Vision and Scope



Advanced Threat Analytics Implementation Services

Prepared for

[Type Customer Name Here]

6/22/2016

Version 0.1 Draft

Prepared by

**[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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Problem statement 1](#_Toc454350232)

[2 Business opportunity 2](#_Toc454350233)

[2.1 Opportunity statement 2](#_Toc454350234)

[3 Project vision and scope 4](#_Toc454350235)

[4 Vision statement 5](#_Toc454350236)

[4.1 Benefits analysis 5](#_Toc454350237)

[4.2 Requirements 6](#_Toc454350238)

[4.2.1 Business requirements 7](#_Toc454350239)

[4.2.2 User requirements 8](#_Toc454350240)

[4.2.3 Operational requirements 8](#_Toc454350241)

[4.2.4 System requirements 9](#_Toc454350242)

[4.2.5 Security requirements 10](#_Toc454350243)

[4.3 Scope of project 10](#_Toc454350244)

[4.3.1 Solution components in scope 11](#_Toc454350245)

[4.3.2 Out-of-scope Solution components 14](#_Toc454350246)

[4.4 Objectives 15](#_Toc454350247)

[4.4.1 Business objectives 15](#_Toc454350248)

[4.4.2 Technical objectives 15](#_Toc454350249)

[4.5 Deliverables 16](#_Toc454350250)

[4.6 Acceptance criteria 17](#_Toc454350251)

[4.7 Operational criteria 18](#_Toc454350252)

[5 Solution design strategies 20](#_Toc454350253)

[5.1 Architectural design strategy 20](#_Toc454350254)

[5.2 Technical design strategy 21](#_Toc454350255)

[5.2.1 ATA Center 21](#_Toc454350256)

[5.2.2 ATA Gateways 25](#_Toc454350257)

[5.2.3 Port mirroring 31](#_Toc454350258)

[5.2.4 Port mirroring considerations 32](#_Toc454350259)

[5.2.5 SIEM integration 32](#_Toc454350260)

[5.3 Constraints 33](#_Toc454350261)

[5.4 Usage analysis 34](#_Toc454350262)

[5.4.1 User profiles 34](#_Toc454350263)

[5.4.2 Usage scenarios 35](#_Toc454350264)

[6 Appendix 36](#_Toc454350265)

[6.1 Overview: How ATA provides detection services 36](#_Toc454350266)

[6.2 Key potential benefits of the ATA technology 37](#_Toc454350267)

Table of Figures

[Figure 1 ATA conceptual architecture 20](#_Toc454350273)

[Figure 2: ATA network capture data flow 31](#_Toc454350274)

[Figure 3: Key potential benefits 37](#_Toc454350275)

Table of Tables

[Table 1: Business requirements 7](#_Toc454350276)

[Table 2: User requirements 8](#_Toc454350277)

[Table 3: Operational requirements 9](#_Toc454350278)

[Table 4: System requirements 9](#_Toc454350279)

[Table 5: Security requirements 10](#_Toc454350280)

[Table 6: In-scope Solution components 12](#_Toc454350281)

[Table 7: Solution components: Out of scope 14](#_Toc454350282)

[Table 8: Engagement deliverables 16](#_Toc454350283)

[Table 9: Acceptance criteria 17](#_Toc454350284)

[Table 10: Operational criteria 18](#_Toc454350285)

[Table 11: Architectural design strategy Solution components 21](#_Toc454350286)

[Table 12: Solution roles: Center 21](#_Toc454350287)

[Table 13: Center hardware 22](#_Toc454350288)

[Table 14: Requirements: Center sizing 23](#_Toc454350289)

[Table 15: Requirements: Center network ports 23](#_Toc454350290)

[Table 16: Requirements: Center software 24](#_Toc454350291)

[Table 17: Solution roles: Gateway 25](#_Toc454350292)

[Table 18: Requirements: Lightweight Gateway hardware 25](#_Toc454350293)

[Table 21: Requirements: Lightweight Gateway network ports 26](#_Toc454350294)

[Table 19: Requirements: Gateway hardware 27](#_Toc454350295)

[See Gateway sizing section: Table 20: Requirements: Gateway sizing 27](#_Toc454350296)

[Table 20: Requirements: Gateway sizing 28](#_Toc454350297)

