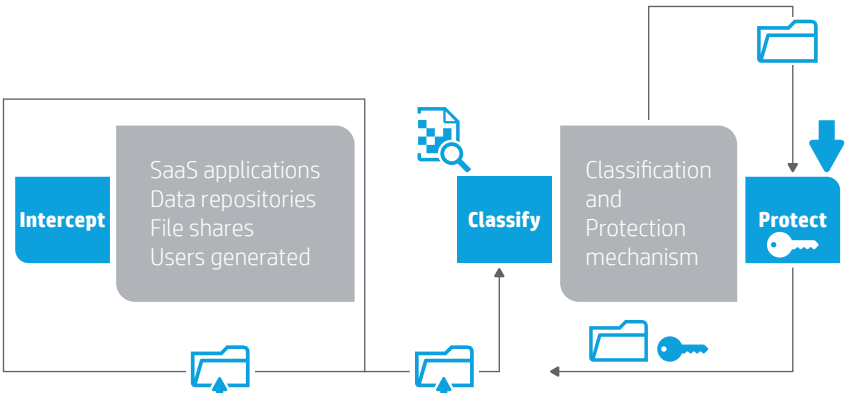
Family data sheet

HP Atalla Information Protection and Control

Automatically classify and protect unstructured data persistently

June 2014

Figure 1. Embed protection in the data at the point of creation



The second-highest return on investment (ROI) in security investments comes from the widespread and effective application of encryption, policy, and access controls on data.

In an era of increasing cyber threats and targeted attacks, organizations must now assume that their network has been breached. How, then, can organizations protect sensitive unstructured data like documents and spreadsheets from improper access? HP Atalla Information Protection and Control (IPC) solves this complex issue by giving organizations the means to bring protection to the data itself. HP Atalla IPC applies protection at the point information is created and makes that protection persistent, so it follows the information wherever it goes. This secures sensitive data no matter where it actually resides.

The challenge of protecting unstructured information

Analysts estimate that by 2015, nearly 90 percent of organizational data will be unstructured.[1] Sensitive organizational data in spreadsheets, documents, presentations, and other files resides in multiple locations—for example, employee laptops/mobile devices, file servers, and storage arrays (NAS and SAN). In today's de-perimiterized environment, collaboration is crucial—but sharing data necessitates exposing it. Traditional data protection solutions inhibit productivity by applying protection unnecessarily, and items classified as "sensitive" easily lose this classification if it's not saved in a predefined format or network location, or if modified out of original context.

Today, this creates enormous challenges for enterprises that are struggling to understand where all their sensitive content lives. They also need to determine how to apply consistent policy to protect that sensitive information from falling into the wrong hands. There is even more complexity federating these controls over information in the various operating environments that their users interact with the data. Today's and tomorrow's enterprise is becoming a very difficult place in which to protect information.

Businesses need advanced capabilities to classify sensitive data, apply consistent policy to the valuable assets they identify, and to federate those protections across the borderless enterprise.

[1] IDC Predictions 2012: Competing for 2020

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, HP Atalla, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

About Secure Islands

Secure Islands develops and markets advanced Information Protection and Control (IPC) solutions for the borderless enterprise. Offering policy-driven classification and protection for unstructured data, Secure Islands lays the foundation for sensitive information security in enterprises as they shift from perimeter defense to persistent protection. Secure Islands' holistic approach literally redefines information security and assists the enterprise in regaining control by identifying, classifying and protecting sensitive information throughout its lifecycle.

Highlights

- One-click protection action
- Extends Outlook user's permission selection to the entire AD RMS permissions set

Nearly 90 percent of the content being created includes unstructured data types such as documents, social content, video, and images

Embed security at the point of data creation

Unlike traditional solutions that attempt to control users, channels or storage, HP Atalla IPC runs the IQProtector® platform engine from Secure Islands. It protects data—uniquely embedding protection within the data itself at the moment of creation or initial organizational access in unstructured form. IQProtector agents on enterprise hosts instantly identify and classify all new, modified, or accessed sensitive data from any origin. This data, identified with extremely high accuracy, is persistently tagged, enabling comprehensive control over access and usage.

The HP Atalla IPC software family is packaged as 1-year term or 3-year term licenses with 24x7 support included, and can be categorized as follows:

HP Atalla Information Protection and Control Suite (HP Atalla IPC Suite)
This is the core information protection suite. It includes management software and:

- Persistent Multi-format File Protection
- Persistent Email Protection
- Persistent Web, Application, and Cloud Protection
- Persistent Information Protection Data Analytics
- Persistent Protection for Remote Desktop Services (e.g., Citrix®/Terminal Services)
- SharePoint Classification and Protection

Licensing unit: Number of users, requires one license for each user

HP Atalla IPC Bridge for content inspection services
This is deployed on enterprise services such as antivirus/DLP/Search/Archive/Indexing to access and scan encrypted content seamlessly.

