ATAIS – Visión y alcance



Preparado por

[Type Customer Name Here]

9/8/2016

Versión 0.1 Draft

Preparado por

**[Update Author in Doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 0.1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabla de Contenidos

[1 Declaración del Problema 1](#_Toc461137144)

[2 Oportunidad de negocio 2](#_Toc461137145)

[2.1 Declaración de Oportunidad 2](#_Toc461137146)

[3 Visión y Alcance del Proyecto 4](#_Toc461137147)

[3.1 Declaración de la Visión 4](#_Toc461137148)

[3.2 Análisis de Beneficios 4](#_Toc461137149)

[3.3 Requisitos 6](#_Toc461137150)

[3.3.1 Requisitos del Negocio 6](#_Toc461137151)

[3.3.2 Requisitos de Usuario 7](#_Toc461137152)

[3.3.3 Requerimientos Operacionales 8](#_Toc461137153)

[3.3.4 Requerimientos de Sistema 8](#_Toc461137154)

[3.3.5 Requerimientos de Seguridad 9](#_Toc461137155)

[3.4 Alcance del Proyecto 10](#_Toc461137156)

[3.4.1 Componentes de la Solución en el Alcance 11](#_Toc461137157)

[3.4.2 Componentes de la Solución Fuera del Ámbito 13](#_Toc461137158)

[3.5 Objetivos 14](#_Toc461137159)

[3.5.1 Objetivos de Negocio 15](#_Toc461137160)

[3.5.2 Objetivos Técnicos 15](#_Toc461137161)

[3.6 Entregables 15](#_Toc461137162)

[3.7 Criterios de Aceptación 17](#_Toc461137163)

[3.8 Criterio Operacional 18](#_Toc461137164)

[4 Estrategia de Diseño 20](#_Toc461137165)

[4.1 Estrategía de Diseño de la Arquitectura 20](#_Toc461137166)

[4.2 Estrategia de Diseño Técnico 21](#_Toc461137167)

[4.2.1 ATA Center 22](#_Toc461137168)

[4.2.2 ATA Gateways 25](#_Toc461137169)

[4.2.3 Port mirroring 32](#_Toc461137170)

[4.2.4 Consideraciones de Port Mirroring 33](#_Toc461137171)

[4.2.5 Integración con SIEM 34](#_Toc461137172)

[4.3 Limitaciones 34](#_Toc461137173)

[4.4 Análisis de Uso 35](#_Toc461137174)

[4.4.1 Perfiles de Usuarios 35](#_Toc461137175)

[4.4.2 Escenarios de Uso 36](#_Toc461137176)

[5 Apendice 38](#_Toc461137177)

[5.1 Resumen: Como ATA proporciona servicios de detección 38](#_Toc461137178)

[5.2 Beneficios potenciales principales de la tecnología ATA 39](#_Toc461137179)

Tabla de Figuras

[Figura 1 Arquitectura conceptual de ATA 20](#_Toc461137180)

[Figura 2: Flujo de captura de datos de red de ATA 32](#_Toc461137181)

[Figure 3: Beneficios potenciales principales 39](#_Toc461137182)

Tabla de Tablas

[Tabla 1: Requisitos del negocio 7](#_Toc461137848)

[Tabla 2: Requisitos del usuario 7](#_Toc461137849)

[Tabla 3: Requisitos operacionales 8](#_Toc461137850)

[Tabla 4: Requisitos del sistema 8](#_Toc461137851)

[Tabla 5: Requisitos de seguridad 9](#_Toc461137852)

[Tabla 6: Componentes del alcance de la solución 11](#_Toc461137853)

[Tabla 7: Componentes de la solucion: Fuera de alcance 14](#_Toc461137854)

[Tabla 8: Entregables del proyecto 15](#_Toc461137855)

[Tabla 9: Criterios de aceptación 17](#_Toc461137856)

[Tabla 10: Criterio operacional 18](#_Toc461137857)

[Tabla 11: Componentes de la solución de la estrategia del diseño arquitectónico 21](#_Toc461137858)

[Tabla 12: Roles de la solución: ATA Center 22](#_Toc461137859)

[Tabla 13: Hardware de ATA Center 22](#_Toc461137860)

[Tabla 14: Requerimientos: Dimensionamiento de ATA Center 23](#_Toc461137861)

[Tabla 15: Requerimientos: Puertos de red de ATA Center 24](#_Toc461137862)

[Tabla 16: Requerimientos: software de ATA Center 24](#_Toc461137863)

[Tabla 17: Roles de la solución: ATA Gateway 25](#_Toc461137864)

[Table 18: Requirements: Lightweight Gateway hardware 26](#_Toc461137865)

[Tabla 21: Requerimientos: Puerto de red de ATA Lightweight Gateway 27](#_Toc461137866)

[Tabla 19: Requerimientos: Hardware de ATA Gateway 28](#_Toc461137867)

[Tabla 20: Requerimientos: Dimensionamienot de ATA Gateway 29](#_Toc461137869)

[Tabla 21: Requerimientos: Puerto de red de ATA Gateway 29](#_Toc461137870)

[Tabla 22: Requerimientos: Software de ATA Gateway 30](#_Toc461137871)

[Tabla 23: Consideraciones de Port-mirroring 33](#_Toc461137872)

[Tabla 24: Limitaciones 35](#_Toc461137873)

[Tabla 25: Perfiles de usuarios 36](#_Toc461137874)

[Tabla 26: Escenarios de uso 37](#_Toc461137875)

**Spell/grammar check is turned ON within all Services Delivery Method (SDM) Word templates.** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click **File**.
2. Click **Options** on the left.
3. Click **Proofing**.
4. Scroll to the bottom and check the following boxes:



**To remove all the Visible Guidance (hot pink text with gray background) all at once:**

1. Press **Ctrl-H** and, in the **Find and Replace** dialog box, place the cursor is in the **Find what** box.
2. In the bottom left, click **More**.
3. On the **Format** menu, in the bottom left, click **Style**.
4. In the **Find Style** dialog box, scroll down to the bottom and click **Visible Guidance**, and then click **OK**.
5. In the **Find and Replace** dialog box, make sure the **Replace with** box is empty.
6. Click **Replace All**.
7. If not empty, click **Format**, click **Style**, select **(no style)**, click **OK**, and then click **Replace all** again.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

**Save as PDF** and send the PDF version to the customer.   
~ OR ~

Inspect the document and **remove comments, revisions, any document properties** you do not want included, personal information, and hidden text. For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

**Template Guidance**

**Description:** The Vision/Scope document represents the ideas and decisions developed during the Envisioning phase. The goal of the phase, represented by the content of the documentation, is to achieve team and customer agreement on the desired Solution and overall project direction (i.e., project goals, constraints, etc.)

The Vision/Scope document is organized into three main sections:

**Business Opportunity**: A description of the customer’s situation and needs

**Scope:** The boundary of the Solution defined though the range of features and functions that can be accomplished within project constraints; what is out of scope, a release strategy and the criteria by which the Solution will be accepted by users and operations.

**Solution Design Strategies:** The architectural and technical designs used to create the customer’s Solution within the project constraints

**Note:** In this template, you must enter specific project information in certain placeholder areas. To view the fields containing these placeholders:

1. Click on **File** and, in the left pane, click **Options**.
2. In the left pane, click **Advanced** and, in the **Advanced** pane, scroll down to the **Show document content** section.
3. In the **Field shading** menu, click **Always**.
4. Click **OK**.

Throughout the template, look for shaded text. Where shaded text appears, click the field and follow instructions.

Depending on the complexity of the project, not all of the sections might be filled out, or some sections might be cut back significantly.

**Justification:** Vision/Scope documentation is usually written at the strategic level of detail and is used during the Planning phase as the context for developing more detailed technical specifications and project management plans. It provides clear direction for the project team; outlines explicit, up-front discussion of project goals, priorities and constraints; and sets customer expectations.

**Team Role Primary:** Product Management is the key driver of the Envisioning phase and is responsible for facilitating the team to the Vision/Scope approved milestone. Product Management defines the customer needs and business opportunity or problem addressed by the Solution.

**Team Role Secondary:** Program Management is responsible for articulating the Solution Concept, Goals, Objectives, Assumptions, Constraints, Scope and Solution Design Strategies sections of this document.

1. Declaración del Problema

**Guidelines for a Problem Statement**

**Purpose:** Provides the business description of the customer’s situation, outlining the motivation for the project

**Responsibility:** Product Management

**Length:** Less than one page, ideally a paragraph

**Guidelines:** Stay at a high level, use clear business language; address why you want to do it and what you want to do; look at known issues

Hoy en día, el tópico de ciberseguridad ha pasado de TI y el Datacenter llegando a los niveles superiores de la organización. Los ataques y amenazas han crecido substancialmente, siendo más sofisticados en frecuencia y severidad. ¿Qué está en Juego? Todo, desde la privacidad de los clientes hasta la identidad de la marca, la reputación ejecutiva y más allá.

Sin un sistema de detección poderoso, los resguardos efectivos y los procesos de control al plan de respuesta, podrían ocurrir muchas cosas. Las identidades de las personas podrían verse comprometidas, las empresas podrían perder clientes como resultado del daño a su reputación y, además, podrían perder el control de los secretos comerciales y la propiedad intelectual (incluso podrían perder su ventaja competitiva en el mercado).

Los atacantes han demostrado que pueden residir dentro de una red un promedio de 8 meses antes que ellos sean detectados. En la gran mayoría de los ataques, los atacantes comprometen las credenciales de usuario y usan cada vez herramientas TI más legítimas en vez de los malware.

