CourtAlert ECF Inform and Case Management
Cloud Security

July 28, 2023

We at CourtAlert understand that in today's digital world, data security is paramount. The CourtAlert systems are designed to treat your data with confidentiality and security, taking significant steps to ensure it is protected at all times. This memo shares our security protocols designed to safeguard your data and outlines our resilient hosting environment, strict access control and authentication mechanisms that reinforces our commitment to keeping high standards in data confidentiality and system integrity.

Hosting Environment Architecture

At CourtAlert, your data's security and confidentiality are of utmost importance. We've established a robust hosting environment architecture with Microsoft Azure's Platform as a Service (PaaS) to ensure comprehensive protection of your sensitive information. One prominent feature of this setup involves dedicating Microsoft Azure Resource Groups, including a unique Virtual Network (VNet), for each client. These prevent data intersection between clients, thereby strengthening data privacy and security by providing strict client data isolation. Each client's data is kept wholly separate from the data of other clients.

The system leverages only PaaS services for hosting, including dedicated Blob File Storage for data files, documents and attachments, client-dedicated Azure database for system data, and a dedicated WebApp instance for web access and data processing.

Data encryption is a central part of our security strategy. All communication between your devices and our services is encrypted using industry-standard encryption protocols like TLS/SSL. This protects your data while it's in transit and reduces the risk of interception. Your data stored, in blob file storage and the database, is also encrypted while at rest. Each client has a dedicated keystore and the data is encrypted with unique keys, ensuring that only authorized users can access and decrypt it.

Leveraging the Platform as a Service (PaaS) capabilities of Microsoft Azure, our instances automatically update servers, manage patches, and reinforce security, keeping up-to-date security measures at all times. With the responsibility of managing the underlying infrastructure — including server updates, patch management, and security hardening — entrusted to Microsoft's reliable hands, CourtAlert can focus on enhancing the security and functionality of our applications, aiming to deliver a consistently secure and reliable user experience.

Attached is an appendix to this memo which supplies a visual representation of our hosting environment architecture. Please consult CMECF Cloud Data Flow and Authentication Flow for further information.

Access Control and Authentication Mechanisms

At CourtAlert, we prioritize security while ensuring ease of access for our clients. Two crucial components contribute to our protective measures: Client Access, managed through Single Sign-On

(SSO) and Identity Provider (IdP) integration and CourtAlert Support Access, which is meticulously regulated via Privileged Identity Management (PIM).

The SSO integration allows you, the client, to quickly and securely access our system. For this to happen, we use what's called an Identity Provider or IdP, which could be the system your organization already uses, like Azure AD or Okta. When you request to use our service, your users log in to the familiar interface provided by your firm, with the Multifactor Authentication (MFA) requirements as your firm requires. You don't have to remember a separate password or username and CourtAlert doesn't need to store them. Once you log in, the IdP provides us with a token confirming your successful authentication and you can use our service.

In order to supply our exceptional support services, at times and only upon client request, CourtAlert may need to access the client environment. This is done strictly upon the request of the client, ensuring your control over your data at all times. This access enables us to help you effectively and efficiently, maintaining the quality of our services while keeping your data secure.

CourtAlert uses Privileged Identity Management (PIM) to regulate access for CourtAlert support. With PIM, our developers only gain access to the client-dedicated environment when needed, for a limited time and only after a request has been made and approved. This request process is meticulous, ensuring that all activities are documented and traceable. This tight control over access safeguards your data while ensuring we can supply the necessary technical support promptly and efficiently.

Here's how it works: when a developer needs access to your data, they log a request into the CourtAlert internal JIRA ticketing system, detailing the reasons for their need to access that client environment. The developer then submits the PIM request including the required ticket number. Next, a senior developer or a member of the management team reviews and approves the request. The developer is then granted access to that client-dedicated resources for a limited time. This approval system keeps a tight control over who can access your data and when.

