Protecting EPIC Systems via ColorTokens Zero Trust Microsegmentation

Healthcare providers are in the business of delivering patient care, so dealing with protecting digital data, as well, can be overwhelming. So, given the rise of cyberattacks on healthcare organizations, it is now more important than ever to ensure that electronic health records (EHRs), electronic medical records (EMRs) and patient data (PHI, PII) are protected against unauthorized access or harmful activity. Today, many healthcare organizations have turned to the Epic system for their digital records management.

In order to protect an Epic system against cyberattacks, including ransomware, hospitals and healthcare organizations increasingly are looking to zero trust microsegmentation to reduce the impact of an attack and prevent lateral movement of malicious software or bad actors within their networked IT infrastructure. This includes segmenting Epic modules and application servers, cache databases, and workloads, as well as ancillary systems, into smaller, protected groups organized systematically by role, function, location, and many other attributes.

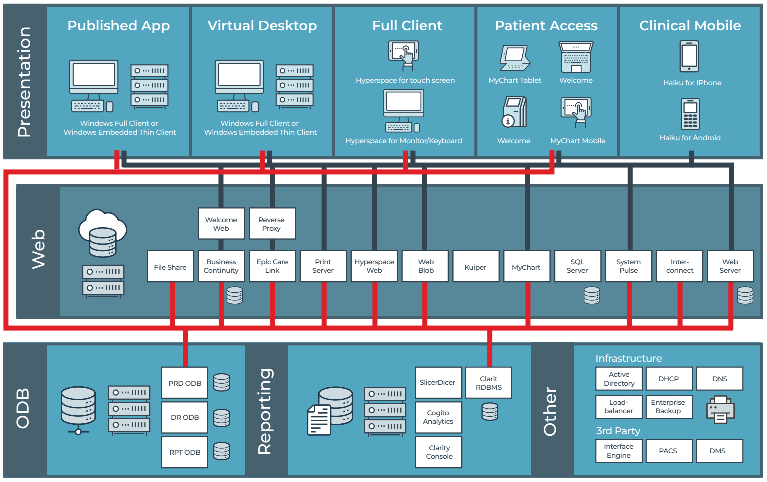
An approach that leverages experience and technology

Having worked over the years with numerous hospitals and healthcare organizations around the world, ColorTokens has developed a significant understanding of the Epic environment and how to protect it.

ColorTokens looks at the customer's Epic architecture in three "layers:"

- A user/mobile layer where users are trying to access the applications from various remote/external locations, for example via Haiko/Canto from mobile devices or MyChart from Citrix or VDI.
- A module layer consisting of Epic modules, such as Epic print, interconnect, blob storage, PCA and hyperspace services that make up the various Epic applications that are accessed by departments within the hospital.
- And third, we look at ancillary systems and the relevant departments connecting into the Epic system, such as PACS and perhaps radiology, lab or pharmacy systems if the Epic option isn't used. These ancillary systems are either the hospital's partner organizations, for which there might be inherited risk, or internal hospital applications that are interfacing with Epic. However, today there may be no way of placing agents on the devices to enable protection, so instead, ancillary systems interface with Epic via Epic Bridge Interfaces only, so access can be restricted utilizing these strategic interfaces.

At each layer, whether it be the user/mobile, the modules, the ancillaries, or the back-end cache storage, ColorTokens zero-trust platform and implementation methodology essentially does two things: 1) we restrict access to only those port protocols, users, and IPs that are supposed to be connecting to it, and 2) when they do connect to it, ColorTokens ensures that a particular layer only connects with and talks to the relevant layer that it is supposed to be communicating with, and doesn't have the ability to connect to another layer that's not approved.



Epic Cache: safeguarding the “crown jewels”

Of course, at the heart of every Epic system is the cache storage databases that underpin all these applications, and which need to be locked down and protected, such that only connectivity from the relevant environments is allowed to connect to them – ex., Epic interconnect, hyperspace, Welcome web kiosk, and others. Microsegmentation of the Epic environment ensures that critical components like the cache are secured against connectivity and attack from any unapproved vector, and the only communication to or originating from the cache is approved traffic from those assets that specifically require it.

Because, for example, if a bad actor were to get in and take hold of primary storage, the impact would be severe, because it contains all of the patient records. It’s essentially the root upon which everything is built. Therefore, it’s necessary to ring fence and protect these such that you’re ensuring it is only getting connectivity from the relevant cache DBs and the relevant environments that are accessing the primary storage.

We’re not only ensuring that whatever is coming in from the web application is only coming in and executing the appropriate port protocol commands, but we’re also ensuring that they don’t have free reign within the environment. They can only see and connect to the modules and units that we enable them to have exposure to, and that are in line with the architecture. They cannot, for instance, jump from a Citrix server to a storage server or to a cache DB.