En el entorno moderno actual de TI, el reconocimiento de los siguientes elementos de amenaza[[1]](#footnote-2) es imperativo para la organización:

* Antes de ser detectados, los atacantes permanecen en una red más de **140 días** en promedio
* El cibercrimen le cuesta a la economía mundial un estimado de **US$500 mil millones**.
* **Sobre el 60%** de las intrusiones de red están relacionadas con credenciales comprometidas.
* Una violación de datos le cuesta a una empresa un promedio de **US$3,5 mil millones**.

1. Oportunidad de negocio

In this section, write a statement of the customer’s situation, expressed in business language rather than technical terms. This section should demonstrate Microsoft’s understanding of the customer’s current environment and its desired future state. This information is the overall context for the project.

Las herramientas de Seguridad tradicionales entregan una protección limitada contra ataques de ciberseguridad sofisticados, como cuando ocurre el robo de credenciales de usuarios. La configuración inicial, crear reglas, y la sintonía fina son engorrosos y podrían tomar años. Cada día, los clientes reciben distintos reportes de falsos positivos y los clientes no tienen recursos para revisar esa información y si lo hacen, podrían no entender que significan esos datos. Esas herramientas son tradicionalmente diseñadas para ayudar a proteger el perímetro, para intentar detener el acceso de los atacantes. Hoy, el complejo escenario de la ciberseguridad, hace que se requiera un enfoque diferente.

Como resultado de este proyecto [Type Customer Name Here] tiene la oportunidad de ser educado sobre las amenazas más recientes que Microsoft Advanced Threat Analytics (ATA) detecta y en cómo construir un plan efectivo para responder a esos indicadores de amenazas que ATA descubre. Este proyecto se enfoca en la arquitectura y despliegue de ATA dentro de la compañía [Type Customer Name Here] para complementar y mejorar su estrategia de detección.

* 1. Declaración de Oportunidad

Describe the customer’s current situation that creates the need for the project. You may include a statement of the customer’s opportunity and the impact of capitalizing on that opportunity (product innovation, revenue enhancement, cost avoidance, operational streamlining, and leveraging knowledge). You may also include a statement of the customer’s problem/situation and the impact of solving the problem or how the Solution will create business value (revenue protection, cost reduction, regulatory compliance, alignment of strategy and technology). Include a statement that connects the customer’s opportunity/problem to the relevant business strategy and drivers. Write the Opportunity Statement concisely using a business executive’s voice.

**Justification:** The Opportunity Statement demonstrates that Microsoft understands the customer’s situation from the business point of view and provides the project team and other readers with the strategic context for the remaining sections.

ATA podría proporcionar una manera más rápida y simple para [Type Customer Name Here] de comprender que está sucediendo dentro de su red identificando actividades sospechosas a través del uso del *Análisis de Comportamiento de Usuarios y Entidades* (por su significado en inglés, UEBA) y proporciona información de amenazas clara y relevante en una simple línea de tiempo de ataques.

Esta solución se enfoca en la detección y en como [Type Customer Name Here] responderá a las amenazas que detecta ATA. Tener un plan de respuesta efectivo para los indicadores de amenazas preparará a [Type Customer Name Here] para que responda apropiadamente basado en la severidad de la amenaza descubierta. También le ayudará a [Type Customer Name Here] para que pueda priorizar las amenazas basado en un entendimiento de las mismas como respuesta al resultado del ejercicio de planeación que es parte de este proyecto.

1. Visión y Alcance del Proyecto
   1. Declaración de la Visión

**Guidelines for a Vision Statement**

**Purpose:** Establish the long-term vision and provide design-making content. Provide unbounded view of the Solution.

**Responsibility:** Product Management

**Length:** One paragraph or even a sentence fragment.

**Guidelines:** Balance all the interests to arrive at a single vision statement; surface enterprise architecture implications early.

Clearly and concisely, describe the future desired state of the customer’s environment once the project is complete. This can be a restatement of the opportunity; however, it is written as if the future state has already been achieved. This statement provides a context for decision-making. It should be motivational to the project team and the customer.

**Justification:** A shared vision statement among all team members helps help make sure that the Solution meets the intended goals. A solid vision builds trust and cohesion among team members, clarifies perspective, improves focus, and facilitates decision-making.

ATA prepara a [Type Customer Name Here] para que pueda detectar amenazas que son actividades maliciosas destinadas a las credenciales de Active Directory Domain Services (Active Directory (AD DS). La visión de este proyecto es implementar capacidades de detección de amenazas, identificar amenazas contra las credenciales de usuarios y entidades y preparar a la organización para responder efectivamente a las amenazas identificadas con ATA.

Microsoft asistirá a [Type Customer Name Here] en el logro de esta visión educando, preparando, diseñando e implementando la solución ATA.

* 1. Análisis de Beneficios

Describe how the customer will derive value from the proposed Solution. Connect the business goals and objectives to the specific performance expectations realized from the project. These performance expectations should be expressed numerically. This section could be presented using the following subsections:

1. Business Goals and Objectives
2. Business Metrics
3. Business Assumptions and Constraints
4. Benefits Statement

**Justification:** Benefits Analysis demonstrates that Microsoft sufficiently understands the customer’s situation. It also defines the customer’s business needs, which may provide vital information for making Solution/technology recommendations. Modify this section or elaborate if you feel this information is not suitable for your customer.

ATA automáticamente analiza, aprende e identifica comportamientos de autenticación anormales sobre la red, alertándolo sobre posibles indicadores de compromiso. Microsoft Services implementará un diseño bien planeado de la solución y [Type Customer Name Here] tendrá la confianza para entender la severidad de los indicadores que ATA entrega y poder responder adecuadamente.

Durante el curso de este proyecto, se pueden obtener los siguientes beneficios:

**Descubrimiento de comportamiento anormal de usuario:** Usando análisis de comportamiento y *machine learning*, ATA descubrirá actividades cuestionables y comportamientos anormales, tales como conexiones extrañas, acceso a los recursos anómalos, acceso a los recursos y horas de trabajo anormales, contraseñas compartidas y movimiento lateral.

**Identificación de ataques maliciosos:** ATA detecta ataques maliciosos conocidos casi inmediatamente, incluyendo *Pass the Ticket*, *Pass the Hash*, *Overpass the Hash*, *forged PAC (Microsoft Security Bulletin 14-068)*, *Golden Ticket*, malware *Skeleton Key*, reconocimiento, fuerza bruta, y ejecución remota.

**Identificación de riesgos y problemas de seguridad:** ATA identifica problemas de seguridad tales como *Broken Trust* y vulnerabilidades conocidas de protocolos.

**Entrega un diseño sensible e implementación considerada:** Siguiendo el *Microsoft Solution Framework* (MSF), Microsoft Services preparará un diseño e implementación bien planeada y segura.

**Comprensión y respuesta al comportamiento de los atacantes:** La metodología de ATAIS permitirá educar en las amenazas específicas que ATA detecta y cómo responder apropiadamente a ellas, permitiendo que se tomen decisiones más informadas sobre mitigaciones y se pueda desarrollar una estrategia de detección de amenazas a largo plazo.

**Desarrollo e integración del plan de respuesta específico de ATA:** Microsoft Services ayudará a entender los indicadores sospechosos descubiertos por ATA, las acciones de respuesta necesarias y como integrarlas en el plan de respuesta existente.

* 1. Requisitos

Identify what the Solution must do. These requirements can be expressed in terms of functionality (for example, a registration website Solution will allow the users to register for events, arrange for lodging, and so on) and the rules or parameters that apply to that functionality (for example, the user can register only once and must stay in lodging approved by the travel department). Requirements exist at both the user level and the organizational level. Note the [Requirements Document](https://spsites.microsoft.com/sites/bizdesk/SDMPlus/SDM%20TemplateDL/RequirementsDocument.docx) is also available if a separate document is needed to document requirements. This is often the case in projects with larger scopes and greater complexity. For smaller projects, this Vision Scope document will likely suffice and this document can be considered optional.

**Justification:** User and organizational requirements are the key input to developing product scope and design strategies. Requirements are the bridge between the usage analysis and Solution description. A complete Statement of Requirements demonstrates that Microsoft understands its customer’s needs. The statement also becomes the baseline for more detailed technical documentation in the Planning phase. Good requirements analysis lowers the risk of downstream surprises.

BR = Business Requirement

UR = User Requirements

OR = Operational Requirements

TR = Technical Requirement, which is where all ATA requirements would be

SR = Security Requirements

La siguiente sección describe los requisitos de la solución que serán entregados en este proyecto.

* + 1. Requisitos del Negocio

Business requirements define the needs of the organization with regard to the Solution. They define what the Solution must deliver to capitalize on a business opportunity or to manage business challenges. Modify the section below.

Este proyecto contempla los requerimientos de negocio de la compañía referentes a las necesidades de detección de amenazas. Es imperativo que [Type Customer Name Here] entienda sus objetivos y retos. Estos variarán basados en muchos factores, pero algunas áreas comunes que [Type Customer Name Here] podría requerir, incluyen:

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. **Please add rows and update or change to your needs.**

Tabla 1: Requisitos del negocio

| Código de Identificación | Requerimiento |
| --- | --- |
| BR1 | Mejorar el proceso existente del plan de respuesta. |
| BR2 | Activar una estrategia de detección de amenazas más robusta. |
| BR3 | La solución debe plantear un riesgo mínimo para el ambiente y el bienestar operativo de la empresa. |
| BR4 | Microsoft necesita revisar y proporcionar información para el plan de respuesta de [Type Customer Name Here] relacionado con las detecciones de ATA. |

* + 1. Requisitos de Usuario

User requirements address individual or groups of users. These have a special focus on information delivery mechanisms (for example, dashboards, reports, ad-hoc navigation). Modify this section based on your customer requirements.