Licensing unit: Number of implementations; it requires one license for each "implementation" of an IT service that needs a bridge, e.g., one antivirus package

HP Atalla IPC Scanner—Classification and protection
Essentially a document crawler, the scanner scans, classifies, and protects pre-existing data on repositories.

Licensing unit: Number of implementations; it requires one license for each implementation which corresponds to one deployment instance. The number of scanner implementations depends on the volume of pre-existing data and required scanning rate.

HP Atalla IPC compliance service for Exchange
This provides the ability to decrypt protected emails and attachments for archiving and compliance purposes. It is deployed on Microsoft® Exchange Hub Transport role servers and managed centrally.

Licensing unit: Per Microsoft Exchange Server and per mailbox. Requires one license for each "implementation" of Microsoft Exchange, typically defined as one Exchange Hub "Transport role Server", as well as one license for each Microsoft Exchange mailbox (email address)

HP Atalla IPC Mobile Support for Microsoft AD RMS
This provides organizations the ability to collaborate with Rights Management Services (RMS) protected emails and attachments securely over major mobile operating systems and devices (iOS, Android, Windows®, BlackBerry).

Licensing unit: Number of users (not number of devices); it requires one license per user.

HP Atalla IPC AD RMS extensions for Outlook
This provides a simple way to apply Microsoft Active Directory Rights Management Services (AD RMS) protection within Microsoft Outlook to increase the effective usage of RMS within the enterprise. It supplies flexibility to end users to apply permissions beyond the standards of Microsoft Outlook.

Licensing unit: Per user

Professional Services, Training, and Support
Professional services to implement the solution, training for deployment and management, and included 24x7 support for the software over the licensed term based on net term license price.

HP Atalla Information Protection and Control Suite

The encryption and the Information Rights Management (IRM) implementation gap
Enterprises and government organizations need to protect sensitive digital information. Persistent encryption is the ideal choice to provide this protection. However, the gap between theory and practice in implementing enterprise-wide encryption remains vast. The HP Atalla IPC Suite from Secure Islands bridges the persistent protection implementation gap with powerful classification and protection using IRM (e.g., AD RMS) or other encryption engines, together with simple policy generation, application, and enforcement.

End-to-end classification and protection
The HP Atalla IPC Suite, running the IQProtector platform engine from Secure Islands, classifies and protects sensitive data throughout its lifecycle—from creation through collaboration and storage. For files, email, enterprise systems, and everything in between, it delivers easily-implemented and cost-effective solutions for all persistent file and email encryption needs.

HP Atalla IPC Suite is designed to work well in small, medium, and large enterprise deployments. The system's unique data-centric architecture allows classification and protection of any volume of data, and supports a wide range of organizational topologies and environments. Designed for scalability, HP Atalla IPC enables gradual enterprise deployment, while still effectively securing data even on hosts on which IPC Suite agents have yet to be deployed.

Key HP Atalla IPC Suite benefits
- True enterprise-wide solution for Microsoft AD RMS and other encryption engines
- Effective control of the entire ecosystem, on and off premises
- Easy integration into IT infrastructure and assimilated into organizational business flow
- Low TCO
- Support for the entire spectrum of sensitive organizational data

Key features of the HP Atalla IPC Suite
- Enables smooth assimilation of IRM and encryption practices into business processes—without complex, lengthy, and costly integration—by leveraging existing IRM (identity and rights management frameworks)
- Can control sensitive data based in context of the user, device, application, and location
- Provides full control over attributes such as viewing, printing, editing, copying, etc.
- Protects data in transit, at rest, and in use
- Light footprint means minimal performance impact
- Automatic, highly accurate classification and protection using Microsoft AD RMS for any data type or format
- User-driven classification with system recommendation options
- Protection of data from any source (app, web, cloud, enterprise content management, repositories, file servers, NAS, SAN) without integration complexity
- Content marking for classification visualization
- Metadata labeling for data loss prevention (DLP) accuracy and classification efficiency
- Adaptive protection to support collaboration across the enterprise
- Enables flexible security policy during implementation, based on business logic and business-centric elements (users, data, and entitlements)—this makes the definition natural and simple. This is in contrast to the challenges that arise in systems that depend on a very technical and infrastructure-centric policy definition during implementation (channels, ports, protocols, devices, etc.).
- Audit reporting and in-depth analysis for forensics and risk assessment
- Seamless content inspection by trusted apps such as antivirus/DLP/Search/Archive/Indexing systems