ColorTokens enables flexible, redundant Epic security management

In many cases, we have seen the Epic application spanning multiple data centers in order to achieve high availability and redundancy, and to allow testing and deployment activities. In these instances, we allow security policies to be tested safely outside of the production environment, and we allow independent protection schemes for each of the high availability instances. This enables an easy migration of a live application from one data center to the other, while still allowing a higher level of protection for disaster recovery instances.

In this case, flexibility and control is made easy because the customer can do enforcement instance-by-instance and ensure stability of the system before moving on to the next instance. With this approach, effective backup of the system is achieved, and the deployment is made even easier because they can replicate what they’ve used in one instance and move that enforcement policy directly across to the next instance. With this “build once, use many” type of environment, the customer doesn’t have to rebuild the entire policy each time.

ColorTokens delivers Epic Systems microsegmentation in less than 12 weeks

ColorTokens uses five phases for implementing zero-trust security around the healthcare provider's Epic system, which in most cases can be achieved in 8-12 weeks:

STAGE 1

Discovery: collecting and consolidating information about all the critical systems and devices that communicate into and out of the Epic system; which servers belong to which modules, who owns them; also critical during this stage is to identify all ancillary systems, lab information systems, pharmacy management systems, and other external systems that need to communicate with Epic. ColorTokens works closely with the customer by providing guidance and templates to ensure all critical systems and devices are assembled and for ColorTokens to fully understand the IT infrastructure.

Derived Benefits from Stage 1:

- Identify critical/high vulnerabilities (CVE scores of 7.0-10.0)
- Identify unknown network subnets (blind spots) in the IT infrastructure
- Discover suspicious communications with bad reputation IP/domains
- Gain visibility of the communication occuring with public IP/domains

STAGE 2

Identification/Tagging: labeling and grouping the servers and devices into logical application groups or modules; with unlimited tags, ColorTokens provides the customer with a deep level of granularity and visibility into its interconnected Epic environment.

Derived Benefits from Stage 2:

- Gain visibility of network traffic between different applications
- Gain visibility into applications communicating with different entities in the network

STAGE 3

Observation Period: learning what communication traffic is happening among the modules, from module-to-module, inter-module and intra-module, and traffic patterns into and out of the Epic system; this process entails monitoring, recording, and gathering detailed knowledge of how the overall system is operating, and requires a minimum of time to build an accurate, comprehensive flow model.

Derived Benefits from Stage 3:

- Discover attack surface, ie., attackers' ability to compromise business applications
- Discover blast radius, ie., attackers' ability to laterally move within the network to other networks, applications, and segments

STAGE 4

Policy Recommendations/Creation: creating policies automatically via ColorTokens policy recommendation engine, based on traffic observations and corporate requirements; ColorTokens assists the customer by providing policy deployment guidance and templates. Once policies are developed, they can be easily duplicated and modified.

Derived Benefits from Stage 4:

- Gain visibility into unauthorized traffic, after creating policies; knowing any unauthorized traffic is the first step towards securing the application
- Measure the reduction (improvement) in the attack surface
- Measure the reduction (improvement) of the impacted blast radius

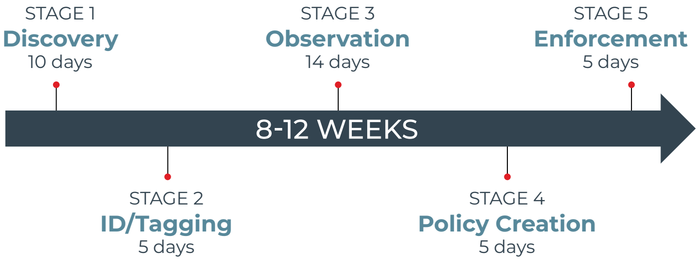
STAGE 5

Policy Enforcement: deploying policies across the Epic modules to begin enforcement and achieving optimal security.

Derived Benefit from Stage 5:

- Achieve optimal defensive posture by blocking all unauthorized traffic; applications are secure from all unknown network traffic

Timeline for ColorTokens Epic Security Implementation



Get started protecting your Epic system with microsegmentation from ColorTokens

By implementing robust security measures like microsegmentation for Epic systems, healthcare providers can keep digital health and medical records and patient data secure from potential cyberattacks, and address critical HIPAA compliance requirements — and ColorTokens can show you how. Protecting this data helps to ensure patient safety and reduces the risk of breaches caused by malicious actors looking to exploit weaknesses in an organization's systems. It is important for healthcare providers to remain vigilant in protecting their digital data stores and take pro-active measures to protect patient data.

ColorTokens' Unified Zero Trust Security Platform delivers a simplified approach to protecting a healthcare organization's critical Epic systems and its most valuable network assets, endpoints, and critical sensitive information, such as ePHI, PII, and EHRs.

To learn more about ColorTokens and our microsegmentation solution, visit us at colortokens.com or contact us at **sales@colortokens.com.**

About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning cyber security solutions. It is a US corporation headquartered in Silicon Valley with offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to **colortokens.com**