La siguiente tabla describe los requerimientos de usuario que deben ser considerados durante todas las etapas de este proyecto.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Tabla 2: Requisitos del usuario

| Código de Identificación | Requerimiento |
| --- | --- |
| UR1 | [Type Customer Name Here] identificará administradores de la solución |
| UR2 | La solución debería hacer uso de cuentas de usuarios estándar, sin privilegios. |
| UR3 | Una cuenta de usuario *honeytoken* es opcional para la solución. Una cuenta para un usuario que no tenga actividades en la red será configurada como el usuario *honeytoken* de ATA. Para configurar el usuario *honeytoken*, se necesitará el identificador de seguridad (SID) de la cuenta de usuario, no el nombre de usuario. |
| UR4 | La solución requiere una cuenta de servicio. |

* + 1. Requisitos Operacionales

Provide an overview of the needs for the Solution from the perspective of operations and IT, that is, to make sure that the Solution can be deployed and operated successfully alongside other systems. Operational requirements describe the qualities of service that must be supported, such as security, performance, and availability. Elaborate in the section and tables below.

La siguiente tabla describe los requerimientos operacionales que deben ser considerados durante todas las fases de este proyecto.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Tabla 3: Requisitos operacionales

| Código de Identificación | Requerimiento |
| --- | --- |
| OR1 | Microsoft necesita proveer una guía operacional clara a [Type Customer Name Here] durante las fases de Visión, Planificación, Construcción, estabilización y Despliegue. |
| OR2 | Una orientación clara de las copias de Seguridad debe formar parte de la excelencia operativa de la solución. |
| OR3 | Microsoft debe proporcionar una guía de implementación clara a [Type Customer Name Here], para que pueda reinstalar la solución si fuera necesario. |

* + 1. Requisitos de Sistema

La siguiente tabla describe los requerimientos de sistema que deben ser considerados durante todas las fases de este proyecto.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Where there are options, select the appropriate text and delete the non-relevant option.

Tabla 4: Requisitos del sistema

| Código de Identificación | Requerimiento |
| --- | --- |
| SR1 | Opción 1: El sistema necesita ser implementado en una plataforma virtualizada.  Opción 2: El sistema necesita ser implementado en una plataforma física. |
| SR2 | Contar con el almacenamiento necesario disponible basado en la visión de la estrategia técnica de diseño. |
| SR3 | Contar con las especificaciones de hardware adecuadas disponibles basado en la visión de la estrategia técnica de diseño. |
| SR4 | Opción 1 (Lightweight Gateway): La solución será desplegada usando hardware mínimo asumiendo un enfoque basado en agentes donde sea posible.  Opción 2 (port-mirrored gateway): La solución será desplegada de una manera en que no se añadan recursos de cómputo a los sistemas existentes.  Opción 3 (combinación de Lightweight Gateway y Port Mirrored Gateways): Cuando sea posible, la solución será desplegada con costos e impactos mínimos a los sistemas existentes. |

* + 1. Requisitos de Seguridad

Identifying the security requirements is the first step to help ensure the security of the proposed Solution. The security requirements can be used to direct the following subsequent security activities:

Focus on what to look for in the Threat Modeling activity.

Focus on what to concentrate on for the Security Code Review and Inspection.

What areas to be aware of when doing the Secure Deployment activity.

What concerns may have to be addressed in the Security Response Plan.

The primary architect and Security SME should use the security requirements section of the Security Architecture document to state the Solution’s security requirements.

La siguiente tabla describe los requerimientos de seguridad que deben ser considerados durante todas las fases de este proyecto.

Tabla 5: Requisitos de seguridad

| Código de Identificación | Requerimiento |
| --- | --- |
| SECR1 | La fase de educación preparará a [Type Customer Name Here] para entender el indicador de amenazas específicos que ATA descubre. |
| SECR2 | El plan de respuesta y los talleres le ayudarán a [Type Customer Name Here] a entender, identificar y priorizar los indicadores de amenaza y responder apropiadamente. |
| SECR3 | Comunicaciones con la administración del portal deberían ser encriptadas. |
| SECR4 | Comunicaciones entre el Center y el Gateway deberían ser encriptadas. |
| SECR5 | Opción (despliegue port-mirrored gateway): Cuando sea posible, el servicio de detección debería permanecer invisible (oculto) de atacantes potenciales en una manera que el servicio de detección no muestre los agentes ejecutándose en los sistemas. |

* 1. Alcance del Proyecto

Guidelines for a Scope Statement

**Purpose:** Map reality against the vision and establish what the customer deems to be essential for success that can be accomplished within the project’s constraints. Shift less essential features into future releases.

**Responsibility:** Program Management

**Length:** As succinct as possible (one to two pages).

**Guidelines:** Be SMART (Specific, Measurable, Achievable, Results-based, Time-oriented). Clearly state what is out of scope.

Place a boundary around the Solution by detailing the range of features and functions, by defining what is out of scope (what will not be part of the project or not being completed by Microsoft Services; be as specific as possible and don’t assume that something is understood), and by discussing the criteria by which the Solution will be accepted by users and operations. The scope clearly delineates what stakeholders expect the Solution to do, thus making it a basis for defining project scope and for performing many types of project and operations planning.

**Instructions:** Replace these with the appropriate items as listed within the “Objectives” and “Services Areas within Scope” sections located within the Statement of Work for your project. Make sure to adjust any in- or out-of-scope items based upon your Envisioning workshops. Note that all changes must go through the formal change-management process and must be approved to be contained within the Vision and Scope document.

El alcance del proyecto consiste del conocimiento y evaluación, visión, planificación y desarrollo de ejercicios y análisis y entrevistas con los participantes de las áreas funcionales. Esto culmina en la entrega de una implementación y ejecución de ciberseguridad que se adapta a la misión singular o requerimientos de negocios y prioridades de [Type Customer Name Here].

La siguiente sección describe los elementos del alcance de este proyecto. Específicamente, este proyecto proveerá un entendimiento de las amenazas sobre las que ATA puede entregar servicios de detección para asistir en la creación de un plan de respuesta específico a los eventos que ATA puede identificar y asistir con el diseño y la implementación de ATA para monitorear las amenazas al ambiente de producción AD DS de [Type Customer Name Here].

* + 1. Componentes de la Solución en el Alcance

Review this scope section with care. Elaborate more on or remove the elements mentioned below.

Los siguientes elementos se consideran incluidos en el alcance cuando se prepara el diseño y la implementación de ATA para proveer servicios de detección de amenazas en el ambiente de producción AD DS de [Type Customer Name Here]. Los elementos del alcance deberían alinearse al documento de *Statement of work* (SOW).

La siguiente tabla detalla los elementos específicos que incluye el alcance de este soporte.

Tabla 6: Componentes del alcance de la solución

|  |  |  |
| --- | --- | --- |
| Componente de la solución | Descripción o consideraciones | Supuestos del alcance |
| Talleres de capacitación | Microsoft realizará tres talleres de capacitación que se centrarán en los siguientes temas (un taller por tema):   * Comprensión del marco de seguridad cibernética * Taller de escenarios de robo de credencial * Taller de información técnica general y avanzada de Advanced Threat Analytics. | * El personal responsable de tomar decisiones en caso de que ATA detecte una amenaza debe asistir a estas sesiones. * El personal responsable del diseño, la implementación y la operación de ATA debe asistir a estas sesiones. |
| Talleres de planificación de respuesta de ATA | Microsoft realizará cuatro talleres, durante los cuales el personal de Microsoft ayudará a crear un plan de respuesta específico para los eventos que ATA pueda identificar. Los talleres incluirán los siguientes temas (un taller por tema):   * Identificación del equipo de respuesta y definición de responsabilidades * Definición y clasificación de eventos de ATA * Manejo de eventos de ATA y definición del proceso de respuesta * Definición del proceso de comunicación en la organización | El personal responsable de determinar lo siguiente debe asistir a los talleres:   * Identificación del equipo de respuesta y definición de responsabilidades * Definición y clasificación de eventos de ATA * Manejo de eventos de ATA y definición del proceso de respuesta * Definición del proceso de comunicación en la organización |
| Plan de respuesta de ATA | Microsoft brindará un documento con el plan de respuesta de ATA, confeccionado en Microsoft Word, que reflejará las decisiones que se tomaron durante los talleres de planificación de respuesta de ATA. | El documento preliminar se compartirá con [Type Customer Name Here] durante una reunión de revisión donde se recibirán comentarios sobre el mismo. Microsoft tendrá en cuenta estos comentarios y realizará las actualizaciones acordadas para crear la versión final que se entregará a [Type Customer Name Here]. |
| Talleres de diseño de ATA | Microsoft conducirá un taller de diseño que se utilizará para determinar el diseño específico de ATA necesario para abordar la solución dentro de alcance. | El personal de BCI necesario debe asistir a estas reuniones. Durante estas reuniones se tomarán decisiones que afectarán el diseño final. |
| Diseño de la solución | Microsoft proveerá un documento con el diseño de la solución, en Word, que detallará el diseño de ATA que se implementará para el alcance de este proyecto. | El documento preliminar se compartirá con BCI durante una reunión de revisión donde se recibirán comentarios sobre el mismo. Microsoft tendrá en cuenta estos comentarios y realizará las actualizaciones acordadas para crear la versión final que se entregará a BCI. |
| Taller de planificación de pruebas | Microsoft conducirá un taller para definir los casos de prueba del sistema y los casos de prueba de validación de la configuración de ATA. | El personal que define los casos de prueba y los procesos asistirá y brindará ideas para el proceso de planificación de pruebas. |
| Planificación de pruebas | Microsoft proveerá una planificación de pruebas, en Word, que detallará los procedimientos de validación y pruebas necesarios para validar la funcionalidad del sistema de ATA. | Este documento se compartirá con BCI durante una reunión de revisión donde se acordará que los casos de prueba deben cumplir con la validación del entorno de implementación. Este documento estará en formato preliminar hasta completar los casos de prueba y documentar los resultados de las pruebas en este documento de planificación de pruebas. |
| Guía de implementación | Microsoft brindará una guía de implementación con los pasos necesarios para instalar y configurar ATA. | El documento preliminar se compartirá con BCI durante una reunión de revisión donde se recibirán comentarios sobre el mismo. Microsoft tendrá en cuenta estos comentarios y realizará las actualizaciones acordadas para producir la versión final que se entregará a BCI. |
| Implementación en producción de ATA | Microsoft ayudará a BCI con la implementación de 3 ATA Centers (1 por forest) y hasta 6 ATA Gateways que monitorearán los bosques de AD DS (bosque nova, bosque corporación BCI y bosque DOM-BCI-PROD) de producción. | Microsoft ayudará a BCI con la implementación de ATA en el entorno de producción. |
| Ajuste de ATA | Microsoft ayudará a BCI con la revisión de los eventos identificados por ATA luego de la instalación durante un máximo de 8 horas y ayudará a abordar las falsas alarmas que se detecten durante este período. | BCI asignará personal operativo que trabajará junto con el equipo de Microsoft para revisar los eventos que ATA capture y para determinar realizar un seguimiento u ocuparse de las falsas alarmas a medida que se produzcan.  Esta ayuda se limita a 8 horas. |
| Guía de operaciones | Microsoft proveerá una guía de operaciones en Word. Este documento proporcionará una guía básica para el mantenimiento de ATA. | El documento preliminar se compartirá con BCI durante una reunión de revisión donde se recibirán comentarios sobre el mismo. Microsoft tendrá en cuenta estos comentarios y realizará las modificaciones acordadas para crear la versión final que se entregará a BCI. |