HP Atalla IPC Suite modules and capabilities

- Persistent Multi-format File Protection—the IQProtector platform engine from Secure Islands uniquely embeds protection within the data itself at the moment of creation—instantly identifying, classifying, and persistently tagging all new, modified, or accessed sensitive data from any origin.
- Persistent Email Protection—Content-sensitive IQProtector encryption protects email, documents or other files tagged as sensitive—encrypting data according to a customizable security policy.
- Persistent Web, Application, and Cloud Protection—For files uploaded or sent to cloud services, the IQProtector platform engine automatically classifies and protects sensitive data. For files and reports downloaded from cloud or web-based services, IQProtector protects sensitive data as it moves beyond application boundaries.
- Analytics—the solution enhances the visibility of sensitive data and its usage—creating an enterprise-wide mapping of where sensitive data resides, who accesses it, where it is sent, and how it is used.
- Persistent Protection for Remote Desktop Services (Citrix/Terminal Services)—the solution enables organizations working via remote virtualized environments to maintain centrally-managed data security for any data type or usage scenario, enforcing the relevant security policy for each concurrent user.
- SharePoint Classification and Protection—IQProtector delivers automatic classification, content marking, metadata labeling, and more at the time of content creation or upload—providing automatic protection of SharePoint data based on a centrally-managed policy.

Table 1. Features and benefits—Persistent Multi-format File Protection

Key features of Atalla IPC Persistent Multi-format File Protection	Benefits
Automatic classification at content creation	Full content identification accuracy, simple deployment, no repository scanning required
Automatic protection based on central policy	Enterprise has comprehensive control over what, why, when, and how to protect data, completely transparent to the end-user
Content marking—classification-driven addition of visual labels to documents	Increase security awareness by visualizing document classification, raise both compliance and user accountability
Scanner mode server	Classification and encryption of pre-existing content on file servers, NAS, SAN, and Enterprise Content Management (ECM), that is, CIFS-based repositories e.g., HP Worksite
Optional user classification—enabling the user to decide the type of classification required for a given document or mail	Increased user accountability, added classification accuracy
Extends AD RMS file format support (multi-format)	Protection for additional file formats by preserving original file formats, without application integration
Protection of client or application-based content	Applies AD RMS protection on files and data exported from applications without integration
Metadata labeling for DLP, File Classification Infrastructure (FCI), e-discovery, archiving	Enhances the value of FCI and lowers the burden on DLP by accurately identifying, classifying, and tagging sensitive enterprise data early in the data lifecycle to allow effective DLP enforcement
Protect documents upon access	Apply AD RMS protection on pre-existing content
Extendable to other encryption schemes	Conversion of AD RMS protected data to other protection schemes
Audit and report on every action on files everywhere	Monitoring and audit mechanisms operate throughout the information lifecycle

Persistent Mail Protection

Email encryption is an excellent method of maintaining data integrity and limiting access to sensitive data in transit and at rest-in-house or in cloud-based mail services. However, existing encryption solutions require end user action to operate, and cannot differentiate between data that could be encrypted, and data that must be encrypted.

IQProtector is based on an ongoing, infrastructure-agnostic, usage-based discovery and centrally-managed classification engine for sensitive data as it is created. IQProtector protects crucial corporate data sent via email without the need for active user intervention. IQProtector classification and encryption are based on a central policy directed by the enterprise. Email, documents or other files tagged as sensitive can be automatically protected according to customizable security policy. HP Atalla IPC enables encryption IRM to be applied automatically, leveraging pre-defined parameters based on content, user, subject, sender, recipient, attachments, and more.

This is ideal for:

- Secure collaboration among partners and customers
- Protection of email in online cloud mail services—this depends on the client used, if the client is Outlook, the infrastructure can be Gmail. If the interceptor is at the Exchange infrastructure level, any client can be used.

Key features and benefits of Persistent Mail Protection

- Automatic email encryption—providing automatic classification of email content and attachments without active user intervention
- Automatic protection based on central policy enables complete centralized control over all sensitive information, enterprise-wide
- User classification empowers users to apply classification to email, raising accountability and awareness
- System classification recommendation enables enterprises to raise awareness by identifying information sensitivity
- Automatic conversion of Windows RMS protected data to other protection schemes based on central policy enables continued use of existing protection/encryption schemes such as Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME), and more
- Content marking—classification-driven addition of visual labels to emails increase security awareness by visualizing mail classification, raising both compliance and user accountability
- Automatic metadata tagging assists DLP systems in accurate identification of sensitive information, significantly reducing the incidence of false-positives
- Monitoring and audit mechanisms operating throughout the information lifecycle ensure all sensitive data sent by mail is audited and monitored

Web, application, and cloud protection

In a cloud environment, sensitive enterprise data such as email in online mail services, web services data, and files uploaded to the cloud are potentially vulnerable—accessible to unauthorized service provider staff and third parties. Data downloaded from cloud or web-based applications is also vulnerable as it moves beyond application boundaries, and can be leaked to unauthorized users by employees and partners, either intentionally or by mistake.

IQProtector maintains tight control and security over unstructured distributed cloud and web services data such as email and files. For data uploaded or sent to cloud services (such as Office 365/Microsoft Online Services, OneDrive, Google™, Salesforce.com® etc.), IQProtector automatically classifies and protects sensitive data—keeping it safe from both service provider staff and third parties.