CourtAlert sees itself as a data steward, caring for and protecting the data owned by you, our client. We strictly use Microsoft Azure to store your data, with all data being encrypted both during transit and while stored, which ensures confidentiality and protection of your sensitive information.

While we manage the Azure database that stores your data, we can only access this information under your express permission and only when necessary for tech or service support. This means that no one, not even us at CourtAlert, much less any third party, can access your data without your approval.

Furthermore, you remain in control of your data; the system allows for segregation of data with ethical walls, offering flexible access tailored to your firm's needs. Authorization within CourtAlert is role-based and decided on a case-by-case basis, ensuring each user only has access to data and features pertinent to their roles and responsibilities. This allows you to remain in control, setting the rules and boundaries for access within your organization.

Through our robust and meticulously planned access control and authentication mechanisms, we ensure the highest level of security, keeping a high level of data protection while enabling easy access for authorized users.

CourtAlert®

Proven Record of Trust and Reliability

CourtAlert recently passed SOC II Type I and Type II audits, a testament to our commitment to confidentiality and a reflection of the trust that our clients place with CourtAlert. The examination by an independent auditing firm, Laika Compliance, scrutinized our Case Monitoring Services and Case Management System, using an established set of criteria.

The auditing period covered several critical aspects of our service, including Security, Availability and Confidentiality. The auditors used a standard known as the Service Organization Control (SOC) 2 Type 2 test, which is recognized worldwide as a benchmark for technology and cloud-computing vendors. This evaluation has provided us with valuable insights into our security design and has helped ensure our system is robust and dependable.

The results of the audit were extremely positive, with no exceptions noted. The auditing firm assessed several key controls in our system to assess their effectiveness. These tests revolved around areas like user access to data, response to identified security incidents and the disposal of confidential information. The auditors have confirmed that our controls are suitably designed and are running effectively - providing assurance that our service commitments and system requirements are met.

The SOC 2 Type 2 report has confirmed the robustness of our system and the effectiveness of our controls. CourtAlert is dedicated to maintaining our high standards in system security and integrity and backing our commitment to our clients. We will continue to enhance and monitor our system, ensuring we remain a trusted provider.

For more information contact info@courtAlert.com

Yaniv Schiller
President

Eytan Schiller
Eytan Schiller (Jul 28, 2023 11:34 EDT)
Eytan Schiller
Chief Technology Officer

2023 - Cloud Security

Final Audit Report 2023-07-28

Created:	2023-07-28
By:	Yaniv Schiller (yschiller@courtalert.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAjwA2EPLhxVpIWSDe_5vhM9flLg-LciQq

"2023 - Cloud Security" History

Document created by Yaniv Schiller (yschiller@courtalert.com)
2023-07-28 - 2:37:02 PM GMT- IP address: 108.30.145.2

Document emailed to eschiller@courtalert.com for signature
2023-07-28 - 2:37:45 PM GMT

Email viewed by eschiller@courtalert.com
2023-07-28 - 3:34:10 PM GMT- IP address: 108.30.145.2

Signer eschiller@courtalert.com entered name at signing as Eytan Schiller
2023-07-28 - 3:34:36 PM GMT- IP address: 108.30.145.2

Document e-signed by Eytan Schiller (eschiller@courtalert.com)
Signature Date: 2023-07-28 - 3:34:38 PM GMT - Time Source: server- IP address: 108.30.145.2

Document emailed to Yaniv Schiller (yschiller@courtalert.com) for signature
2023-07-28 - 3:34:39 PM GMT

Email viewed by Yaniv Schiller (yschiller@courtalert.com)
2023-07-28 - 4:18:37 PM GMT- IP address: 108.30.145.2

Document e-signed by Yaniv Schiller (yschiller@courtalert.com)
Signature Date: 2023-07-28 - 4:18:56 PM GMT - Time Source: server- IP address: 108.30.145.2

Agreement completed.
2023-07-28 - 4:18:56 PM GMT