downloads or unusual access volume.	Predictive Analysis Engine: Uses machine learning and behavioral baselines to predict and identify unusual or suspicious user behavior.
Targeted Threats	Addresses both internal and external threats by securing documents and monitoring access.	Detects and mitigates insider threats (e.g., data exfiltration) and external threats (e.g., phishing).

Capabilities for Two Types of Threats

1. Phished Credentials (External Threats):

- **eDOCS Defense** flags suspicious activity, such as an unusually high number of document accesses or access from unexpected locations, which may indicate that a valid user's credentials were compromised.
- **Guardian** enhances this by leveraging its Predictive Analysis Engine to detect discrepancies in behavior, such as logging in from multiple locations or accessing unusual files.

2. Insider Threats (Internal Bad Actors):

- **eDOCS Defense** identifies insider threats primarily by monitoring for threshold-based anomalies like excessive file downloads or accessing restricted documents.
- **Guardian** uses advanced behavior analytics to detect more subtle deviations from typical activity, such as an employee gradually accessing sensitive files over time, and can automatically disable accounts to stop malicious actions.

Conclusion

Both **eDOCS Defense** and **Guardian for eDOCS** provide effective detection and mitigation for external and internal threats, including phishing attacks and insider data exfiltration. However, **Guardian's Predictive Analysis Engine** gives it a significant edge in identifying subtle behavioral anomalies, making it more comprehensive for advanced threat detection in environments where both phishing and insider risks are a concern.

Note: This chart and the conclusions were created on 11/18/2024 by ChatGPT, when asked to compare the two solutions. I merely copied and pasted the response into this document as-is.

Overall Conclusions

Through our discussion, we've explored the challenges of insider threats, the importance of robust monitoring systems, and how various tools and frameworks address these needs. Here are the key conclusions:

1. Insider Threats Require Targeted Solutions

- High-profile cases like Edward Snowden highlight the dangers of insider threats, where trusted individuals with valid credentials misuse their access to exfiltrate sensitive data.
 - Addressing these risks requires a combination of **continuous monitoring**, **behavior analysis**, and **context-aware access control** to identify anomalies and mitigate threats in real time.
-

2. The Role of Zero Trust

- The **Zero Trust framework** provides a solid foundation for modern security practices by assuming no user or system can be trusted by default.
 - Its principles, such as **least privilege access**, **continuous verification**, and **assume breach**, align well with the need to monitor and restrict insider activity.
-

3. Guardian as a Superior Solution

- Guardian stands out as an ideal solution for addressing insider threats within systems like OpenText EDOCS due to its:
 - **Comprehensive monitoring** of user activity.
 - **Behavioral analysis** to detect anomalies.
 - **Context-aware access control** to restrict or adjust permissions dynamically.
 - Guardian is **cost-effective** (starting at \$6,000 per organization) and **simple to implement**, making it accessible for organizations of all sizes.
-

4. The Importance of Continuous Monitoring

- Organizations without continuous monitoring and behavior analytics are vulnerable to insider threats, delayed breach detection, and regulatory non-compliance.
- Tools that combine monitoring, real-time alerts, and automated responses are essential to safeguarding sensitive data.

5. Context-Aware Access Control is Critical

- Security solutions must dynamically adapt access permissions based on user behavior, roles, and activity context. This approach minimizes risks and ensures data is only accessible under the right conditions.
- Guardian excels here, offering targeted, real-time adjustments without the complexity of larger, more general toolsets.

6. Cost and Simplicity Matter

- Tools like Guardian are uniquely positioned to provide **high-impact security** at a lower cost compared to integrated systems.
- The simplicity of implementation and maintenance is crucial for organizations with limited IT resources, reducing the burden on security teams.

7. A Holistic Approach is Necessary

- Effective security requires a combination of:
 - **Robust tools** like Guardian to detect and respond to threats.
 - **Proactive policies** based on Zero Trust principles.
 - **Role-based rules** to limit data access based on user needs and sensitivity levels.

Final Thoughts

Organizations face increasing threats from insiders and external actors, making it imperative to adopt solutions that address these challenges effectively. Tools like Guardian Internal Information Security not only provide targeted monitoring and analysis but also offer affordability and ease of use, making them a practical choice for addressing modern security needs.

By implementing solutions aligned with Zero Trust principles and ensuring continuous monitoring, organizations can protect sensitive data, enhance compliance, and maintain the trust of their stakeholders.

Although we have limited this discussion to how our Guardian Internal Information Security solution integrates perfectly into an organization's Zero Trust processes, we also have solutions for automated access control and would be happy to discuss our other offerings as well.



WERTHEIM GLOBAL SOLUTIONS LLC


Contact Us for More Information

- **Get a demo** of Guardian for OpenText Content Server and eDocs.
- Learn more about Guardian's capabilities.
- Start your Guardian pilot.
- Find an OpenText partner certified on Guardian.

Protect your most valuable asset - your information.

opentext SolEx Partner
Gold



- [My LinkedIn](#) 
- [Email me](#)
- [Watch a video](#)
- [Fill out a contact form](#)
- [Read more about Guardian](#)

