NOVARAD®
ENTERPRISE HEALTHCARE SOLUTIONS

SECURITY INFORMATION

OpEyes

Novarad Security Information for OpEyes Customers

Novarad uses a proprietary system called NCC (Novarad Central Control) to manage systems and control passwords. NCC regularly and automatically changes the passwords for the accounts that Novarad employees use to access the machines hosting the Novarad software and customer data.

What user account are needed by Novarad?

- 2 accounts for windows services to run. The passwords are 55 characters, very complex and don't change
- NrService (admin privilege)
- NrDbService (non-admin)
- 2 accounts for support personnel to login. The passwords are 12 characters, very complex and change every 3 days.
- NrAdmin (admin privilege + database access for escalation-level support – 55 characters)
- NrSupport (admin privilege – 12 characters)
- All the passwords contain upper, lower, numbers and symbols

How are security-related events (e.g. SIEM, HIDS/HIPS, vulnerability scanning) monitored within the hosting environment?

- Novarad utilizes Cisco FP to monitor for security-related events at its data centers.
- Novarad employs an outside contractor, Security Metrics, to further monitor and test for vulnerabilities.
- If the customer is hosting Novarad equipment at its facilities, it is advised to employ a similar system.

What kind of logs are maintained, who accesses them and how, and what is the log retention policy?

- Windows Events are generally configured to 16,384K (rotational.)
  - Events are access through traditional means (Windows Event Viewer).
- Novarad events are stored in its database and are divided into two categories: System events and Audit (Data Access) events.
  - System events are quite verbose and as such are generally configured to be kept for three days on a rotational basis.
  - Audit events are generally configured to be kept forever. The main purpose is to show when data exits the Novarad system.
- Novarad events may be accessed through the Administration Consoles provided with the Novarad software.

What is Novarad's policy for updating Windows?

- By default, Novarad configures its systems to apply security patches automatically in the early morning hours as they become available. If the customer desires to be more involved, this is welcomed, and a new policy may be negotiated, provided the customer is willing and able to take on the responsibility of applying the patches in a timely manner.

What is the policy for updating Novarad software?

- Novarad software updates are generally created monthly. High priority updates, including fixes for security issues, are distributed automatically. Customers are notified before receiving updates to customer-facing (non-management) software. Other updates are pushed out on a case-by-case basis if new features or bug fixes are relevant for the customer.

What is Novarad's policy regarding anti-malware software?

- By default, Novarad provides Windows Defender (or equivalent for legacy customers) and configures it to automatically, monitoring for active threats and regularly scanning the system for, and quarantining malware-related files.

  If the customer wishes to provide their own anti-malware solution this is welcomed, and a new policy may be negotiated. This policy would require that the customer apply Novarad's list of file/folder exemptions and keeps the anti-malware software up to date.

What data at rest encryption technology is used for system disk media and/or databases?

- Each object (Image File) is encrypted with AES-256 encryption

Please describe your encryption key management approach:

1. Is a specific key management solution used?
   - Software embedded
   - Novarad issues its own keys.
   - Keys are used for encryption, authentication, and secure communication.
   - Keys are distributed through our NCC server. The keys are changed yearly. The keys are stored encrypted on the NCC server.
   - There are a number of special keys that have a higher level security: (root key, ca key, and encryption recovery key). These are not stored on any active computer. They reside on a thumb drive held by a company executive and are encrypted with a password in possession by another executive. There is another thumb drive and another pair of executives setup the same way for redundancy.

2. How often are keys rotated?
   - Annually

3. Who has access to the keys and how is access reviewed, and at what frequency?
   - 4 Novarad employees reviewed annually at shareholder meeting
     - 2 Corporate Officers hold part 1 of key
     - 1 IT Director and 1 Development Director hold part 2 of the key
   - An Officer and a Director must both provide their key to utilize

Are the movements recorded of hardware and electronic media associated with Novarad systems that store CUSTOMER data?

