



The Power to Prevent:
It's the Next Generation

FIDELIS SECURITY SYSTEMS, INC. 4416 EAST WEST HIGHWAY, SUITE 310, BETHESDA, MD 20814



Deploying Fidelis XPS: Achieving Comprehensive Information Protection in Your Enterprise

Fidelis Security Systems
Tami Stein, Product Manager

March 2010
Version 1.0

Table of Contents

Table of Contents	2
Introduction	2
Approach	3
Ascertain	4
Amnesty	6
Action	7
Automation	7
Conclusion	8

Introduction

Technology and the uses of information are constantly evolving. And along with that innovation and evolution comes threats and risks—talented and persistent threat actors, black market for information, compliance mandates, proliferation of consumer-based communication channels, to name a few.

Built on a patented Deep Session Inspection™ platform, the Fidelis Extrusion Prevention System®, Fidelis XPS™, is the industry's only network security solution with the power to deliver comprehensive information protection. With unparalleled session-level visibility and control to monitor and inspect network traffic, and to stop data breaches, Fidelis XPS provides a powerful and highly flexible technology approach to help organizations protect sensitive data and enforce information security policy.

However, even the most sophisticated technology cannot enforce policy and educate users without human involvement, thus the successful deployment of any security solution requires detailed planning and ongoing management of the solution's interaction with people, policy, and processes.

At Fidelis Security Systems, we take an active role in partnering with our customers—including commercial organizations and government entities around the world—to provide the capabilities, features, and support required to solve their biggest data leakage challenges and defend against cyber attacks. Current customer deployments and the associated first-hand experiences form the basis for this paper, which describes the steps to successful deployment of Fidelis XPS for comprehensive information protection in the enterprise.

The tactical installation process to deploy Fidelis XPS is extremely quick and is nearly almost always completed before lunchtime on the first day of an engagement. More complex is the planning process prior to this installation and the subsequent execution of an orderly and controlled deployment plan. We advise our customers to divide this activity into five phases, three of which were coined by Charles Thompson, CIO of the City of Phoenix, and are used by permission. These phases are the five "A's": Approach, Ascertain, Amnesty, Action, and Automation.

Approach

The most important phase of deployment involves articulation of goals and objectives for the project, and development of a detailed and comprehensive plan. Thus there are several critical steps that should precede the arrival and installation of the technology product(s). This first phase involves establishing the desired relationships between corporate information security policy and the flow of sensitive data.

- What kind of sensitive information is in scope for the project?
- Who owns sensitive information?
- How is sensitive information expected to be used and communicated in the normal conduct of business?
- Are corporate information security and acceptable network use policies current?
- Will this project require revisions or changes to existing policies?

To answer these and many other questions during the *Approach* phase, business leaders and data owners must be closely involved with the network security project team responsible for the Fidelis XPS deployment. The orderly rollout and ultimate success of the project requires a focused planning process managed by the project team, as well as review and buy-in from business stakeholders and data owners. Stakeholder inclusion, review, and buy-in is essential, not only at the project kick-off meeting, but throughout each subsequent phase of the project.

This phase can consume days or weeks depending on customer circumstances, and certain policies and processes may require iterative revisions. Faster time-to-value and process efficiencies are realized when the information protection project is rolled out with a narrow and specific focus, centered on information most critical to the organization. Compliance-related information is the obvious starting point for most enterprises, since it typically includes privacy sensitive information covered by regulations such as HIPAA, PCI-DSS, FERPA, GLBA, and others. Depending on the nature of the business, intellectual property or trade secrets—such as contracts, financial statements, source code or design specifications—may also be among the high-priority information targeted for protection in the first phase of the Fidelis XPS project. The planning team—including data owners—must identify the information to be protected and rank each data type as critical, high, medium, or low. We recommend addressing only the critical data types in the initial phase of an information protection project.

The planning team must also establish clear expectations around how people are allowed to access, modify, and share sensitive information. Existing policies such as Computer Use Agreements, Information Security Policies, and Acceptable Use Policies should provide basic guidelines for acceptable methods of communication of the organization's critical digital assets, both within and outside the enterprise. However, these policies are often not current and may require a review, particularly in the context of compliance-related information.

