



## FairWarning<sup>®</sup> Privacy Auditing & Enterprise Security FairWarning<sup>®</sup> Ready for Enterprise Security Certified Program

Healthcare organizations are deploying FairWarning<sup>®</sup>'s proven, out-of-the-box [privacy monitoring solution](#) for clinical applications and systems because it is the foundation for a culture of privacy, and core to regulatory compliance. These organizations are increasingly leveraging FairWarning<sup>®</sup>'s privacy monitoring results into their Enterprise Security deployments to perform a security deep dive on privacy incidents.

### Overview

**Privacy, security and compliance.** With an increase of highly-publicized patient privacy incidents, the passage of the [ARRA-HITECH bill with strengthened HIPAA enforcement](#) provisions, as well as new state privacy laws, healthcare organizations have come face-to-face with a series of challenges related to 1) privacy, 2) security and 3) multiple forms of regulatory compliance.

FairWarning<sup>®</sup> [customers](#) have chosen to prioritize the monitoring and auditing of their [clinical systems](#) because these applications are at the core of patient privacy and regulatory challenges. Some FairWarning<sup>®</sup> customers as well as other healthcare organizations have acquired or are planning to acquire an Enterprise Security solution such as SIEM and DLP. Healthcare organizations are seeking the benefits of both FairWarning<sup>®</sup> [privacy monitoring](#) and Enterprise Security solutions while minimizing the complexity of their environments.

This paper outlines how FairWarning<sup>®</sup> privacy monitoring complements Enterprise Security solutions which are FairWarning<sup>®</sup> Ready for Enterprise Security Certified and, based on a customer-driven model, outlines how both technologies seamlessly operate together.

***Leading Enterprise Security vendors support the FairWarning<sup>®</sup> Ready for Enterprise Security program and are delivering on a combined privacy monitoring and Enterprise Security solution. Contact FairWarning<sup>®</sup> for more information on a combined solution by sending an email to: [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com)***

#### **FairWarning, Inc.**

Email: [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

Phone: 727 576 6700 x115



## FairWarning® Privacy Monitoring and Enterprise Security Comparison

FairWarning®'s patents-pending [privacy monitoring solution](#) for healthcare applications is highly specialized and focused on patient privacy incident investigations, proactively detecting privacy incidents and generally providing healthcare privacy and compliance personnel the right tool for their job. Enterprise Security solutions such as SIEM and DLP are also highly specialized and are targeted at infrastructure monitoring. These solutions are used by trained, certified information security professionals. A comparison between FairWarning® privacy monitoring, SIEM and DLP is provided below:

	FairWarning® Privacy Monitoring	SIEM	DLP
<b>Threats Defense</b>	<ul style="list-style-type: none"> <li>• <a href="#">Clinical application</a> layer focus</li> <li>• Internal threat focus - authorized user misuses of electronic health records (employee, partners, contractors). Medical record snooping, internal identity theft, internal medical identity theft</li> <li>• Privacy driven non-compliance with HIPAA, ARRA-HITECH, state-provincial patient privacy laws, UK-EU privacy and security laws</li> </ul>	<ul style="list-style-type: none"> <li>• Infrastructure layer focus</li> <li>• Wide range of external threats. Internal threats related to infrastructure layer (viruses, worms, Trojan horses, etc)</li> <li>• Security driven non-compliance with a wide-range of Federal, state-provincial and international laws</li> </ul>	<ul style="list-style-type: none"> <li>• Data focused.</li> <li>• Protects data in stored devices, network and on individual endpoints i.e. data at a lower level.</li> <li>• General security and compliance requirements such as PCI.</li> </ul>
<b>Primary Users</b>	<ul style="list-style-type: none"> <li>• Privacy Officers, managers, compliance and other business users. Information security in some organizations</li> </ul>	<ul style="list-style-type: none"> <li>• Information security professionals</li> </ul>	<ul style="list-style-type: none"> <li>• Privacy Officers</li> </ul>
<b>User Interface</b>	<ul style="list-style-type: none"> <li>• Web-based, point-and-click appropriate for Privacy Officers and other business related users</li> <li>• Healthcare-rich interface based on users, patients, treatment-function codes, physical patient &amp; user locations as well as other care-related information.</li> </ul>	<ul style="list-style-type: none"> <li>• Sophisticated user interface appropriate for information security personnel</li> </ul>	<ul style="list-style-type: none"> <li>• Sophisticated user interface appropriate for information security personnel</li> </ul>
<b>Administrative Interface</b>	<ul style="list-style-type: none"> <li>• Web-based, point-and-click appropriate for business users. Moderate to non-technical business users can create reports, investigation paths, policies, alerts using the point-and-click interface</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration and user interface appropriate for information security professional</li> </ul>	<ul style="list-style-type: none"> <li>• Configuration and user interface appropriate for information security professional</li> </ul>
<b>Audit Sources</b>	<ul style="list-style-type: none"> <li>• Out-of-box support for over <a href="#">145 clinical application audit sources</a>, agent-less</li> <li>• Extreme flexibility to add new application audit sources into core of solution without professional services</li> </ul>	<ul style="list-style-type: none"> <li>• Routers, IDS, IPS, firewalls, and many infrastructure layer devices</li> </ul>	<ul style="list-style-type: none"> <li>• Network data: Data in motion over a network.</li> <li>• Stored data: Stationary data stored in archives.</li> <li>• End-point data: Data residing in 'endpoints' i.e. Laptops and Desktops</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>• Event correlation on patients and users across clinical application audit sources</li> <li>• Sophisticated algorithmic and behavioral-based patient-privacy scenarios which are domain rich in user and patient data. Focus on patient-privacy business logic accumulated from years of experience with healthcare providers</li> </ul>	<ul style="list-style-type: none"> <li>• Event correlation across infrastructure audit sources</li> <li>• Sophisticated algorithms for incident detection involving computer servers, desktops, email systems and wide range of infrastructure components.</li> </ul>	<ul style="list-style-type: none"> <li>• Event correlation across data sources.</li> <li>• Reporting capabilities on e-mail, word docs, archives, network traffic</li> <li>• Relies on auxiliary SIEM product for advanced reporting, dashboards, workflow, analysis and correlation.</li> </ul>