* + 1. Componentes de la Solución Fuera del Ámbito

Review this scope section with care. The customer must be responsible for configuring their SIEM Solutions. Elaborate more or remove on the elements mentioned below.

Los siguientes elementos son considerados como fuera de alcance en la preparación, diseño e implementación de ATA para proporcionar un servicio de detección de amenazas para el ambiente de producción AD DS de [Type Customer Name Here]. Los elementos del alcance deben estar alineados con lo acordado en el SOW.

La siguiente tabla detalla los elementos específicos que no serán incluidos dentro de los alcances.

Tabla 7: Componentes de la solución: Fuera de alcance

| Solution component | Description and considerations | Scope assumptions |
| --- | --- | --- |
| Plan de Respuesta | Definir un plan de respuesta completo para [Type Customer Name Here]. Microsoft proveerá solo información para el proceso y plan de respuesta existente. | Se asume que [Type Customer Name Here] tiene un plan existente para responder a los elementos que descubra ATA; Microsoft puede ayudar a mejorar este plan. |
| Licencias de Productos | Licencias para Windows Server 2012 R2 (edición Datacenter o Standard) | [Type Customer Name Here] es responsable de obtener todas las licencias de productos. |
| Despliegue de Public key infrastructure (PKI) | Una solución PKI para desplegar certificados. | [Type Customer Name Here] es responsable de todos los requerimientos PKI y la emisión de certificados. |
| Certificados Secure Sockets Layer (SSL) | Emisión de certificados de una PKI interna. Los requerimientos de certificados están descritos en la sección de requerimientos de software de este documento. (Ver requerimientos de software para cada rol de ATA.) | [Type Customer Name Here] responsable de proveer todos los certificados SSL requeridos para implementar ATA. |
| Port mirroring | Configuración de port mirroring. | Si el uso de ATA Gateway es requerido, ATA requiere que *port mirroring* sea configurados entre los *domain controllers* (DC) que serán monitoreados y el correspondiente ATA Gateway. [Type Customer Name Here] is responsible for configuring port mirroring. |
| Integración con Security information and event management (SIEM) | Integración de la información de SIEM hacia y desde ATA | La configuración de la integración entre la información de ATA y del SIEM está fuera del alcance de este proyecto. [Type Customer Name Here] será responsable de seguir la guía de integración en línea para las soluciones de SIEM soportadas. |

* 1. Objetivos

Ver la declaración de visión procedente para el objetivo de este proyecto. La declaración de la visión entrega el contexto para la toma de decisiones durante las etapas posteriores cuando se discutan características, costos y tiempos de entrega. No se entregará un contrato jurídico para la solución. Cualquier revisión de este documento proporciona el alcance detallado de lo que se realizará y lo que no, para cumplir con la declaración de la visión. Las características principales implementadas por la solución estarán de acorde a los siguientes objetivos y metas.

* + 1. Objetivos de Negocio

Describe the business objectives the customer is trying to achieve. Elaborate more on the elements mentioned below.

Los objetivos de negocio de este proyecto serán orientados para la necesidad de [Type Customer Name Here] de contar con un sistema de detección de amenazas que entregue una telemetría útil. La solución incluye lo siguiente:

Implementación de una solución de detección de amenazas que identifique y entregue alertas de potenciales ataques de ciberseguridad sobre las credenciales de AD DS.

Establecer un plan de respuesta para definir como la organización responderá a las amenazas que la solución identifique.

Educar sobre las amenazas comunes que ATA detecta y como priorizar y responder basados en lo descubierto.

* + 1. Objetivos Técnicos

Describe the technical objectives the customer is trying to achieve. Elaborate more on the elements mentioned below.

Este proyecto cumplirá los siguientes objetivos técnicos:

La habilidad de analizar datos desde y hacia los DC, de manera no intrusiva, por medio de port mirroring.

Después de que ATA ha realizado el periodo de aprendizaje (30 días), cualquier desviación en ese periodo podría ser una potencial amenaza de ataque.

Los requerimientos de hardware y software serán configurados para tener el máximo impacto para detecciones efectivas.

* 1. Entregables

La siguiente tabla enumera los entregables de este proyecto.

Tabla 8: Entregables del proyecto

| Fase del proyecto | Nombre del entregable | Descripción del entregable | Críterios de Aceptación |
| --- | --- | --- | --- |
| Visión | Visión y Alcance | Un documento que incluye la visión del proyecto, todos los acuerdos en requerimientos y enfoque del diseño de la solución. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Plan | Plan de Respuesta ATA | Un documento que entrega información acerca de los roles y responsabilidades para responder a los eventos que identifica ATA. También incluye identificación de eventos, clasificación de riesgos y procesos de respuesta y comunicación. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Plan | Diseño de la Solución | Un documento que detalla la configuración técnica de la solución. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Plan | Plan de Prueba Preliminar | Un documento que describe la estrategia y el enfoque usado para planear, organizar y administrar las actividades de pruebas del proyecto. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Construcción | Guía de Implementación | Un documento que incluya las instrucciones paso a paso para implementar ATA en un ambiente de producción. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Construcción | Sistema de Prueba de ATA | La finalización de todos los casos de prueba identificados en el documento de Plan de Pruebas y de acuerdo con los alcances de la solución. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Construcción | Plan de Pruebas Final | Un documento que incluya los resultados finales de todos los casos de prueba y notas para completar cada caso de prueba indicado en el documento. | El documento es entregado y describe con precisión los elementos descritos en esta tabla. |
| Estabilización | Guía de Operación | Un documento que detalla como operar y administrar ATA. | El documento es entregado y describe con precisión los elementos descritos en esta tabla.  Este documento no contiene información o procesos específicos para responder a un evento detectado. Esos elementos están documentados en el Plan de Respuesta de ATA. |
| Despliegue | Implementación | Implementación de la solución. | El despliegue de la solución de acuerdo al Documento de Diseño. |

* 1. Criterios de Aceptación

Define the metrics that must be met in order for the customer to understand that the Solution meets its requirements.

**Justification:** Acceptance criteria communicate to the project team the terms and conditions under which the customer will accept the Solution.

La siguiente tabla describe los criterios de aceptación para un proyecto exitoso.

**Instructions:** Increase the identification codes as you continue to add requirements for future tracking. The following have been provided as an example. Please add rows and update or change to your needs.

Also, you may need to remove specific items if your scope has omitted anything. Read through them carefully to make sure they all apply to your delivery.

