



Capturx Security Whitepaper

Summary

Capturx software helps teams of mobile workers easily collect and share digital data using pen and paper. In addition to faster workflows, Capturx also reduces the costs and risks of scanning, data re-entry, and misplaced documents. Handwritten data is directly integrated into leading software applications as native data without intermediate file types or applications. Teams can capture digital data in the field and leverage their existing file, network, and PC security. This white paper describes the different types and levels of security provided by Capturx software.

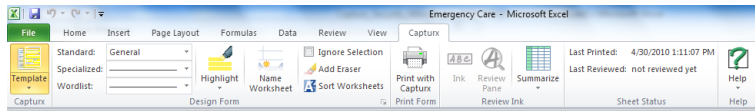
How Capturx Works

Capturx software enables teams to collect and integrate data into Microsoft Office, ArcGIS, PDF files, and SharePoint using digital pens and plain paper. Capturx works as an add-in to these applications enabling printed forms, maps, and PDF files to be marked up with digital pens which integrate the handwriting back into the original applications. Teams print forms, maps, and PDF files on ordinary paper. At the time of printing, Capturx software encodes a unique watermark which is a pattern of dots similar to a 2D barcode found on the back of many driver licenses. This dot pattern gets printed in the background of the page at the same time as the visual information for the form, map, or PDF file. That dot pattern is unique to each file, application, and print.

The digital pen has an infrared sensor which scans the barcode-like dot pattern as the pen writes. The pen records the handwriting and tracks the dot-pattern references. When the pen connects to a PC, Capturx software uses the dot-pattern references to identify the target files for the ink strokes. Capturx then creates the appropriate data structures – formatted data in OneNote, Excel, SharePoint, ArcGIS or PDF files – and inserts them into the original files or database.

Step 1. Encoding the paper

The Capturx add-ins allows teams to print specific files directly from native applications like Excel. This creates the unique, 2D barcode-like pattern of dots encoded by Capturx used to connect the data back to this file. An example of the printing tool in the Capturx toolbar for Excel is shown here.



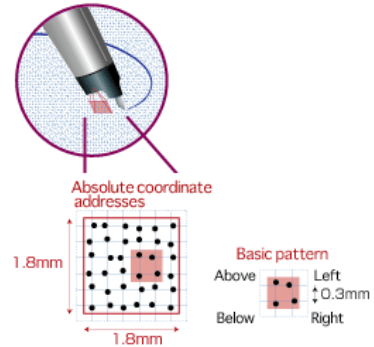
(In the case of Capturx for OneNote, teams are not printing existing files but using blank notebooks – either pre-printed or printed from OneNote. These dot-pattern references are handled slightly differently and will be explained further in section 6.)

Contents

- Summary..... 1
- How Capturx Works..... 1
- Capturx Security in Practice.. 3
- Capturx Security Methods..... 3
- Conclusion..... 7

Step 2. Writing with the digital pen

The digital pen has an infrared sensor which scans the dot pattern as the pen writes. The pen records the handwriting and tracks the dot-pattern references.



Step 3. Uploading data to PCs

The digital pen connects to the PC by USB, which also re-charges the digital pen's battery.

When connected to the PC, the Capturx Pen Manager software confirms the identity of the pen and that the data on the pen is destined for a file or application accessible by that PC.

If the file or application is accessible, Capturx transfers the ink to the PC, where it is either immediately processed or stored in an internal Capturx database awaiting action from the appropriate Capturx application.

Once the data is transferred from the pen to the source through pen manager, the original ink is erased from the pen.



Step 4. Integrating the ink into the Application

Capturx software then converts the ink into the appropriate data structures for the target application, whether it's OneNote, Excel, SharePoint, PDF, or ArcGIS.

Item	Units	Unit Price	Total
Trailer	1	100	100
FX Harness	3	200	600
R2 Turbine	2	300	600
Regulator	4	150	600
3X Valve	50	100	5000
Cylinders	2	200	400
Authorized Signature		Subtotal	7300
Barb Goldner		Tax	730
		Due	8030



	A	B	C	D	E
1	Item		Units	Unit Price	Total
2	Trailer		1	\$ 100.00	\$ 100.00
3	FX Harness		3	\$ 200.00	\$ 600.00
4	122 Turbine		2	\$ 300.00	\$ 600.00
5	Regulator		4	\$ 150.00	\$ 600.00
6	3 X Valve		50	\$ 100.00	\$5,000.00
7	Cylinders		2	\$ 200.00	\$ 400.00
8	Authorized Signature		Subtotal	\$7,300.00	
9	Barb Goldner		Tax	\$ 730.00	
10			Due	\$8,030.00	

Capturx Security in Practice

Capturx software is used in a range of scenarios requiring both data confidentiality and data integrity. While all customers rely on Capturx for security and data integrity, the examples below reflect some of the more demanding examples of Capturx in use.