For data accessed from Cloud or web-based services, IQProtector protects your sensitive data as it moves beyond application boundaries in the form of webpages, reports, printouts, and more—with no integration overhead.

Key features and benefits of Persistent Web, Application, and Cloud Protection

- File protection on upload or store—Prevents exposure of sensitive files to third parties from administrators to opportunistic attackers.
- Download file protection—Applies automatic protection on downloaded files.
- Preconfigured policy for Salesforce.com—Simple and rapid to get up and running with Salesforce.com protection.
- Audit of sensitive data viewed or extracted on web or cloud—Protects any web or cloud-based application with no integration required.

Data analytics

In the tight regulatory and security environment where enterprises and governments operate, it is important to keep security policy in-line with real-world usage. This is done, in part, by quantifying exposure (internal and external) for effective risk assessment, and maintaining strict auditing and forensics capabilities.

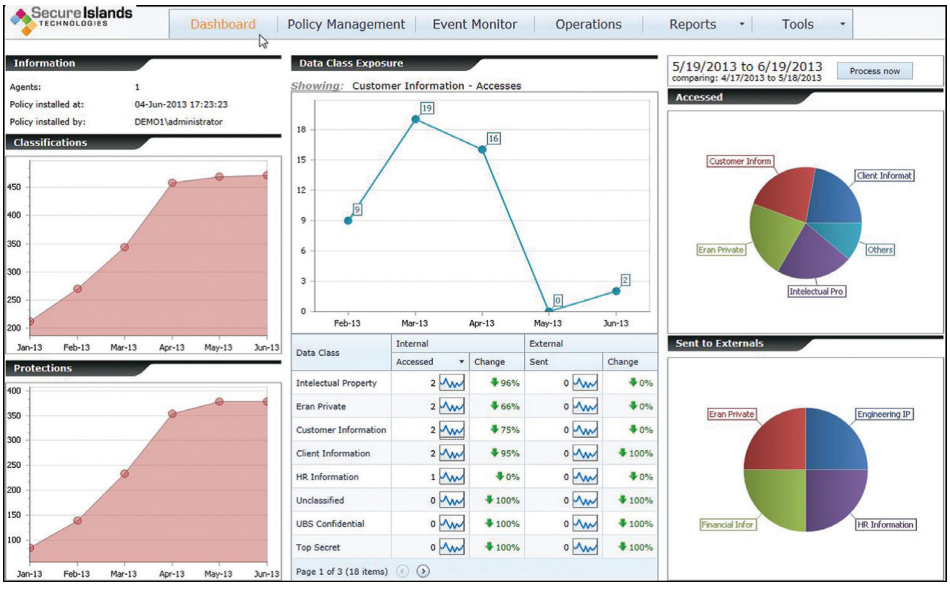
The HP Atalla IPC Suite has powerful analytics capabilities that enhance the visibility of sensitive data and how it is used—enterprise-wide.

Leveraging predefined parameters, the IQProtector platform engine performs a rapid, content-aware, infrastructure-agnostic, usage-based discovery process. Enterprises draw powerful insights by analyzing and classifying data accessed during actual business activity, because it allows them to create an enterprise-wide mapping of where sensitive data resides, who accesses it, where it is sent, and how it is used.

In a self-reinforcing cycle, the IQProtector platform engine enables an adaptive security policy to match evolving data usage, i.e., the tools are flexible enough for policy to be redefined when business decides to take action to change inputs. Leveraging its infrastructure agnostic characteristics, the platform's analytical capabilities enable ongoing data-centric risk assessment and reporting for any internal or external network locations and features. This allows:

- Complete visibility based on sophisticated Online Analytic Processing (OLAP) analysis of data usage inside and outside the enterprise
- Quantification of exposure internally and externally based on data, locations, and users
- Audit and forensics reporting capabilities for compliance

Figure 2. Security and Data Analytics



Key features and benefits of persistent information protection Data Analytics

- Information exposure matrix—Helps organizations build protection based on actual usage patterns, measures effectiveness of overall security policy in absolute terms
- Internal and external data-centric exposure analysis reports—based on location, users, and data—Complete exposure visibility, track, and monitor data usage across the entire organization
- User behavior anomaly detection—Immediate anomaly detection maximizes data security

Persistent Protection for Remote Desktop Services (Citrix/Terminal Services)

IQProtector enables organizations working via remote virtualized environments to maintain centrally-managed data security for any data type or usage scenario, enforcing the relevant security policy for each concurrent user.

Organizations move to virtualized environments to enable the workforce to use a secure, centrally controlled, remote desktop work environment. Existing solutions are hard-pressed to provide a centrally managed data security policy for any data type and usage scenario in remote virtualized environments. HP Atalla IPC running the IQProtector engine from Secure Islands can do this while enforcing the correct role-based policy for each concurrent user.