Tabla 9: Criterios de aceptación

| Código de Aceptación | Requerimiento |
| --- | --- |
| AC1 | ATA intercepta exitosamente el tráfico de red desde y hacia los DC. |
| AC2 | Los ATA Gateways reúnen exitosamente la información de entidades desde los DC. |
| AC3 | [Type Customer Name Here] entiende completamente cada una de las amenazas que entregan los servicios de detección de ATA. |
| AC4 | [Type Customer Name Here] entiende el Plan de Respuesta de ATA y cómo abordar y priorizar las amenazas descubiertas. |
| AC5 | Un Plan de Respuesta de ATA refleja con exactitud el plan para los eventos que ATA detecte. |
| AC6 | Visión y Alcance: Un documento que refleja de manera precisa el alcance del trabajo que será realizado, los requerimientos de la solución y una estrategia inicial de diseño que será expandida durante la Fase de Planificación. |
| AC7 | Diseño de la Solución: Un documento que registra precisamente la configuración de la visión y despliegue de la solución. |
| AC8 | Plan de Pruebas: Un documento que refleja de manera complete y precisa todos los casos de Prueba que necesitan ser validados para la funcionalidad del sistema. |
| AC9 | Guía de la Implementación: un documento que indica las instrucciones paso a paso para implementar los componentes de ATA que están dentro del alcance. |
| AC10 | Guía de Operaciones: Un documento que contiene la información operacional específica para operar y administrar ATA. |
| AC11 | Transferencia de conocimientos informal durante el proyecto de los elementos de diseño, implementación y pruebas de ATA. |

* 1. Criterio Operacional

Define the conditions and circumstances by which the customer’s operations team determines that the Solution is ready to deploy in their production environment. Once deployed, the customer takes ownership of the Solution. This section may specify the customer’s requirements for installing the Solution, training operators, diagnosing and managing response plans, and so on.

**Justification:** Operational criteria communicate to the project team the terms and conditions under which the customer will allow deployment and ultimately sign off on the project. This information provides a framework for planning the Solution’s deployment.

La siguiente tabla resume los criterios operacionales para un proyecto exitoso.

Tabla 10: Criterio operacional

| Código de Identificación | Requerimiento |
| --- | --- |
| OC1 | Los administradores de ATA pueden acceder a la consola de ATA. |
| OC2 | La consola de ATA muestra las actividades sospechosas detectadas en la línea de tiempo de ataques. |
| OC3 | ATA alerta a los administradores permitidos para interactuar y facilitar la entrada y reconocimiento humano. |
| OC4 | ATA pone a disposición alertas de estado de salud. Por ejemplo, cuando la comunicación entre el Gateway y el Center es interrumpida o cuando la cuenta de usuario que es utilizada para catalogar identidades expira en el AD. |
| OC5 | La solución permite la exclusión de subredes arrendadas a corto plazo, tales como VPN, herramientas de prueba de subredes internas o direcciones IP de Wi-Fi. |
| OC6 | [Type Customer Name Here] puede copiar y restaurar la base de datos de ATA. Puede también mover la base de datos a otro disco o volumen. |

1. Estrategia de Diseño
   1. Estrategía de Diseño de la Arquitectura

**Instructions:** Describe how the features and functions will operate together to form the Solution. Identify the specific components of the Solution and their relationships. A diagram illustrating these components and relationships is an excellent communication device.

**Justification:** The Architectural Design Strategy converts the list of features and functions into the description of a fully functional, integrated environment. This information enables the customer to visualize the Solution in its environment. It may drive the selection of specific technologies. The Architectural Design Strategy is key input to the design specification. Update the diagram below to reflect your customer’s proposed architecture.

El siguiente diagrama contempla la arquitectura propuesta de ATA.



Figura 1 Arquitectura conceptual de ATA

La figura 1 muestra el diseño teórico que será considerado para la implementación de ATA de [Type Customer Name Here]. Es importante tener en cuenta que el diseño actual, que reúne los requerimientos y necesidades de [Type Customer Name Here], se establecerá durante los talleres de diseño de la solución como parte de la Fase de Planificación.

La siguiente tabla contiene los elementos que serán usados para los propósitos de este diseño.

**Instruction:** Update the following text to provide specifics about your customer’s envisioned ATA deployment. While you will not know specifics, you will be able to explain how many ATA Center deployments you will need (1 per AD DS forest) and talk about the gateway role.

Tabla 11: Componentes de la solución de la estrategia del diseño arquitectónico

|  |  |
| --- | --- |
| Componente de la Solución | Justificación |
| ATA Center | Se implementará un ATA Center para entregar servicios de detección para los siguientes *forest*:  **Instruction:** Update this cell to list the total number of ATA Center deployments and each forest name that the project will provide detection services for. |
| ATA Lightweight Gateway | ATA Lightweight Gateways será desplegado en todos los DC para monitorear, analizar y reenviar toda la actividad de la red relevante para ATA.  **Instruction:** Update this cell with a complete list of all DCs and site locations where an ATA Lightweight Gateway will be deployed. |
| ATA Gateway | ATA Gateways serán desplegarán para monitorear los DC en las siguientes ubicaciones:  **Instruction:** Update this cell with a complete list of all site locations where an ATA Gateway will be deployed to monitor DCs. An ATA Gateway deployment will be required in the same network segment (VLAN) as any DC that is in scope for this project. |

* 1. Estrategia de Diseño Técnico

Esta sección entrega detalles específicos para los requerimientos y configuraciones de ATA. La información de esta sección se entrega para ayudar al diseño técnico de la solución como parte de la Fase de Planificación de este proyecto. La información es para que [Type Customer Name Here] pueda revisar y entender y de esta forma preparar a sus equipos adecuadamente para las discusiones en los talleres de diseño.

* + 1. ATA Center

Esta sección cubre los requerimientos del Center. Las configuraciones y diseño detalladas son registradas en el documento. La siguiente tabla indica las tareas que realiza el ATA Center.

Tabla 12: Roles de la solución: ATA Center

|  |  |
| --- | --- |
| Rol | Descripción |
| Center | * Administra las configuraciones de ATA Gateway * Recibe información desde los ATA Gateways * Detecta actividades sospechosas y es responsable de UEBA * Soporta múltiples ATA Gateways * Ejecuta la consola de ATA |

System requirements address the hardware and operating system needs. Ensure that the appropriate capacity planning has been done to help make sure the storage requirements reflect the amount of traffic from the DCs and is adequate.

* + - 1. Hardware de ATA Center

El ATA Center requiere un mínimo de 30 días de información para el comportamiento analítico de usuarios. La siguiente tabla define el espacio requerido para la base de datos de ATA por DC. Si existen múltiples DC, se debe agregar el espacio en disco requerido por DC para calcular el monto total del espacio requerido para la base de datos de ATA.

El número de DC que [Type Customer Name Here] esté monitoreando y la carga de cada uno de esos DC determina los requerimientos de hardware.

La siguiente tabla resume los requisitos base de hardware para el ATA Center.

Tabla 13: Hardware de ATA Center

| Componente | Requerimientos de hardware para ATA Center |
| --- | --- |
| Procesador | Ver sección de tamaño de ATA Center. |
| Memoria | Ver sección de tamaño de ATA Center. |
| Espacio de disco disponible  Almacenamiento de Base de Datos | Ver sección de tamaño de ATA Center. |
| Red | La comunicación entre el ATA Center y el ATA Gateway es encriptada usando SSL sobre el puerto 443. Adicionalmente, la consola de ATA se ejecuta sobre Internet Information Services (IIS) y es asegurada usando SSL sobre el puerto 443. Se requieren **dos direcciones IP**. El servicio de ATA Center se enlazará al puerto 443 a la primera dirección IP y al IIS en el Puerto 443 para la segunda dirección IP. También se deben revisar los puertos de red necesarios, que se listan en la tabla a continuación.  **Nota:** Se debe confirmar una conexión de red estable y efectiva entre el Center y el Gateway. Ver los requerimientos de memoria del Gateway.  **Nota:** Subredes de arriendo de corto plazo  Identificar las subredes en las cuales las direcciones IP son reasignadas entre dispositivos entre un muy corto periodo de tiempo (segundos o minutos). ATA reduce la duración de caché para todas las direcciones IP de las subredes para dar una rápida cabida a la reasignación entre dispositivos. Redes VPN o Wi-Fi son ejemplos comunes de redes con arriendo de corto plazo. |
| Virtualización | La instalación del ATA Center en una máquina virtual es soportado. |
| BIOS | Las bases de datos de ATA requiere que [Type Customer Name Here] DESHABILITE Non-uniform memory access (NUMA) en la BIOS. Algunos sistemas podrían referirse a NUMA como Node Interleaving, en ese caso se debería HABILITAR Node Interleaving. |

* + - 1. Dimensionamiento de ATA Center

El ATA Center requiere un mínimo de 30 días de datos para usar el análisis de comportamiento. La siguiente tabla define el espacio en disco requerido para la base de datos por DC. Si existen múltiples DC, se debe agregar el espacio en disco requerido por DC para calcular el monto total de espacio requerido para la base de datos ATA.

Tabla 14: Requerimientos: Dimensionamiento de ATA Center

| Paquetes por segundos\* | CPU (cores\*\*) | Memoria (GB) | Almacenamiento de DB por día(GB) | Almacenamiento de DC por mes (GB) | IOPS\*\*\* |
| --- | --- | --- | --- | --- | --- |
| 1,000 | 2 | 32 | 0.3 | 9 | 30 (100) |
| 10,000 | 4 | 48 | 3 | 90 | 200 (300) |
| 40,000 | 8 | 64 | 12 | 360 | 500 (1,000) |
| 100,000 | 12 | 96 | 30 | 900 | 1,000 (1,500) |
| 400,000 | 40 | 128 | 120 | 1,800 | 2,000 (2,500) |

\* Promedio diario total de número de paquetes por Segundo desde todos los DC monitoreados por los ATA Gateways.

\*\* Incluye cores Físicos, no cores hyperthreaded.

\*\*\* Operación de Input/output por segundo; números en promedio (números peak)

**Notas:**

El ATA Center puede manejar un máximo acumulado de 400.000 frames por segundo desde todos los DC monitoreados.