US Army Certificate of Networthiness

Capturx software has received a Certificate of Networthiness (CoN) from the U.S. Army's Network Technology Command (NETCOM) for automating paper-based medical records within MedCom. The certification signifies successful completion of a stringent assessment to ensure that the Capturx software installed on U.S. Army computers are secure, supportable, sustainable, and compatible with the Army Enterprise Infrastructure's (AEI).

Regulatory Compliance (eg: HIPAA, FERC)

Capturx software is used in a range of processes with regulatory compliance requirements, such as HIPAA. Capturx software integrates data directly into native applications, file systems, and file formats – enabling IT teams to easily manage data and leverage their existing security, compliance, and auditing processes and investments. The pen simply stores ink strokes and references to the digital watermarks – the 2D-barcode-like pattern of dots. The ink strokes are only decoded when they are integrated into the original files using Capturx software. Capturx does not require any intermediate file formats, applications, or file storage not controlled by the IT team.

The PDF image files created by Capturx for SharePoint and Capturx Markup for PDF provide an extra level of data validation unique to digital pens. The date, time, and pen ID used for each ink stroke are tracked and embedded in these PDF files as permanent, read-only annotations. Tracking the actual time of the handwriting provides a more precise audit trail than what is available from scanners and manual data entry processes. Scanners track the later dates when documents were scanned. IT systems track the later dates when records were created by manual data re-entry.

Capturx and the Intelligence Community

Adapx is a strategic partner with In-Q-Tel, the independent strategic investment firm that identifies innovative technology solutions to support the missions of the Central Intelligence Agency (CIA) and the broader Intelligence Community (IC). "Every year, we review hundreds of innovative solutions but select only a small percentage with the superior capabilities that can best serve the critical technology needs of the U.S. Intelligence Community," said Troy M. Pearsall, Executive Vice President of Technology Practices and Insertion at In-Q-Tel. "Adapx technology dramatically improves the way in which organizations streamline field data collection and dissemination."

Capturx Security Methods

Capturx solutions include a range of data integrity and security methods:

1. Data Redundancy
2. Integrity for Data on Paper
3. Destroying Physical Paper Records
4. Secure Ink Storage on the Digital Pen
5. Password Protection for Digital Pens
6. Secure Ink Processing
7. Security for Capturx for SharePoint and Capturx Mobile
8. Integrity for Digital Data

1. Data Redundancy

Capturx automatically creates data redundancy, since two copies of data are simultaneously captured as the pen writes: physical ink on the printed page and copies of that ink on the digital pen. If the paper is lost, the digital pen retains the data. If the digital pen is lost, the data remains on paper.

2. Data Integrity on Paper

Capturx can also operate where the written data on paper might be at risk from harsh environmental conditions. Teams can use Capturx with all-weather Rite in the Rain paper to print forms and maps from office printers or in the Capturx field notebook. When used with water-proof ink in the digital pen, handwritten data will retain integrity and legibility. Capturx can also be used with laminated prints.

3. Destroying Physical Paper Records

In some cases, teams want to keep digital copies of data and have paper records destroyed for confidentiality. Capturx can be used with water soluble paper, which can be destroyed along with confidential notes, by using liquids in the field to help protect against the dissemination of confidential information.

4. Ink Storage on the Digital Pen

When the digital pen records written information, it is actually recording the ink strokes and the location of the ink strokes with respect to the dot pattern which was generated when the original file was printed. The position of the ink is identified as an offset from the upper left corner of a particular digital paper page. These pages are specified by a code that consists of four numbers similar in form to a standard IP address.

The pen has no information about the original file or the context of the ink strokes. The pen does not record any of the visual reference information on the printed page nor does it have any information or context about how Capturx will use ink strokes to create structured digital data, such as points, lines, polygons, words, or numbers. The ink is simply stored in page space coordinates. There is no indication of the overlying picture, map, or form on the page or of the type of application that will eventually consume the ink.

The Capturx software that encoded the original print uses a secure database to store the corresponding dot-pattern reference which acts as a key to decode the handwriting and apply it to the appropriate file and application. That Capturx software is installed on PCs or servers – not the pen – enabling IT teams to fully secure access to the key using their existing regimes for physical, network, and file security.

5. Password Protection for Digital Pens

Access to the ink stored on the digital pen may also be controlled by a user-specified password. This digital pen password is created and modified using the Capturx Pen Manager. Once a digital pen has been assigned a password, the Capturx software will not be able to read ink from the digital pen without the assigned password. The original password must be typed in order to change an assigned password or to connect a new digital pen to that Capturx Pen Manager installation.