IQProtector enables organizations working via remote virtualized environments to maintain centrally-managed data security for any data type or usage scenario, enforcing the relevant security policy for each concurrent user. It also applies protection to pre-existing content and converts protection to meet other data protection or encryption schemes.

Key features and benefits of Persistent Protection for Remote Desktop Services

- Automatic classification of email content and attachments enable sensitive emails are protected even without user intervention
- Automatic classification of file content on creation and access allow for extremely high content identification accuracy, simple deployment, no repository scanning required
- Automatic protection of file content based on central policy ensures that an enterprise has comprehensive control over what, why, when, and how to protect data, completely transparent to the end user
- File protection on upload to web services prevents exposure of sensitive files to third parties from administrators to hackers
- Protects items downloaded from web services and applies automatic protection on downloaded file

SharePoint Classification and Protection

IQProtector delivers automatic classification, content marking, metadata labeling, and more at the time of content creation or upload—providing automatic protection of SharePoint data based on a centrally-managed policy.

Many enterprise and public sector organizations use Microsoft SharePoint® for content management. Part of these organizations' business requirements is the definition of permissions for stored documents. Often, the level of flexibility to set permissions within SharePoint cannot meet key customer demands, such as defining permissions based on sensitivity, data classifications, or content. Furthermore, the SharePoint permission model doesn't handle segregation of duties between data owners and SharePoint database administrators—which poses a risk to sensitive data stored in SharePoint.

The HP Atalla IPC suite has an IQProtector engine for SharePoint that solves the challenges of SharePoint data security, delivering automatic classification, content marking, metadata labeling, and more at the time of content creation or upload. It also provides automatic protection based on a centrally-managed policy. This delivers hardened, item-based security, without lowering SharePoint productivity and functionality.

Key features and benefits of SharePoint Classification and Protection

- Classification at content creation—full content identification accuracy, simple deployment, no repository scanning required
- Automatic protection based on central policy—Comprehensive centralized control over all sensitive information, enterprise-wide
- Content marking—Increase security awareness by visualizing document classification, raising both compliance and user accountability
- Metadata labeling for DLP, FCI, e-discovery, archiving—Lowers the burden on DLP by accurately identifying, classifying, and tagging sensitive enterprise data early in the data lifecycle to allow effective DLP enforcement
- Protection based on SharePoint columns (metadata)—Alignment of both SharePoint and RMS permission schemes into a coherent and persistent entitlement model

The IQProtector platform engine from Secure Islands enhances the visibility of sensitive data and its usage—creating an enterprise-wide mapping of where sensitive data resides, who accesses it, where it is sent, and how it is used. In a tight regulatory and security environment, keeping security policy in-line with real-world usage, quantifying exposure (internal and external) for effective risk assessment, and maintaining strict auditing and forensics capabilities are mission-critical to enterprises and governmental organizations alike.

HP Atalla IPC Bridge for Content Inspection Services

This is a content inspection engine for Trusted Applications and Services. For enterprises that deploy the HP Atalla IPC Suite, there may be a need to ensure that trusted applications and services are allowed to continue to inspect content that has been protected and encrypted. The HP Atalla IPC Bridge for Content Inspection Services, allows Enterprise Content Management tools, DLP, antivirus, and other enterprise IT systems to inspect, index, and classify encrypted content—preserving significant prior investments in existing systems. Seamless content inspection by trusted apps such as antivirus, DLP, search engines, and archiving systems is vital to enterprises.

With the move to wide-scale encryption, enterprises have found these mission-critical tools impaired in their ability to access data, lowering productivity and ROI. The content inspection bridge is assimilated in ongoing usage patterns, ensuring continuing productivity and access to key enterprise data, while still maintaining the highest level of data security.

Key feature and benefit of the HP Atalla IPC Bridge for Content Inspection Services

- Seamless access to encrypted content by trusted apps and services, which allows easy assimilation and implementation into the existing IT setup, allowing different scanning engines (DLP, antivirus, search, index, archive, and more) to read protected content.

HP Atalla IPC Scanner—Classification and Protection

This is a content inspection engine that is deployed on Windows servers. It scans, classifies and protects pre-existing data on repositories based on the HP Atalla IPC policies that have been defined for new and ongoing content in the IQProtector engine from Secure Islands.

This is deployed on Windows servers. Essentially a document crawler, the scanner scans, classifies, and protects pre-existing data on repositories.

Licensing unit: Number of implementations; it requires one license for each implementation which corresponds to one deployment instance. The number of scanner implementations depends on the volume of pre-existing data and required scanning rate.

HP Atalla IPC Compliance Service for Exchange-Server

This provides the ability to decrypt protected emails and attachments for archiving and compliance purposes. It is deployed on Microsoft Exchange Hub Transport role servers and managed centrally.

Licensing unit: Per Microsoft Exchange Server and per mailbox. It requires one license for each "implementation" of Microsoft Exchange, typically defined as one Exchange "Hub Transport Server", as well as one license for each Microsoft Exchange mailbox (email address).