El monto de almacenamiento indicado acá son valores netos; debería tenerse encuentra el crecimiento futuro para asegurar que el disco donde reside la base de datos tenga al menos un 20% de espacio disponible.

* + - 1. Puertos de red de ATA Center

La siguiente tabla indica el mínimo de puertos que necesita ATA Center.

Tabla 15: Requerimientos: Puertos de red de ATA Center

| Protocolo | Transporte | Puerto | Desde o Hacia | Dirección |
| --- | --- | --- | --- | --- |
| SSL (comunicaciones ATA) | TCP | 443 | ATA Gateway | Inbound |
| HTTP | TCP | 80 | [Type Customer Name Here] network | Inbound |
| HTTPS | TCP | 443 | [Type Customer Name Here] network and ATA Gateway | Inbound |
| SMTP (opcional) | TCP | 25 | SMTP server | Outbound |
| SMTPS (opcional) | TCP | 465 | SMTP server | Outbound |
| Syslog (opcional) | TCP | 514 | Syslog server | Outbound |

* + - 1. Software de ATA Center

La siguiente tabla ilustra los requerimientos de software de ATA Center.

Tabla 16: Requerimientos: software de ATA Center

| Componente | Requerimientos de software de ATA Center |
| --- | --- |
| Certificados | ATA Center requiere certificados para los siguientes servicios:   * IIS: Certificado de Servidor Web * Servicio de ATA Center: Certificado de autenticación de Servidor |
| Sistema Operativo | Windows Server 2012 R2 Standard o Datacenter |
| Miembro de dominio o workgroup | El ATA Center puede ser instalado sobre un servidor que sea miembro del dominio o de un workgroup |
| Cuenta de usuario | **Administrador local** (no **miembro del dominio**)  **Cuenta de usuario estándar (unida al dominio)**: Agregado como administrador local y al grupo de administradores de ATA |
| Componentes | Los siguientes componentes serán instalados y configurados durante la instalación de ATA Center:   * IIS * MongoDB * Servicio de ATA Center y Sitio IIS de Administración de ATA * Monitor de rendimiento personalizado * Un certificado X.509 es recomendado y debe ser emitido por una PKI interna. Los certificados auto firmados son recomendados solo para ambientes de prueba. |
| Soporte de Navegador | La Consola de ATA se accede por medio de un navegador. Los siguientes navegadores están soportados:   * Internet Explorer 10 * Google Chrome 40 * Ancho de pantalla mínimo con resolución de 1700 pixeles |
| Actualizaciones Microsoft | Se deben instalar todas las actualizaciones de Microsoft en el servidor. |

* + 1. ATA Gateways

ATA tiene dos componentes, el ATA Center y el ATA Gateway. Esta sección discute los requerimientos del gateway.

Se puede desplegar ATA usando una combinación de configuraciones de Gateway: sólo ATA Gateway, sólo ATA Lightweight Gateway o una combinación de ambos. El ATA Lightweight Gateway es recomendado por sobre el ATA Gateway cuando sea posible, mientras los DC cumplan con el dimensionamiento para la instalación (que se muestra en la tabla más abajo). La mayoría de los DC pueden, y deberían, se cubierto por el ATA Lightweight Gateway a menos que el DC no cumpla los requerimientos de la siguiente tabla

Tabla 17: Roles de la solución: ATA Gateway

| Rol | Descripción |
| --- | --- |
| El ATA Gateway y el Lightweight Gateway tienen las mismas funcionalidades. | * Capturar e inspeccionar el tráfico de red de los DC (el tráfico por medio de port mirroring en el caso de ATA Gateway y el tráfico local del DC en el caso del ATA Lightweight Gateway). * Recibir eventos de Windows desde el SIEM o desde servidores Syslog, o desde los DC usando reenvío de eventos de Windows. * Recibir datos sobre usuarios y computadores desde el dominio AD. * Resolver entidades de red (usuarios, grupos y computadores). * Transferir los datos relevantes al ATA Center. * Monitorear múltiples DC desde un único ATA Gateway o monitorear un solo DC desde un ATA Lightweight Gateway. |

System requirements address hardware and operating system needs. Ensure that the appropriate capacity planning has been done to help make sure the storage requirements reflect the amount of traffic to/from the domain controllers and is adequate.

* + - 1. Dimensionamiento de hardware de ATA Lightweight Gateway

Un ATA Lightweight Gateway puede monitorear solo un DC, dependiendo del monto de tráfico de red que el DC genera.

El ATA Lightweight Gateway requiere un mínimo de 2 cores y 6 GB de RAM instalada sobre el DC. Para un rendimiento óptimo, configure **Power Option** del ATA Lightweight Gateway en **High Performance**. El ATA Lightweight Gateway puede ser instalado sobre DC de variadas cargas y tamaños, dependiendo del monto de tráfico de red desde y hacia los DC y los recursos instalados. La siguiente tabla indica los detalles de los tamaños.

Tabla 18: Requerimientos: Hardware del ATA Lightweight Gateway

| Paquetes por segundo\* | CPU (cores)\*\* | Memory (GB)\*\*\* |
| --- | --- | --- |
| 1,000 | 2 | 6 |
| 5,000 | 6 | 16 |
| 10,000 | 10 | 24 |

\*Número total de paquetes por segundo sobre el DC que el ATA Lightweight Gateway está monitoreando.

\*\*Monto total de cores nonhyperthreaded que el DC tiene instalados. Si bien hyperthreading es aceptado para el ATA Lightweight Gateway, cuando se esté haciendo la planificación de la capacidad, se deben considerar los cores físicos.

\*\*\*Monto total de memoria instalada sobre el DC.

**Notas:**

Si el DC no tiene los recursos necesarios que requiere el ATA Lightweight Gateway, el rendimiento del DC no será afectado, pero el ATA Lightweight Gateway podría no operar de la forma esperada.

El ATA Lightweight Gateway puede ser instalado sobre un DC ejecutando Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2.

El DC puede ser un RODC.

El DC no puede ser un servidor Core.

El ATA Lightweight Gateway monitorea el tráfico local sobre todos los adaptadores del DC. Después de la implementación, se puede usar la Consola de ATA para cambiar el adaptador de red que será monitoreado.

* + - 1. Puerto de red del Lightweight Gateway

La siguiente tabla muestra los puertos mínimos que el ATA Gateway requiere que sean configurados sobre el adaptador administrado.

Tabla 21: Requerimientos: Puerto de red de ATA Lightweight Gateway

| Protocolo | Transporte | Puerto | Desde o Hacia | Dirección |
| --- | --- | --- | --- | --- |
| DNS | TCP y UDP | 53 | Servidores DNS | Outbound |
| NTLM over RPC | TCP | 135 | Todos los dispositivos sobre la red | Outbound |
| NetBIOS | UDP | 137 | Todos los dispositivos sobre la red | Outbound |
| SSL | TCP | 443 o el que sea configurado para el servicio Center | ATA Center:  Dirección IP del Servicio Center  Dirección IP IIS | Outbound |
| Syslog (opcional) | UDP | 514 | Servidor SIEM | Inbound |

**Notas:**

Como parte del proceso de resolución que el ATA Lightweight Gateway realiza, los puertos NetBIOS y NT LAN Manager (NTLM) sobre remote procedure call (RPC) necesitan ser abiertos inbound sobre los dispositivos de red desde los ATA Lightweight Gateways.

* + - 1. Requerimientos de Hardware de ATA Gateway

Un ATA Gateway puede monitorear múltiples DC, dependiendo del tráfico de red desde y hacia los DC.

Tabla 19: Requerimientos: Hardware de ATA Gateway

| Componente | Requerimientos de hardware de ATA Gateway |
| --- | --- |
| Procesador | Ver la sección de dimensionamiento de ATA Gateway. |
| Memoria | Ver la sección de dimensionamiento de ATA Gateway. **Nota:** El ATA Gateway utiliza su memoria para almacenar los datos capturados y enviarlos al ATA Center. El valor predeterminado es 1.000.000 entidades y es configurable. Dependiendo de la carga del DC conectado al Gateway, esto puede generar una enorme cantidad de datos.  **Precaución:** Si las comunicaciones entre el ATA Center y el Gateway son interrumpidas, el Gateway usará la memoria como cache, y 1.000.000 de entidades pueden tomar hasta 5 GB de memoria. Una vez que el límite es alcanzado, el Gateway detendrá la recolección de datos hasta que la comunicación sea restaurada con el ATA Center. Dependiendo de la carga del DC, esto puede ser horas o minutos. |
| Espacio disponible en disco | Ver la sección de dimensionamiento de ATA Gateway. Tabla 20: Requerimientos: Dimensionamiento del Gateway |
| Red | El Gateway requiere dos o más adaptadores de red.  **Adaptador de Administración**—será utilizado para comunicaciones sobre la red de la compañía. Este adaptador debería ser configurado con lo siguiente:   * Dirección IP estática que incluya el default gateway. * Servidores DNS preferido y alternativo. * “DNS suffix for this connection” debería ser el nombre DNS del dominio que será monitoreado.   **Adaptador de Captura**—será utilizado para capturar tráfico desde y hacia los DC:   * Configure port mirroring desde el adaptador de captura como el destinatario del tráfico de red del DC. * Configure una dirección IP no ruteable para el ambiente sin default gateway y sin dirección de DNS server. Por ejemplo, 1.1.1.1/32 * Esto confirma que el adaptador de red de captura puede obtener el monto máximo de tráfico y que el adaptador de red de administración es usado para enviar y revivir el tráfico de red requerido.   **Nota:** Subredes de arriendo de corto plazo  Identificar las subredes en las cuales las direcciones IP son reasignadas entre dispositivos entre un muy corto periodo de tiempo (segundos o minutos). ATA reduce la duración de caché para todas las direcciones IP de las subredes para dar una rápida cabida a la reasignación entre dispositivos. Redes VPN o Wi-Fi son ejemplos comunes de redes con arriendo de corto plazo. |
| Virtualización | La instalación del ATA Gateway como una máquina virtual es soportada cuando el DC que está siendo monitoreado también esté siendo ejecutado como máquina virtual sobre el mismo host de virtualización. |

* + - 1. Dimensionamiento del ATA Gateway

Un ATA Gateway puede monitorear múltiples DC, dependiendo del tráfico de red de los DC que están siendo monitoreados.