The level of security afforded by password protection on the digital pen is comparable to the password protection provides for the user desktop or laptop computer. However, there is no administrative password for overriding this setting. If the password is not known, then accessing and using the pens will require hardware reset, which will erase both the password and all data stored on the pen.

6. Secure Ink Processing

In addition to providing digital pen management features, such as password management, the Capturx Pen Manager also controls how ink is taken off digital pen and how data is uploaded into the proper Capturx application.

When connected to a digital pen containing ink for uploading, Capturx Pen Manager identifies the dot-pattern references for the ink to determine whether to process the ink or leave it on the pen.

Capturx Pen Manager will:

- Process any ink destined for OneNote directly, if Capturx for OneNote is installed
- Query the local secure Capturx database to determine whether the dot-pattern references correspond to Excel, PDF or ArcGIS files registered to that PC and that user.
- Query any SharePoint sites registered with Pen Manager to determine whether any dot-pattern references correspond to forms solutions on SharePoint.
- Leave ink for unregistered pages on the pen

6.1 Ink for Unrecognized Pages

In some cases, Capturx Pen Manager will query pens and find pages whose dot-pattern references are not registered with OneNote, the local or SharePoint Capturx databases. Capturx will then provide the option to view the ink by itself or to leave the corresponding ink on the digital pen. Since the Capturx Pen Manager does not assign semantics to the ink and cannot interpret any ink strokes, if view ink is selected, then the ink will appear without any conversion or context. To prevent unauthorized viewing of ink, we strongly suggest the use of a pen password. If the pen is password protected, then no ink can be viewed or uploaded without knowing the password.

6.2 Ink Forwarding

With Capturx Pen Manager and Capturx Mobile, teams can send ink files via email as attachments. Capturx creates a file with the .XID extension. This extension is registered with the Capturx Pen Manager. When the file is opened, Capturx Pen Manager opens and processes the ink in the same way that it processes ink from a docked pen. Pen Manager queries the local and/or SharePoint Capturx databases to confirm the presence of the dot-pattern references. If the ink is not registered with OneNote, the local or SharePoint Capturx databases, then Capturx Pen Manager will provide the option to view the ink. Since the Capturx Pen Manager does not assign semantics to the ink and cannot interpret any ink strokes, if view ink is selected, then the ink will appear without any conversion or context. As above, to prevent unauthorized viewing of ink, we strongly suggest the use of a pen password. If the pen is password protected, .XID files cannot be created, viewed or uploaded without knowing the password.

6.3 Capturx for OneNote Ink Processing

Capturx for OneNote is the only Capturx application that uses a common set of pre-defined dot-pattern references, in this case for notebooks. Each installation of Capturx for OneNote contains the same set of several hundred pages of dot-pattern pages. Each page within the set has a unique dot pattern, which enables Capturx to distinctly track pages within individual notebooks – whether they are pre-printed Capturx notebooks or notebooks printed from OneNote.

When the pages are filled, teams can simply purchase or print new paper notebooks and associate them with new digital notebooks in OneNote. The dot-pattern references are re-used, but Capturx puts all new written notes into the new digital notebooks. This common set of dot patterns makes it easy for people to use off-the-shelf pre-printed notebooks.

When a digital pen with OneNote ink is docked to a PC, the Capturx Pen Manager downloads the ink, starts Capturx for OneNote, and hands the ink to the application through the Capturx “bridge.” The bridge transforms the digital ink into OneNote ink or other OneNote objects. The ink is not stored until it is handed to OneNote, where it is immediately transformed into native OneNote file data– which inherit the same security which protect the native file itself.

To prevent handwritten data on one person’s pen from being inadvertently uploaded into a OneNote notebook on a different person’s PC in shared workgroup scenarios, we recommend that teams use pen password protection in Capturx Pen Manager. In that case, only the password holder of the pen will be able to download data written with that pen.

6.4 Ink Processing for Capturx Ink Database Applications

In the case of Capturx Forms for Excel, PDF, and ArcGIS, Capturx does not automatically open the target application and integrate the data. When ink for one of these applications is transferred, the Capturx service determines which Capturx application will process the ink based on the original dot-pattern references stored and tracked by Capturx. That ink is added to the Capturx ink database until the processing application is started. This database is secured, and can only be accessed using a private Capturx password. Since the data is stored as digital ink using pattern space coordinates, the actual application semantics are not assigned to the ink until it is removed from the database for processing.