Take a Look into Unofficial Communication Channels

While reviewing and revising policies during the Approach phase, project planning teams are also advised to identify and document the unofficial communication methods specifically prohibited on the network. In addition to data protection based on content inspection, Fidelis XPS can prevent information from flowing out of the network on unauthorized channels while legitimate business is securely conducted on official or authorized channels such as SMTP e-mail and HTTP access to approved websites. Rogue or unofficial communication methods, such as P2P file sharing services, tunneling applications, and certain consumer webmail and instant messaging (IM) applications, can be blocked during the initial deployment, with confidence that legitimate business over official channels will not be impacted.

Ascertain

This is the learning phase in which Fidelis XPS provides the means to educate the constituents involved in the information protection project on how the network is being used to communicate, and to validate the specific focus areas identified above. In particular, the *Ascertain* phase is not intended to include enforcement or discipline activities (unless a breach is discovered which is so egregious that such action is unavoidable). During this phase, Fidelis XPS reveals the relationships between corporate information security policies and the actual practices of users, so that adjustments and corrections to business processes—and to the deployment plan—can be made. With actual network data in hand, the project team begins to address the next set of key questions:

- How is the information used and communicated in the normal conduct of business?
- How will alerts generated by the solution be classified, reviewed and handled within the organization?
- How will the enterprise communicate with individual users about the information protection project?

As Fidelis XPS is deployed in high-traffic or strategic locations—typically one or more internet egress points and/or internal network segments—the project team gains immediate visibility into the *who, what, where and how* of the organization's network communications. While it is tempting to 'open the floodgates' and enable multiple types of policies, we see the most benefit when project teams launch this phase by activating just a few pre-built policies for detection of sensitive content (e.g., PII, PHI, credit card data, embedded images), application activity (Facebook, IM, webmail), or location-oriented traffic (e.g., nation of origin/destination), as appropriate for the scope of the initial project plan.

At this stage, the project team has real, actionable data that they've probably never seen before—this is one of the reasons why we often remind deployment teams to expect the unexpected. The depth and volume of information may be daunting at first, but with the management tools provided by Fidelis XPS, the iterative process of reviewing network activity, managing and analyzing alert information, assessing potential violations and associated risks, and tuning policies accordingly is intuitively manageable, thus enabling the project team to:

- Identify high traffic areas and applications, as well as specific host systems;
- Learn where sensitive data is stored and observe how that data is put into motion, and where it goes, inside or outside of the secure perimeter;
- Identify rogue channels and unofficial traffic—for egregious violations of acceptable use, move quickly to Action/Automate;
- Identify broken business process processes, report back to data owners for process remediation;
- Identify high risk areas for further monitoring and investigation.

This phase can last for days or weeks depending on customer circumstances. It is most effective when observed and tuned over the course of a full business cycle (1 -3 months); given that monitoring and analyzing alerts and refining policies is an iterative process, and it takes time to observe and measure results. Allow sufficient time for the 'learning' portion of the *Ascertain* phase, and—as noted above—expect the unexpected.

Fidelis XPS Differentiator: Discover Information Flow

In the earliest stages of deployment, even before policies are implemented, the Fidelis XPS Information Flow Map feature provides the visibility the project team can leverage to:

- *Determine information usage to know where to focus Fidelis XPS content policies;*
- *Discover existing business processes as a precursor to setting data leakage policies;*
- *Ascertain the most active hosts on their network, including what information is being sent and protocols being used;*
- *Enable comprehensive information protection by illustrating where additional resources need to be applied in the network.*

Working out-of-the-box with minimal or no configuration involved, an immediate collection of network traffic presents information flow knowledge, allowing customers to automatically have their Fidelis XPS sensors synthesize details of every network flow including sender, recipient, application/protocol, payload content, as well as a variety of other details. The Information Flow Map feature provides a filterable graphical representation of this information, enabling broad views of information flow down to filtered specific views of users, applications, and/or specific information types. Over time, with policies and remediation strategies in place, Fidelis XPS Information Flow Map provides additional benefits, enabling organizations to:

- *Take the knowledge of their network beyond mere "alerts" to an actual understanding of how information is being circulated inside their enterprises and where it is going outside the network;*
- *Gain greater visibility, in real-time, of any policy violations, hidden or unauthorized activities, rogue business processes, and abuse, in order to automate policies to remedy any found problems quickly and easily;*
- *Test the outcome of new Fidelis XPS rules and triggers;*
- *Manage network data security even in situations where the administrator is not permitted to view or act on sensitive content.*

Some customers skip right to *Action* and *Automate* for Channels Control (i.e., network usage violations) as they have been through the *Ascertain* and *Amnesty* phases using other network security technologies previously, and, with Fidelis XPS, have quickly identified rogue channels and unofficial traffic, and are therefore comfortable blocking this activity.

During the *Ascertain* phase, the project team and the business leaders will also determine how alerts, policy violations, and related information from Fidelis XPS will be reviewed and handled, not only within the security team, but across the organization and all data owners. Alerts must be classified into different severities for incident handling and management, and decisions made regarding who is responsible for viewing those alerts. Some customers have a central resource (or resources), often in information security, for managing all alerts and conducting forensics investigations. Others have decentralized management by groups such as legal departments, privacy officers, data owners, and network security teams, who receive notification of the violation from the security team, along with detailed information (as captured by Fidelis XPS) for further investigation and action.

Establishing responsibility and procedures for incident response—whether the incident is a high-impact breach or a minor policy violation—will produce a more effective and repeatable process for all phases of the project, particularly since disciplinary actions and reporting of breaches are human-intensive processes requiring intervention by one or more departments/functions.

Amnesty

The *Amnesty* phase involves a focus on educating the organization as well as the first direct contact with employees whose actions are contrary to information security policy, in accordance with the communication plan developed in the previous phases. Policies and procedures for the daily operations of Fidelis XPS should be well established prior to this phase. The goal is information and education: no disciplinary action is taken (except for particularly egregious or malicious violations) during this phase, whose dual purpose is to (a) educate end users on acceptable use policy and provide notice that an automated solution is in place to enforce this policy; and (b) educate management and data owners on areas for business process improvement. The length of this phase can vary widely depending on a variety of factors, unique to each organization.

To ensure that the education message reaches and is understood by all constituents, multiple communication methods are recommended, with the approval and—importantly—the endorsement of business leaders. Wherever possible, sanitized, real-world examples of unacceptable use and other policy violations should be provided to all parties to the violation, including end users, their managers, and owners of the protected data. This enables the data owners to adjust business processes accordingly, and to educate the organization as to the risks and consequences of data leakage, often the result of unintended behavior.

Key elements of the successful education component of this phase are awareness that leadership is serious about enforcing information security policy, and that technology is in place for visibility and automation. When these messages are clearly articulated, organizations typically report an increase in overall security practices and fewer violations, even though penalties are not assessed and disciplinary actions are not taken.

Action

The goal for the *Action* phase is to permit an enterprise to take an active enforcement posture with respect to information security policy violations, communicating these violations to end users, data owners and management in accordance with the communication plan developed earlier. This includes formal communication of violations to end users and data owners as defined in previous phases, as well as real-time notification, responses, and disciplinary actions as required and appropriate. Many of these actions will be taken manually, due to the involvement of other teams, such as HR, legal, etc.

During this phase, organizations take enforcement actions as policy violations occur, leveraging each event to educate users, particularly on official traffic such as web channels and outbound e-mail. Since these are typically the first channels applicable to automation and prevention, the user experience is key, and must include immediate notification, action, and policy education.

In this phase of deployment, we reiterate the importance of staying focused on information most critical to the organization, as identified by the project team in the *Approach* phase. Once incident response processes are well-documented and consistently carried out for the high severity violations, organizations find it much easier to model appropriate responses and processes for less serious violations.