Tabla 20: Requerimientos: Dimensionamiento de ATA Gateway

| Paquetes por segundo\* | CPU (cores\*\*) | Memoria (GB) |
| --- | --- | --- |
| 1,000 | 1 | 6 |
| 5,000 | 2 | 10 |
| 10,000 | 3 | 12 |
| 20,000 | 6 | 24 |
| 50,000 | 16 | 48 |

\* Número total de paquetes por segundo desde todos los DC que el ATA Gateway está monitoreando durante las horas más ocupadas del día.

\*Monto total de tráfico de port-mirrored del DC no puede exceder la capacidad de la captura del NIC sobre el ATA Gateway.

\*\* Hyperthreading debe estar deshabilitado.

* + - 1. Puertos de red de ATA Gateway

La siguiente tabla lista los puertos mínimos que el ATA Gateway requiere configurar sobre el adaptador de administración.

Tabla 21: Requerimientos: Puerto de red de ATA Gateway

| Protocolo | Transporte | Puerto | Desde o Hacia | Dirección |
| --- | --- | --- | --- | --- |
| LDAP | TCP y UDP | 389 | Domain controllers | Outbound |
| LDAP sobre SSL (LDAPS) | TCP | 636 | Domain controllers | Outbound |
| LDAP a Global Catalog | TCP | 3268 | Domain controllers | Outbound |
| LDAPS a Global Catalog | TCP | 3269 | Domain controllers | Outbound |
| Kerberos | TCP and UDP | 88 | Domain controllers | Outbound |
| Netlogon | TCP and UDP | 445 | Domain controllers | Outbound |
| Windows Time | UDP | 123 | Domain controllers | Outbound |
| DNS | TCP and UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | Todos los dispositivos sobre la red | Outbound |
| NetBIOS | UDP | 137 | Todos los dispositivos sobre la red | Outbound |
| SSL | TCP | 443 | ATA Center:   * Dirección IP servicio ATA Center * Dirección IP IIS | Outbound |
| Syslog (opcional) | UDP | 514 | Servidor SIEM | Inbound |

* + - 1. Software de ATA Gateway

La siguiente tabla resume los requerimientos de software del ATA Gateway.

Tabla 22: Requerimientos: Software de ATA Gateway

| Componente | Requerimientos de software del ATA Gateway |
| --- | --- |
| Certificados | ATA Gateway requiere certificados para los siguientes servicios:   * Un certificado soportando **Server Authentication** es requerido para instalarlo en el computador en el que está instalado el ATA Gateway en el almacenamiento local computer. Este certificado desde ser de confianza del ATA Center. |
| Sistema Operativo | Windows Server 2012 R2 Standard o Datacenter. |
| Miembro de Dominio o workgroup | El ATA Gateway puede ser instalado sobre un servidor que sea miembro de un dominio o de un workgroup. |
| Cuentas de Usuario | **Administrador Local (No unido al dominio)**  **Cuenta de usuario estándar (Unida al dominio)** – Agregada al local Admin y al grupo de Administradores de ATA  **Cuenta estándar de servicio** – Usada para consultar al Active Directory para indexación y catálogo de objetos y entidades. (Conectividad de dominio)  **Cuenta Honeytoken** – SID que utiliza (Opcional) |
| Componentes | Los siguientes componentes son instalados y configurados durante la instalación del ATA Gateway:   * KB 3047154 (no instale KB 3047154 sobre un host de virtualización. Esto podría causar que el port mirroring deje de trabajar apropiadamente.). * Servicio de ATA Gateway. * Microsoft Visual C++ 2013 Redistributable * Monitor de rendimiento personalizado |
| Microsoft updates | Ejecutar Windows Update y asegurarse que todas las actualizaciones **Important** hayan sido instaladas. Antes de instalar ATA Gateway se debe confirmar que la actualización [KB2919355](https://support.microsoft.com/en-us/kb/2919355/) haya sido instalada. Si la actualización no está instalada, instálela antes de la instalación del servicio de ATA Gateway. |

* + 1. Port mirroring

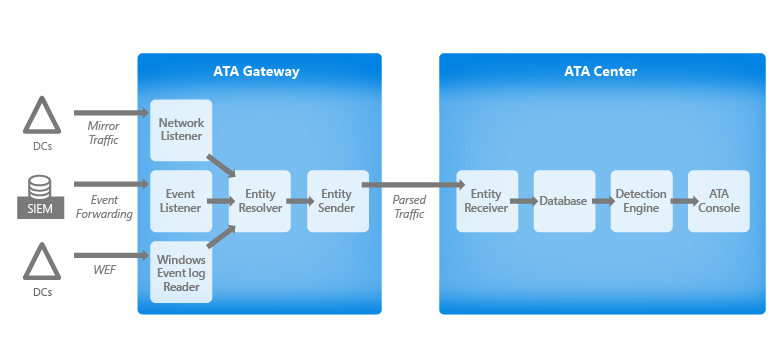


Figura 2: Flujo de captura de datos de red de ATA

La fuente principal de datos que ATA utiliza es una inspección de paquetes en profundidad del tráfico de red desde y hacia los DC de [Type Customer Name Here]. Si no se está implementando un ATA Lightweight Gateway, se debe configurar port mirroring para ATA para ver el tráfico de red. Port mirroring copia el tráfico sobre un puerto, conocido como el *puerto origen* a otro puerto, conocido como *puerto destino*. ATA trabaja con soluciones que pueden espejar el tráfico, si el tráfico puede ser configurado como port mirroring a ATA, este puede ser usado para analizar amenazas a los sistemas de [Type Customer Name Here]. Para configurar port mirroring, revise la documentación del fabricante.

Los DC y ATA Gateways de [Type Customer Name Here] pueden ser Físicos o virtuales.

Los siguientes son los métodos comunes para port mirroring y algunas consideraciones:

**Switched Port Analyzer (SPAN):** Copia el tráfico de red desde uno o más puertos del switch a otro puerto en el mismo switch. El ATA Gateway y los DC deben estar conectados al mismo switch físico.

**Remote Switch Port Analyzer (RSPAN):** Permite a una organización monitorear el tráfico de red desde unos puertos origen distribuidos sobre múltiples switch físicos. RSPAN copia el tráfico de origen en una especial RSPAN-configured virtual LAN (VLAN). Esta VLAN necesita ser acoplada a los otros switch involucrados. RSPAN trabaja en capa 2.

**Encapsulated Remote Switch Port Analyzer (ERSPAN):** Una tecnología propietaria de Cisco que trabaja en capa 3. Con ERSPAN, el usuario puede monitorear el tráfico a través de los switch sin la necesidad de trunks de VLAN. ERSPAN usa un ruteo de encapsulación genérico para copiar el tráfico de red monitoreado. ATA actualmente no puede recibir tráfico directo de ERSPAN. Para que ATA trabaje con tráfico ERSPAN, un switch o router que pueda desencapsular el tráfico necesita ser configurado como una destinación ERSPAN donde el tráfico es desencapsulado. El switch o router entonces necesita ser configurado para reenviar al ATA Gateway usando SPAN o RSPAN.

* + 1. Consideraciones de Port Mirroring

Tabla 23: Consideraciones de Port-mirroring

| ATA Gateway | Domain controller | Considerations |
| --- | --- | --- |
| Virtual | Virtual en el mismo host | El switch virtual necesita soportar port mirroring.  Mover una de las máquinas virtuales a otro host por sí mismo podría romper el port mirroring. |
| Virtual | Virtual en hosts diferentes | Se debe asegurar que el switch virtual soporta este escenario. |
| Virtual | Físico | Requiere un adaptador de red dedicado, de otra forma ATA verá todo el tráfico que venga desde el host y este tráfico será enviado al ATA Center. |
| Físico | Virtual | Se debe asegurar que el switch, sea físico o virtual, soporta port mirroring, basado en el siguiente escenario:   * Si el host virtual está en el mismo switch físico, se necesitará configurar en el switch el level span. * Si el host virtual está sobre un switch diferente, se necesitará configurar RSPAN o ERSPAN. \* |
| Físico | Físico en el mismo switch | El switch físico debe soportar SPAN/port mirroring. |
| Físico | Físico en un switch diferente | Requiere switch Físicos que soporten RSPAN o ERSPAN. \* |

\*ERSPAN esta solo soportado cuando la desencapsulación se realiza, de esta forma ATA analiza el tráfico.

**Nota:** Port mirroring es una nueva característica en los virtual switch de Hyper-V en Windows Server 2012. Así, los hosts de virtualización necesitan ejecutar al menos Windows Server 2012 para el ATA Center y el ATA Gateway para hacer uso de esta característica en los huéspedes Hyper-V.

* + 1. Integración con SIEM

Los siguientes delineamientos desde ser tomados en consideración:

Configure uno de los servidores de ATA Gateway para escuchar y aceptar el reenvío de los eventos desde el SIEM o el servidor Syslog.