HP Atalla IPC Mobile Support for AD RMS

Key benefits
- Full AD RMS usage rights on mobile devices
- Control corporate emails and documents on mobile devices
- No un-encrypted data on the mobile device

Highlights
- Low TCO
- No additional infrastructure
- Clientless solution
- Perfect for both BYOD and managed devices

Supported platforms
- iOS
- Android
- BlackBerry OS 5/6/7
- AD RMS natively supported in Windows

Bring your own device (BYOD) and the use of mobile devices to enhance productivity create opportunities and challenges for enterprise IT executives. IT executives understand the benefits of this trend, but are also concerned about the security risks involved when data is stored and used in uncontrolled devices.

Microsoft AD RMS is an information protection technology that works with AD RMS–enabled applications to help safeguard digital information from unauthorized use. Content owners can define who can open, modify, print, forward, or take other actions with the information.

IRM technologies such as AD RMS provide an excellent model to overcome the challenges inherent when data is used and stored in uncontrolled devices. AD RMS protects the data irrespective of the underlying device, even if it is beyond the reach of corporate IT. However, AD RMS needs augmentation to fully support all mobile scenarios.

HP Atalla IPC removes these barriers by introducing HP Atalla IPC Mobile Support for AD RMS. This is an easy-to-use, manage, and deploy solution. Users in an enterprise can securely send sensitive emails and be sure that the intended recipient will be able to read them securely, anywhere. Enterprises can apply RMS protection without having to supply any additional training to end users. This allows secure viewing of mails and attachments on major mobile OS platforms without the need to manage or install an application on the mobile devices.

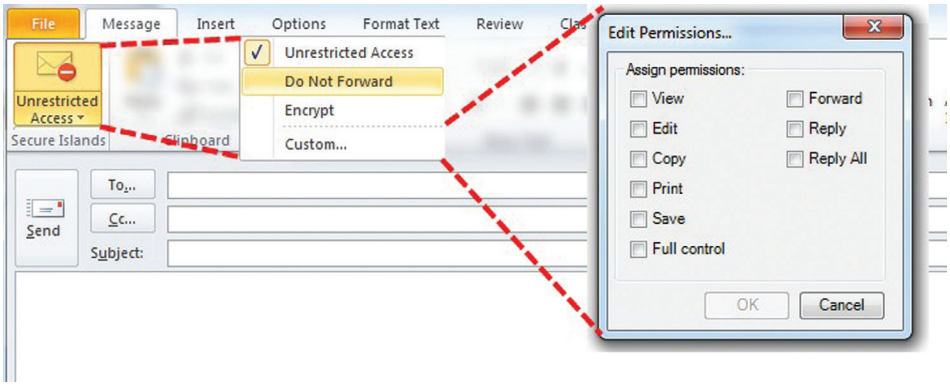
Table 2. Features and benefits—Mobile Support for AD RMS

Key features of Atalla IPC Mobile Support for AD RMS	Benefits
Full AD RMS usage rights on mobile devices on e-mails and attachments (including Office and PDF files)	Control the usage of sensitive e-mails and attachments on mobile devices (view, edit, forward, reply etc.).
Control corporate emails and documents on mobile devices	The control of the data is always at the organization control, even when the device is lost or stolen.
Major mobile OS platforms supported (iOS, Android, Windows, and BlackBerry devices)	Users have the freedom to choose any major device. Perfect for BYOD initiatives.
Same UI on all platforms—The UI for the end user is known and simple	Users are familiar with the interface, no learning curve in using the solution, no change when moving from one platform to the other.
No additional infrastructure—The product is installed directly on the Microsoft Exchange infrastructure using standard Exchange mechanisms	Low TCO—easy to install, no extra management is needed, no complicated settings.
Clientless—No application is needed to be installed on the mobile device	Supports every MDM solution in the market including the usage of any mobile client.
Compose/reply/forward options on e-mails in a secure manner while retaining the items in the same user's inbox	Users can have complete flow of e-mail conversations even those which are protected.

Key benefits

- Enables smooth assimilation of IRM into business processes without complex, lengthy, and costly integration by leveraging existing frameworks
- Can control sensitive data based in context of the user, device, and location
- Provides full control over attributes such as viewing, printing, editing, copying, etc.
- Protects data in use, in transit, and at rest
- Light footprint means minimal performance impact

Figure 3. HP Atalla IPC AD RMS Extensions for Outlook



HP Atalla IPC AD RMS Extensions for Outlook

AD RMS infrastructure is an excellent and widely used data protection offering. However, the solution rarely meets its full potential in the enterprise, particularly when e-mails are involved. One of the main reasons is functionality and usability barriers to Microsoft Outlook users.

There are real usability challenges because end users are required to hit multiple clicks and tabs when trying to apply protection. This also assumes that they know where to find the RMS protection functions to apply.

