VIDEONETICS

the future of video computing

Cybersecurity

Our Philosophy

At Videonetics, we place cybersecurity at the forefront of our innovations and strive to keep your operations protected from cyber threats. Videonetics recognizes the sensitivity associated with data, particularly video data, and is committed to keep the data secured, both at rest and while in movementand also protect your assets.

Numerous strategies are adopted at every stage of the systemsarchitecture design, encompassing secured communications between various components in the system.

Not just that, at Videonetics, we ensure to keep our customers up to date with recent advisories and mitigate risk exposure through software updates as soon as possible, provided the product is still supported.

Broadly, all our efforts towards ensuring a cyber resilient product & deployment are guided by 4 objectives.

Operational Endurance

There can be no exception to any vulnerability. Customer's operations must endure and withstand any cyber threat.

Secure Development

Our Products are designed to be more cyber-resilient and tested with benchmark techniques.

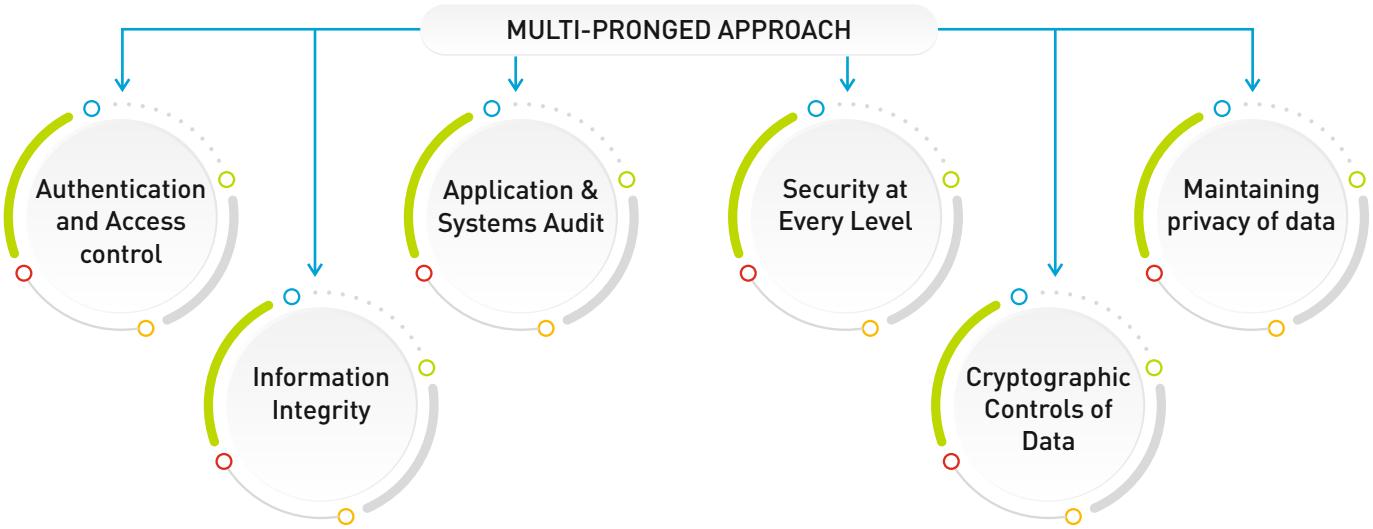
Secure Deployment

Our experts guide customers in best practices of solution design and deployment and ensure data security is at forefront.

Rapid Response

Quickly assess new threats or vulnerabilities and advise customer on how to reduce their cybersecurity risk.

Our Architectural Design Strategies



1 Authentication and Access control

Three levels of Authentication and Access control mechanisms are used in our applications, over and above Username-Password based login.

a) ***Role based authentication:*** The users are categorized into 5 categories. Number of user categories can be increased or decreased. Major functionalities of the system are also categorized into several buckets. The administrator can establish a mapping between user category and functionality buckets. Depending on this mapping established by the administrator of the system, the authorized users are allowed to access the system for various services like live viewing, configuration of the system, Video clip downloading, Receiving Event notification, etc. as permitted by the administrator for that user category.

b) ***Session control using encrypted tokens:*** User login sessions are maintained and continuously monitored within the system. The system generates an 'encrypted token' against each user login. Each request from client workstation to the server is accompanied with the encrypted token. The token is changed dynamically & continuously to prevent relay attack and hence safe from related security threats.

c) ***User stickiness to machine:*** Each user can be tagged to a particular terminal, thereby barring him to login from any other terminals. Additionally, the system supports Google sign in, and single sign-on based on LDAP/Active directory. This way, authorized administrator permits users to access only designated terminals. All the activities performed by the users are logged as part of systems health monitoring.