**FairWarning, Inc.**

Email: [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

Phone: 727 576 6700 x115



<b>Service and Maintenance</b>	<ul style="list-style-type: none"> <li>• Deployed as <a href="#">appliance server</a> and runs as an on-customer-premise service with FairWarning® responsible for operation, maintenance</li> <li>• Privacy, management or business users required to research user-patient-privacy incidents</li> </ul>	<ul style="list-style-type: none"> <li>• Software or appliance based deployment models</li> <li>• FTE(s) or a significant allocation of FTE to operate</li> <li>• Information security resources to research security related threats</li> </ul>	<ul style="list-style-type: none"> <li>• Software or appliance based deployment models</li> <li>• FTE(s) or a significant allocation of FTE to operate</li> <li>• Information security resources to research sensitive data discovery and fine tune/reinforce policies</li> </ul>
--------------------------------	---	--	---

**Figure 1. FairWarning®, SIEM & DLP Comparison**

**“We will build it” promises, *understand the risks***

A select number of Enterprise Security vendors have promised to build a best of both worlds solution using professional services for the clinical applications functionality. Unfortunately for their customers, this has turned out to be a high risk approach with very little payback.

The “we will build it” approach to auditing and monitoring [clinical applications](#) has resulted in lengthy, expensive, and one-off engagements in which the Enterprise Security vendor has found that working with a myriad of clinical application audit sources is very different than working with infrastructure audit sources. *The difference between patients, departments, function codes, floors and users versus TCP/IP addresses and network layer attributes involves completely different architectural approaches.* Unfortunately, there are well established, high profile failures of the “we will build it” approach to a combined privacy monitoring and Enterprise Security approach.

*FairWarning® [customers](#) have taken a proven approach of deploying best-of-breed privacy monitoring, then leveraging FairWarning® Ready for Enterprise Security to perform a security deep-dive on privacy incidents.*

**FairWarning® Privacy Monitoring & Enterprise Security Working Together  
Proven Healthcare Deployments**

Based on use cases from production deployments of its healthcare [customers](#) along with input from service partners as well as hundreds of additional healthcare organizations, FairWarning® and its Ready for Enterprise Security partners have established a deployment model which provides best-of-breed functionality while streamlining proactive incident detection and follow-on investigation.

The proven FairWarning® Ready for Enterprise Security model positions each respective solution to audit and monitor events for which they were specifically designed: FairWarning® for [clinical applications](#) and Enterprise Security for infrastructure layer events. FairWarning® applies patents-pending business logic to the clinical audit sources to detect potential incidents leveraging 100+ existing FairWarning® patient privacy scenarios. The customer Privacy Officer sees the potential privacy incident in the FairWarning® Dashboard and optionally in the form of an email alert. *In parallel, FairWarning® sends the potential privacy incident along with a*

**FairWarning, Inc.**

Email: [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

Phone: 727 576 6700 x115



*payload of clinical application events to Enterprise Security.* The privacy incidents appear in the Enterprise Security dashboard, with additional correlation and analysis on the network elements of the events performed by the Enterprise Security solution. The interface between FairWarning® and Enterprise Security leverages standards based best practices which are well established.

## Summary

Proven deployment models for [FairWarning® privacy monitoring](#) leveraging Enterprise Security solutions have been established. Deployments are based on using each respective product for its out-of-the-box intended use. Privacy Officers, compliance and business users use the best-of-class fraud and privacy detection capabilities of FairWarning®, and with FairWarning® Ready for Enterprise Security, information security officers are in a position to do a deep dive on the security aspects of potential trouble spots. FairWarning® and its partners now truly deliver a best of all worlds solution for privacy, compliance and security. Solutions which involve a “we will build it” approach to clinical application support have proven to be expensive, time consuming, difficult to maintain and have resulted in well established high profile failures.

**For more information on privacy breach detection solutions from FairWarning® and information on FairWarning® Ready for Enterprise Security partners, e-mail [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com) or contact us using the information below.**

**FairWarning, Inc.**

Email: [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com)

Web: [www.FairWarning.com](http://www.FairWarning.com)

Phone: 727 576 6700 x115