Organizations often give special consideration to outbound e-mail, since it is the easiest and most frequent route by which protected as well as unprotected information leaves the organization, therefore Fidelis XPS provides multiple options for automation and remediation as well as the end user experience. For example, serious violations can be blocked and/or additional graceful actions for remediation and incident handling can include quarantine, allowing for further review before release or discard, and automated encryption, and secure delivery when paired with e-mail gateway encryption solutions from one of our partners (PGP, PKWARE). For a smooth deployment with minimal impact to the existing mail chain, customers often deploy Fidelis XPS for content inspection and appropriate response to the organization's existing MTA via Milter plug-in.

Automation

The final phase leverages the real-time prevention capabilities of the Fidelis XPS solution in concert with the network security team's confidence in the system to distinguish critical violations from low-priority alerts and false positives—all of which will have been observed and tuned during prior phases. In addition to automation through prevention (network blocking), automatic systems for enterprise notification and alert management are brought online during this phase.

There are four key areas of automation within the Fidelis XPS solution: prevention, encryption, notification, and alert management.

- 1) **Prevention:** Most customers introduce blocking for the most egregious violations using the prevention sniffer (Fidelis XPS Direct, Edge, and Internal), as it enables comprehensive detection paired with prevention for unofficial and rogue traffic, where organizations are most comfortable preventing. Although protected or sensitive information shouldn't be leaving the organization at all, there may be official communications that contain mishandled sensitive information, so the ability to prevent based on content is equally critical. Based on the traffic monitored, the alerts reviewed, and the policies tuned in the learning phase, customers

typically implement their prevention strategies to address alerts with Severity level of *Incident* first, followed by alerts using Rogue or Unofficial communications methods or unauthorized locations.

- 2) Encryption: Using Fidelis XPS Mail and server-side mail encryption solutions, the process of encrypting sensitive information to approved recipients via SMTP e-mail traffic can be automated, with simultaneous notification to end users and incident handlers.
- 3) Notification:
 - a) Official communication protocols often allow the end user notification process to be automated, in many cases even without preventing the session. If there is an e-mail address in the message (webmail, SMTP, etc.), the message can be delivered, prevented, encrypted, or quarantined with an informational message sent to the end user notifying them of the action taken on the email. This form of notification also has the ability to educate the user regarding information security policies as well as the user's responsibility to protect the organization's digital assets. Traffic through a Web Proxy server can be redirected to a policy page, providing another form of policy education and informational messaging to the end user.
- 4) Alert Management: Alert management can also be automated. Virtually all Fidelis XPS deployments integrate alert information from Fidelis XPS into existing security and compliance management processes, often handled with SEIM, log management, help desk, or other event/alert management mechanisms.

Each of these project phases may reveal the need to update information security or acceptable use policy, or even business process policy as new information is discovered about how business is (or should be) done within an enterprise. These revelations are common in Fidelis XPS deployments and should be accounted for as much as possible during the formulation of engagement project plans.

Conclusion

Fidelis XPS provides a powerful and highly flexible technology approach to help enterprises protect sensitive data and enforce information security policy. This goes far beyond traditional data leakage prevention—it is comprehensive information protection, your ability to actively defending the sensitive data that your organization requires to do business. By leveraging the immediate visibility of network activity provided by the Information Flow Map feature in Fidelis XPS, including content, Fidelis XPS deployments not only yield more holistic security benefits than traditional DLP solutions, these benefits are realized in a fraction of the time when using the methodology described in this paper to integrate the project into the organization. The most important part of any technology deployment—especially as it relates to privacy and security—is recognizing that deploying the technology only solves part of the problem. Therefore it is essential to take the time to develop a detailed deployment plan, get the business leaders involved early, and make sure the team understands, and is well prepared to appropriately address, the intersection of people, process, and technology.

FIDELIS SECURITY SYSTEMS, FIDELIS EXTRUSION PREVENTION SYSTEM, FIDELIS XPS, the FIDELIS SECURITY SYSTEMS logo, and/or other FIDELIS SECURITY SYSTEMS products referenced herein are trademarks of Fidelis Security Systems, Inc. Copying, use or distribution of any material contained herein is expressly prohibited. *Copyright © 2010 Fidelis Security Systems, Inc. All rights reserved.*