- Yes, and none anticipated

Regarding the Novarad PACS and OpEyes software, how is authentication accomplished?

1. Can authentication be accomplished using CUSTOMER's Active directory system (via LDAP, SAML, etc.)?
2. What is the minimum length and complexity requirements for passwords?
3. Are password changes require at a specific interval?
4. Are user accounts either disabled or locked for a period of time after a predetermined number of failed logon attempts? If so, please provide those details.
5. How are passwords stored by the application? Please provide specific on hashing or encryption algorithms.

- CUSTOMER Domain / policy

Regarding the same applications/software:

1. How does the system maintain user session state? (E.g. Cookie/Token based.)
   - Token is used, passed in http headers
2. If cookies are used, are both the HTTPOnly and Secure flags attributed to them?
   - When cookies are used both HTTPOnly and Secure are set
3. Are session IDs randomly generated and of sufficient length to protect against brute force attacks?
   - Session IDs are randomly generated UUID (128-bit ver.4 bits are entirely random)
4. Are user sessions terminated after a period of inactivity?
   - Yes, 15 min.

What are the user types that can be assigned in the applications?

- There is only one user type in OpEyes at the present.

Regarding common application vulnerabilities, how does the application protect against the following:

1. Cross-Site Request Forgery (CSRF)
   - MVC AntiForgeryToken helper
2. Cross-Site Scripting (XSS)
   - MVC AntiXssEncoder
3. SQL Injection
   - Database access is done through Entity Framework. All input is done with parameterized queries.

Can you please expand on what kind secure development training the developers go through?

- We do OWASP training yearly. OWASP ZAP scanning is regularly run on our web applications.
- Novarad's data center is regularly penetration tested for security weakness by the independent testing firm Security Metrics.

How does Novarad maintain HIPAA compliance?

- Novarad performs risk analysis on an as needed basis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information for which we have access.
- Novarad performs HIPAA training for each new employee as well as periodic training for all other members of our workforce.
- PHI is processed, stored or transferred in accordance with HIPAA regulations.

Novarad Data center PHYSICAL SECURITY

- On-site security and support personnel 24x7x365
- Monitored security cameras and intercom system
- Full perimeter fence with secured parking
- Concrete wall surrounding the mechanical/electrical equipment yard
- Dual-factor authentication (key card access w/secondary biometric) on exterior entry and all data center halls
- Camera surveillance on all ingress/egress points and critical areas
- Video with access log retention for 90 days
- Custom physical security controls available for customer deployments
- Power delivery, generator and diesel fuel infrastructure maintained in secured areas

Who ultimately would have management control over the HoloLens devices?

- CUSTOMER Domain / policy

Are the HoloLens limited in functionality? As opposed to how they can function outside of this 3D augmented reality workflow.

- No limited functionality, they use a MS OS and can be loaded with additional software as required as long as the additional software does not conflict with OpEyes

Taking in to consideration that the HoloLens devices run on Windows 10, can they be tied to the CUSTOMER domain to receive Windows updates?

- CUSTOMER Domain / policy

Is there authentication to the HoloLens devices? Can unique IDs be provisioned?

- CUSTOMER Domain / policy

Can the HoloLens devices be plugged into a computer to allow users to view the files stored by it and potentially export if off of it?

- HoloLens does not support physical connectivity to other workstations, however files and content may be shared similar to the methodology used in traditional workstations
- Cloud drives (OneDrive, Dropbox, etc.)

Regarding the DICOM Receiver appliance, can it be tied to the CUSTOMER domain and configured to use CUSTOMER AD, have our AV installed, and receive regular security updates as part of our schedule?

- CUSTOMER Domain / policy

Can the hard drive be encrypted with BitLocker?

- Yes

Can IP based restrictions be put in place so that VM endpoint hosted by Novarad can only be accessed from the CUSTOMER network?

- Yes