2 Information Integrity

There are two categories of information that is stored in the system.

a) ***System configuration data:*** System configuration data: This includes system configuration, user credentials, audit logs, system logs, etc. Data are kept in encrypted files with checksum. Users can select the encryption algorithms (MD5 or sha256) for such encryption. Two copies of each file are maintained in the system.

b) ***User data:*** These are event metadata, images, and videos. The data is stored in proprietary formats and are encrypted at rest; they are converted to standard format by the presentation layer of the software while displaying the information on terminals or while generating reports. Downloaded videos are watermarked and can be encrypted with user given key. The watermark authenticates theoriginality of a video and ensures that there is no tampering.

3 Application & Systems Audit

The system automatically maintains audit trails of user interaction in system files (bypassing DBMS). All the activities of users are automatically loggedin system files that can be searched any time by authorized personnel for any interactions by its users or to investigate system failures or behaviors.

Our Software comes with system audit tools that are installed in every server along with the application software. The tool generates a report depicting health of network connectivity andthe throughput of storage devices against each server, thereby providing an overall health status of infrastructure. Users can generate and store the report periodically and compare them to check whether the performance of the hardware backbone is deteriorating or not, thus providing information on possible outrages in the system, including DDOS attracts.

Additionally, the system automatically generates reports with numerous statistics such as uptime of individual cameras, recording continuity, health status of each component, etc. which is useful while carrying out preventive maintenance tasks.

a) ***Application Layer:*** Our software deploys very strict access control and authentication mechanisms to prevent unwanted access to the system. Additionally, the data exchange between any two servers and between server and client terminals takes place over secured and encrypted channels (TLS 1.3).

b) ***Database Layer:*** Videonetics applications allows database access through a custom-built database manager software component that ensures session control and authenticated access. The database password is changed periodically, and the password can only be deciphered through a separate maintenance software application.

c) ***Workstation Layer:*** Workstations can be locked to users so that the system is inaccessible by any arbitrary client terminal/workstation. This mechanism holds good also for accessing the system over Cell phones apps. The system displays active login sessions to monitor users currently logged in at any point of time, and the administrator has the privilege to bar any user from accessing the system at any point of time.

All communications between workstations and the server are carried out over secure communication channel and a strict session control is in place in the system.

Operator screen of any workstation can be imported in the dashboard panel to check the activity of any operator who is logged in.

d) ***Server Layer:*** The servers are partitioned between militarized and demilitarized zones for inter-server and out-bound communications respectively. Separate VLANs are created, and inter-server accessibility is established using inter-VLAN routing.

Videonetics software and related products are OS agnostic and do not use any OS-intrinsic features, thus providing an additional layer of server security bypassing inclusive security threats and vulnerabilities compared to any other system which may be inherently dependent on a particular OS and its intrinsic features by virtue of its design. This significantly reduces cybersecurity threats and makes it difficult by the hackers to enter the system through known OS vulnerabilities.

5 Cryptographic Controls of Data

Data is encrypted with either MD5 or SHA256 cryptographic hash functions, and video data are stored in proprietary format when at rest. The video data is also watermarked and can be checked for tampering. Data are transferred between various computing nodes including between Server and Workstation over Secured encrypted channels (TLS 1.3).

The software can be customized to incorporate country specific Cryptography control measures, e.g., Personal Data Protection acts, etc.

6 Maintaining Privacy of Data

In accordance with General Data Protection Regulation (GDPR), the system can be configured to mask personal attributes of people captured in an image/Video, depending on the requirement. Faces and License plates of the vehicles can be masked while displaying video/image, as for example, to protect identity in public.

Additionally, attributes of peoples and vehicles as extracted by the System is also kept in encrypted vectorized form, and they cannot be used by any third party software for identification of those objects.

Our Products are Certified

At Videonetics, we adopt a holistic methodology which has been the principal mindset that guides our cybersecurity practices during the three main lifecycle phases of our products: Development, Deployment and Rapid Response to cyber incidents.

For our customers' peace of mind and assurance, we embark to get our products tested rigorously and certified for various data security parameters, regularly. Certifications and approvals only reiterate our concentrated and no-compromise cyber security program.

VIDEONETICS
the future of video computing

Write to us at
marcom@videonetics.com
W: www.videonetics.com