AD RMS functionality within Outlook limits the user to a single set of permissions, for example—"Do Not Forward" or allows pre-defined AD RMS templates, which are often suboptimal in mail usage scenarios. These limitations may discourage AD RMS usage because users want to apply different rights.

HP Atalla IPC removes these barriers and makes it easy to apply AD RMS protection without requiring additional end user training. In addition, the solution allows users to apply additional protection, for example: "View", "Edit", "Copy", "Print", "Save", "Forward", "Reply", and "Reply All."

System requirements

• Outlook 2003/2007/2010/2013

Table 3. Features and benefits—AD RMS Extensions for Outlook

Key features of Atalla IPC AD RMS Extensions for Outlook	Benefits
One click protection button	Provides a simple way to apply AD RMS protection within Microsoft Outlook. No additional training needed. It dramatically increases the AD RMS usage within the enterprise.
Permissions selection—Extends permissions set beyond "Do-Not-Forward" right such as: Encrypt only, view, edit, copy, print, save, forward, reply, and reply all.	Supplies flexibility to end users to apply permissions beyond the standards of Microsoft Outlook. Dramatically increases the AD RMS usage within the enterprise.
Extra "Owner"—Automatically adds a supplementary default owner user to protected mails.	Suitable for e-discovery and archiving systems without the need to configure an AD RMS superuser group.
Boilerplate text* customization—*This text is viewed in scenarios when AD RMS protected items are not supported.	Be able to "brand" the page with customized text, images and links.
Multilingual support—Customization of text labels within the user UI.	Could be adjusted to customers' native languages.
IQProtector integration—Definition of automatic protection rules based on the mentioned permission extensibility model.	Allows automatic protection based on central policy; assures organizations are able to enforce protection on sensitive mails.
Simple installation	Requires zero configuration and administration for end users.

Professional services

Professional services provided primarily by Secure Islands
In addition to providing advanced technology solutions, HP and Secure Islands provide a range of professional services around security for HP Atalla IPC.

- Quick Start Program
- On-Site Consulting and Implementation
- Microsoft AD RMS Consulting, Planning and Implementation
- Secure Islands IQProtector Training

Quick Start Program
The Secure Islands Quick Start Program is a pre-packaged professional services solution that covers all of the steps in an IQProtector deployment, including planning, design, configuration, and tuning, without requiring a detailed statement of work or custom professional services. By engaging specialized and highly-skilled professional services consultants, your IQProtector platform engine deployment can be fully operational in a matter of weeks. The Quick Start Program reduces the risk of network disruption and provides you peace of mind. For deployments of five or fewer discovery/classification/protection use cases, the Quick Start Program is the ideal choice for a timely, effective product installation.

On-Site Consulting and Implementation
Secure Islands provides on-site assistance with custom and large deployments, or other activities not covered under Secure Islands' standard program. Secure Islands consultants know to ask the right questions, and—especially—to listen carefully to the answers. Secure Islands and HP will work with clients on solutions for today's needs and for expansion as you grow or change.

Our on-site consulting services are customized to address specific business needs and include:

- Planning and design—Successful deployments start with effective planning. By relying on a Secure Islands consultant, your deployment will get off to the best possible start. Secure Islands consultants help prepare every aspect of your deployment and network security solutions—from the initial planning stages through implementation. Our qualified team will thoroughly review your business goals, application architecture and security requirements, creating a comprehensive deployment plan that is tailored to your organizational IT requirements.
- Configuration and implementation—HP Atalla and Secure Islands create relationships with our clients, learn their business, and adapt our technology to maximize results.

  Secure Islands consultants are extensively trained in all aspects of the HP Atalla IPC products and solutions. Employing their knowledge and experience with the internal workings of our product family, our consultants will help you configure and adjust the technology so that it addresses your specific requirements and needs.

- Tuning—As a final step, Secure Islands offers Fine Tuning services to ensure maximum data security and performance for your organization. Consultants will confirm that IQProtector is correctly and efficiently installed to ensure top-level performance. Fine tuning services include the confirmation of proper information profile definitions as well as classification and protection definitions and management.

Microsoft AD RMS Consulting, Planning, and Implementation
With experience in major organizations worldwide, Secure Islands Microsoft AD RMS Planning and Implementation services can help your organization overcome the challenges of rolling out Active Directory Rights Management Services. Secure Islands works with you throughout the process to ensure a successful AD RMS deployment. The range of services offered includes needs analysis, architecture design and planning, full deployment including backup, high availability, performance, and sizing.

Training

Preparing for success
One of the keys to successful implementation of any security solution is the training of the personnel that will run the system on a day-to-day basis. Hewlett-Packard and Secure Islands are committed to giving its customers effective and flexible training support. When taking part in one of our comprehensive training courses, you will find that your concern is our concern.