Configura el SIEM o el servidor Syslog para reenviar eventos específicos al ATA Gateway.

No reenvíe todos los datos del Syslog al ATA Gateway.

ATA soporta tráfico UDP desde el SIEM o el servidor Syslog.

ATA soporta los siguientes fabricantes de SIEM:

RSA Security Analytics

HP Arcsight

Splunk

IBM QRadar

Se refieren a [Type Customer Name Here] documentación del producto SIEM/Syslog para obtener información acerca de cómo configurar el reenvío de eventos específicos a otro servidor.

Si [Type Customer Name Here] no usa SIEM/Syslog, [Type Customer Name Here] puede configurar los DC para que reenvíen el Evento de Windows ID 4776 que sean colectados y analizados por ATA. El Evento de Windows ID 4776 proporciona datos referentes a autenticaciones NTLM.

Mayor profundidad y guía será provista como parte del documento de la guía operacional de este proyecto.

* 1. Limitaciones

**Guidelines for Documenting Constraints**

**Purpose:** Identify any business, project or technical constraints that will need to be considered in design of the Solution.

**Responsibility:** All

**Length:** As succinct as possible (one to two pages).

**Guidelines:** Identify those factors that will be critical to accurately designing the Solution for all team perspectives.

**Instructions:** As, or if, you have identified constraints for your delivery, use the following table to populate your list. These will be important to capture and illustrate, as they will serve as supporting material during your design sessions in the Planning phase. Your constraints might also result in risks that should be documented in a Risk Assessment Plan during your engagement.

Tabla 24: Limitaciones

| Código de Identificación | Explicación |
| --- | --- |
| C1 | DC con Windows Server 2008 o superior es requerido. (2008 R2 utilizando un ATA Lightweight Gateway) |
| C2 | DC Físicos versus virtuales indicará donde los servidores Gateway será ubicados como parte de la visión y diseño de la solución. |
| C3 | Conexión de red estable entre el Gateway y el Center. Vea los requerimientos de red de Gateway y Center. |
| C4 | Reúna los requerimientos de port-mirroring para configurar los DC en el alcance de este proyecto. Nosotros recomendamos incluir todos los DC para una capacidad máxima de descubrimiento y detección de amenazas. |
| C5 | Controles de cambio para implementaciones de servidores. |
| C6 | El PKI interno es necesario para emitir certificados al ATA Center y Gateway para el portal y comunicaciones entre ellos. |

* 1. Análisis de Uso

List and define the Solution’s users and their important characteristics. Also describe how the users will interact with the Solution. This information forms the basis for developing requirements.

La siguiente sección resume el análisis de uso del ATA.

* + 1. Perfiles de Usuarios

Describe the proposed Solution’s users and their important characteristics. The users are identified in groups, usually stated in terms of their functional areas. Often users are from both the IT (help desk, database administration, and so on) and business (accounting, warehouse, procurement, and so on) areas of the customer’s organization. The important characteristics identify what the users are doing that the Solution will facilitate. These characteristics can be expressed in terms of activities: for example, the accounting user receives invoices and makes payments to suppliers.

This section should contain a level of user profile information that enables the identification of unique requirements.

**Justification:** Initially, user profiles enable the development of usage scenarios (next section). Beyond that, user profiles provide the project teams with vital requirements information. A complete set of user profiles helps make sure that all high-level requirements can be identified. The product team uses these profiles as input when developing the Feature/Function List. The development team uses these profiles as input to its architecture and technology design strategies. The user education team uses these profiles to establish the breadth of their work.

**Instructions:** Update the following table with specifics for each role based upon your delivery.

Tabla 25: Perfiles de usuarios

|  |  |
| --- | --- |
| Tipo de Usuarios | Explicación |
| Administradores ATA | Este es un grupo integrado y debería contener los administradores del ATA Center and Gateway. |
| Usuarios  ATA | Una cuenta de usuario y contraseña con acceso de lectura a todos los objetos en los dominios que serán monitoreados. |
| Usuario ATA honeytoken | **Opcional:** Una cuenta de usuario de un usuario que no tiene actividades de red. El SID es usado en la configuración de ATA. ATA debe ser configurado para proporcionar servicios de detección para múltiples cuentas honeytoken. |

* + 1. Escenarios de Uso

Define the sequences of activities the users perform within the proposed Solution’s environment. This information is comprised of a set of key events that will occur within the users’ environment. These events should be described by their objectives, key activities and their sequences, and the expected results.

**Justification:** Usage scenarios provide vital information to identify and define the Solution’s user and organizational requirements, the look and feel of user interfaces, and the performance users expect of the Solution.

Discuss the response plan approach and what is within scope of the project if threats are discovered during the engagement.

Tabla 26: Escenarios de uso

| Código de Identificación | Explicación |
| --- | --- |
| US1 | ATA es exitosamente configurado e intercepta comunicaciones de red desde los DC |

1. Apéndice
   1. Resumen: Como ATA proporciona servicios de detección

**Paso 1:** **Analizar**—Después de la instalación, usando un pre configurado, port mirroring no intrusivo, todo el tráfico relacionado con AD es copiado al ATA mientras permanece invisible a los atacantes. ATA usa una tecnología de inspección de paquetes en profundidad para analizar todo el tráfico AD. También colecta eventos relevantes desde SIEM y otras fuentes.

**Paso 2:** **Aprender**—ATA automáticamente inicia el aprendizaje y perfilamiento del comportamiento de los usuarios, dispositivos y recursos, y entonces usa una tecnología de auto aprendizaje para construir un Gráfico de Seguridad Organizacional. El Gráfico Organizaciones de Seguridad es un mapa de interacciones de entidades que representa el contexto y actividades de usuarios, dispositivos y recursos.

**Paso 3:** **Detectar**—Después de construir un Gráfico de Seguridad Organizacional, ATA puede buscar anormalidades en el comportamiento de una entidad e identificar actividades sospechosas—pero no antes que esas actividades anormales hayan sido contextualmente agregadas y verificadas.

ATA usa años de búsquedas de Seguridad de clase mundial para detector ataques conocidos e incidentes de seguridad que toman lugar regional y globalmente.

ATA automáticamente será una guía, hacienda preguntas simples para ajustar el proceso de detección de acuerdo a las respuestas.

**Paso 4:** **Alertar**—Aun cuando la esperanza es nunca alcanzar esta etapa, ATA está ahí para alertar de actividades anormales y sospechosas. Para aumentar la precisión y ahorrar tiempo y recursos, ATA no solo compara el comportamiento de la entidad propia, sino que la compara con el comportamiento de otras entidades en este camino de intersección antes de emitir una alerta. Esto reduce dramáticamente el número de falsos positivos, hasta centrarse en las amenazas reales.

En este punto, es importante para la información presentada en el reporte se claro, funciona y accionable. La línea de tiempo de ataque simple es similar a las de medios sociales sobre una interfaz web y una superficie de eventos de una manera fácil de entender.

* 1. Beneficios potenciales principales de la tecnología ATA

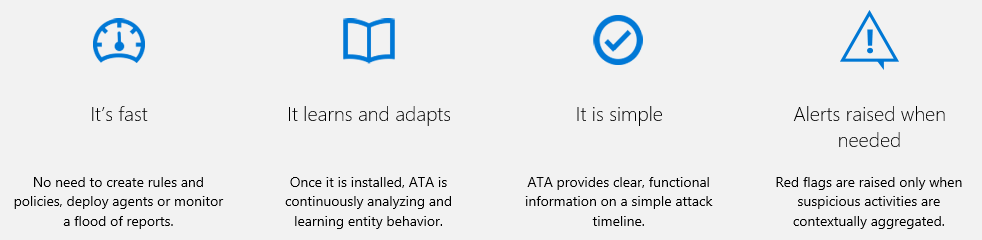


Figure 3: Beneficios potenciales principales

**Detectar:** Usando un algoritmo propietario, ATA trabaja alrededor del reloj para ayudar a detector actividades sospechosas en los sistemas perfilando y conociendo que buscar ATA también detecta ataques avanzados e incidentes de seguridad.

**Foco:** La divulgación constante de herramientas de Seguridad tradicional y examinar a través de ellas para ubicar las alertas importantes y relevantes, puede ser abrumador. La línea de tiempo de ataque es una manera clara, eficiente y conveniente que muestra las cosas correctas. Este puede entregar el poder de tener la perspectiva sobre quién, qué, cuándo y cómo. ATA también provee recomendaciones para la investigación y remediación de cada actividad sospechosa.

**Adaptable:** ATA continuamente aprende del comportamiento de las entidades organizaciones (usuarios, dispositivos y recursos) y se ajusta para reflejar los cambios en el ambiente evoluciona rápidamente. Como los atacantes toman tácticas más sofisticadas, ATA ayuda a adaptarse a la naturaleza de los Cambios de los ataques de ciberseguridad con análisis de comportamiento de aprendizaje continuo.

**Reducir:** Las herramientas TI tradicionales de Seguridad a menudo no son equipadas para manejar las crecientes cantidades de datos, levantando banderas tojas innecesarias y distrayendo de las amenazas reales. Con ATA, esas alertas suceden una vez que esas actividades sospechosas son contextualmente agregadas a su propio comportamiento como también con la interacción con otras entidades. El mecanismo de detección también guía automáticamente a través del proceso, hacienda preguntas simples para ajustar el proceso de detección de acuerdo a las respuestas entregadas.

1. <http://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/overview.aspx> [↑](#footnote-ref-2)