7. Security for Capturx for SharePoint and Capturx Mobile

With Capturx for SharePoint, data is integrated into servers either deployed on the customer's premises or managed as a software service by the Adapx team. Forms are printed from Capturx for SharePoint software that encodes the printed pages with the unique dot-pattern references. The references for those printed pages are retained solely on the server. After writing, ink records are sent to a server either by the Capturx Pen Manager software installed on a PC or by Capturx Mobile software on a mobile device. When data is being transferred from the pen, Capturx software queries the server for the page references to determine whether the ink belongs on the SharePoint server.

7.1 Secure server access

The Capturx for SharePoint software is built on top of Microsoft SharePoint Services, which itself is built on top of Microsoft SQL Server and Microsoft Windows Server 2008 R2. Capturx creates native data in SharePoint, stored in the underlying SQL database and accessible in SharePoint.

Access to the server is controlled by standard SharePoint authentication through user names and passwords. Capturx works with all the standard SharePoint rights and permissions managed by IT teams in SharePoint or through Active Directory. The SharePoint sites can be configured to require password authentication for printing blank forms, viewing data, and uploading data. If a device is lost or employee departs the organization, then access can be immediately controlled by IT's changing of the password.

7.2 Secure password management

Before printing, viewing data, or uploading data, SharePoint can be configured to require user names and passwords. For both Capturx Pen Manager and Capturx Mobile, the user names and passwords are stored in the encrypted credentials services provided by the respective PC and device operating systems. Windows users can opt to have credentials cached or to be prompted with each access.

7.3 Capturx Pen Manager controls

As described above, access to Capturx Pen Manager for downloading ink on a PC can be controlled by a pen password. Even if a pen password is not enabled, the Capturx Pen Manager can be configured to require a user prompt before any data is uploaded. If the Windows PC is locked and the pen is docked, Pen Manager will not take any data off the pen. By using standard Windows best practices for log-on and access, teams can prevent unauthorized PC access and data downloads by Capturx.

Mobile device users have a parallel set of options for controlling access to their devices. Bluetooth can be configured to require user confirmation for each upload attempt with a digital pen. Users can control access to their device to manage that data connection using standard password protection for locking devices. Without the password, the handset can be configured to be inaccessible- preventing any ink downloading and processing.

7.4 Encrypted connections

The Capturx for SharePoint Service uses 128-bit SSL encryption to secure the data connection between the Capturx clients and the SharePoint Server. This is the same encryption standard which is used to secure most consumer banking and credit card transactions over the internet. Capturx for SharePoint can also be configured for use within a corporate network with VPN access, where the data is never transmitted over the internet. When deployed on premises, Capturx can be used with a range of security procedures and third-part security applications for SharePoint.

7.5 Capturx for SharePoint Service secure hosting

The Capturx for SharePoint Service is hosted at a SAS 70 Type II Certified Facility, with secure physical access, off-site data redundancy, and premium hardware and network infrastructure.

8. Digital Data Integrity

Capturx takes a number of steps to preserve the integrity of digital copies of the handwritten data and to provide validation of the date, time, and source of the original handwriting. When handwritten data is uploaded into PDF files, Excel files or SharePoint, Capturx tracks the date, time, Pen ID, and associated pen owner for each ink stroke. Managers can see the actual date and time of when the information was written in each field for Excel- and SharePoint-based forms or on PDF files.

To determine the precise time of the ink strokes, the digital pen uses an offset between its clock and the local clock on the PC or device running the Capturx software used to process the data. Capturx provides no way to change the time on the digital pens. IT administrators can use standard tools to lock down access to time changes on their PCs and devices to prevent tampering. Once the files are processed by Capturx and uploaded into their native files, all the ink-stroke time references associated with files are tracked as universal times.

If paper documents were written on or edited at different periods of time, Capturx will track all the original handwriting including the different dates and times for each field (Excel, SharePoint) or ink stroke (PDF).

The original handwriting in SharePoint and in PDF files becomes read only and cannot be edited. The handwriting in Excel files is also read only: it can never be permanently altered.

Managers can also configure Capturx Mobile for BlackBerry to send GPS coordinates to associate specific forms with the locations from where they were sent. That GPS data is available in SharePoint. Access to that information for viewing or editing can be controlled using standard SharePoint permissions.

While Capturx software can create the equivalent of scanned copies, unlike scanned PDF files, Capturx can also enable the tracking of metadata showing the date, time, and source of each stroke of ink on the actual paper.

Conclusion

The Capturx product philosophy of integrating seamlessly into existing workflows and applications also applies to security. By integrating into existing applications, file formats, and creating native data structures, Capturx enables IT teams to fully leverage their existing data security and integrity investments and processes. At all points in the Capturx process, from encoding the paper to decoding the handwriting, data is at least as well protected as it would be on PCs or mobile devices with password protection for its user accounts. In many other cases, Capturx offers additional data integrity and redundancy options.