Expert trainers
Secure Islands' in-house specialists have undergone intensive theoretical and practical study to tailor their knowledge to your needs. Secure Islands trainers will provide you with all the knowledge necessary to ensure rapid implementation, seamless integration, and smooth ongoing operation of all our systems.

Innovative training programs
Secure Islands experts deliver and accredit a range of core training schemes, taking participants from basic level through to advanced skills. Options also incorporate the power and flexibility of e-learning, using a combination of global electronic classrooms, and video conferences. The course details are:

Foundations of IQProtector
Designed for IQProtector customers and system engineers, this is a foundation course for Secure Islands IQProtector. This course includes product presentations and hands-on lab exercises to ensure both product concept understanding as well as practical experience installing, configuring and managing an IQProtector deployment.

Course length: 3 days

Prerequisites:

- Familiarity with Active Directory
- Knowledge of Windows Server and Microsoft SQL Server
- Basic networking knowledge
- Basic data security knowledge

Subjects learned:

- Deploy and manage IQProtector suite
- Audit IQProtector online events
- Define new, simple and complex information profiles
- Use discovery mode correctly

HP Atalla IPC support

HP Atalla IPC support services 24x7

Support is calculated and included as a percentage of the software net term license price.

Specifications for HP Atalla IPC family

	Licensing terms: 1-year and 3-year term licenses, with 24x7 support
IQProtector Agent Platform support	Windows® 7 (32 and 64 bit) Windows® XP Pro (32-bit, SP2 and later) Windows Server 2003 (32 and 64 bit) Windows Server 2008 (32 and 64 bit, excluding Core edition) Windows Server 2008 R2 Windows Server 2012
Minimum hardware requirements	CPU: Intel® Pentium® III 1 GHz or faster RAM: 512 MB Disk space: 250 MB Network connection: TCP/IP for remote access
Microsoft Office support	Microsoft Office 2003 Microsoft Office 2007 Microsoft Office 2010 Microsoft Office 2013
Web file download protection support	Web client/browser of any type (HTTP/HTTPS)
Microsoft Outlook support	Microsoft Outlook 2003 Microsoft Outlook 2007 Microsoft Outlook 2010 Microsoft Outlook 2013
IQProtector Management Server Platform support	Windows 7 (32 and 64 bit)—for a proof of concept only Windows XP Pro (32-bit, SP3 and later)—for a proof of concept only Windows Server 2008 (32 and 64 bit, excluding Core edition) Windows Server 2008 R2 (excluding Core edition)
Server hardware requirements for IQProtector Agent Platform support	CPU: Dual core CPU RAM: 2 GB Disk space: 40 GB Network connection: TCP/IP for remote access
HP Atalla IPC Suite Remote Desktop Services (Citrix/Terminal Services) support	Windows Server 2003 (32 and 64 bit) Windows Server 2008 (32 and 64 bit) Windows Server 2008 R2

Specifications for HP Atalla IPC family (continued)

Database requirements	• SQL Server 2008 SP1 Standard or higher with full text indexing installed. For reporting and dashboard features (IQP Analytics) you must install SQL Server Analysis Services (SSAS), and SQL Server Reporting Services (SSRS). • SQL Server 2008 Express (with advanced services) with full text indexing installed—for a proof of concept only or a SMB configuration • For HP Atalla IPC Bridge for Content Inspection Services (Content Inspection Bridge)—SQL Server 2008 Express (with advanced services) with full text indexing or higher. • For data analytics: SQL Server Integration Services (SSIS), SSAS, and SSRS
System requirements for HP Atalla IPC mobile support for AD RMS	Microsoft Exchange 2010
Supported platforms for HP Atalla IPC mobile support for AD RMS	iOS Android 2 and higher BlackBerry OS 5/6/7/10 Windows
HP Atalla IPC AD RMS Extensions for Outlook Microsoft Windows Platform support	Windows 7 (32 and 64 bit) Windows XP Pro (32-bit, SP2 and later)
HP Atalla IPC AD RMS Extensions for Outlook minimum hardware requirements	CPU: Intel Pentium III 1 GHz or faster
HP Atalla IPC AD RMS Extensions for Microsoft Outlook support requirements	Microsoft Outlook 2003 Microsoft Outlook 2007 Microsoft Outlook 2010 Microsoft Outlook 2013
Additional notes	Microsoft AD RMS is supported today as the primary IRM protection platform for HP Atalla IPC. Support for additional IRM platforms to be added at HP's sole discretion.

Customize your IT lifecycle management, from acquisition of new IT, management of existing assets, and removal of unneeded equipment.
hp.com/go/hpfinancialservices

HP Factory Express

HP Factory Express provides customization and deployment services along with your storage and server purchases. You can customize hardware to your exact specifications in the factory—helping speed deployment. hp.com/go/factoryexpress

Learn more at
hp.com/go/AtallaIPC

4AA5-2724ENW, June 2014

This is an HP Indigo digital print.