[Table 21: Requirements: Gateway network ports 29](#_Toc454350298)

[Table 22: Requirements: Gateway software 29](#_Toc454350299)

[Table 23: Port-mirroring considerations 32](#_Toc454350300)

[Table 24: Constraints 34](#_Toc454350301)

[Table 25: User Profiles 35](#_Toc454350302)

[Table 26: Usage scenarios 35](#_Toc454350303)

**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. Problem statement

**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

Today, the topic of cybersecurity has moved from IT and the data center to the top levels of the boardroom. Attacks and threats have grown substantially more sophisticated in frequency and severity. What is at stake? Everything from customer privacy to brand identity, executive reputations, and beyond.

Without a strong detection system, effective safeguarding, and response plan process controls in place, several things might occur. The identities of individuals might be compromised, businesses might lose customers as a result of reputational damage, and companies might lose control of trade secrets and intellectual property—they might even lose their competitive edge in the market.

Attackers have been shown to reside within a network an average of eight months before they are detected. In the vast majority of attacks, attackers compromise user credentials, and they are increasingly using legitimate IT tools rather than malware.

In today’s modern IT environment, recognizing the following threat elements[[1]](#footnote-2) is imperative for your organization:

* Before being detected, attackers stay in a network more than **140 days**, on average.
* Cybercrime costs the global economy an estimated **$500 billion**.
* **Over 60%** of all network intrusions are traced back to compromised credentials.
* A data breach costs a company an average of **$3.5 million.**

1. Business opportunity

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.

Traditional IT security tools provide limited safeguarding against sophisticated cybersecurity attacks when user credentials are stolen. Initial setup, creating rules, and fine-tuning are cumbersome and could take years. Each day, customers receive several reports full of false positives. Customers do not have the resources to review this information and if they do, they still might not understand what the data is telling them. These tools are traditionally designed to help protect the perimeter—primarily stopping attackers from gaining access. Today’s complex cybersecurity attacks require a far different approach.

As a result of this engagement, [Type Customer Name Here] has the opportunity to be educated on the latest threat landscape that Microsoft Advanced Threat Analytics (ATA) detects against and how to build an effective plan to respond to the threat indicators ATA discovers. This engagement also focuses on the architecture and deployment of ATA within [Type Customer Name Here]’s enterprise to complement and further enhance their detection strategy.

* 1. Opportunity statement

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 might provide a simpler and faster way for [Type Customer Name Here] to understand what is happening within their network by identifying suspicious activity through using User and Entity Behavior Analytics (UEBA), and providing clear and relevant threat information on a simple attack timeline.

This Solution focuses on the detection core and how [Type Customer Name Here] will respond to the threats ATA detects. Having an effective response plan for the threat indicators will prepare [Type Customer Name Here] to respond appropriately based on the severity of the discovered threat. It will also help [Type Customer Name Here] prioritize threats based on an understanding of the threats as a result of the response planning exercise that is part of this engagement.

1. Project vision and scope
   1. Vision statement

**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 prepares [Type Customer Name Here] to detect threats that are malicious activities targeted at Active Directory Domain Services (Active Directory (AD) DS) credentials. This project’s vision is to implement threat-detection capabilities, to identify threats posed against user and entity credentials, and prepare the organization to effectively respond to the threats ATA identifies.

Microsoft will assist [Type Customer Name Here] in achieving this vision by educating, preparing, designing, and implementing the ATA Solution.

* 1. Benefits analysis

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 automatically analyzes, learns, and identifies abnormal authentication behavior on your network—alerting you to possible indicators of compromise. Microsoft Services will implement a well-thought-out design of the Solution and [Type Customer Name Here] will have the confidence to understand the severity of the indicators ATA produces and can respond appropriately.

During the course of this engagement, the following potential benefits can be gained:

**Discovery of abnormal user behavior:** Using behavioral analytics and machine learning, ATA will uncover questionable activities and abnormal behavior, such as anomalous logins, abnormal resource access and working hours, password sharing, and lateral movement.

**Identification of malicious attacks:** ATA detects known malicious attacks almost instantly, including Pass the Ticket, Pass the Hash, Overpass the Hash, forged PAC (Microsoft Security Bulletin 14-068), Golden Ticket, Skeleton Key malware, reconnaissance, brute force, and remote execution.

**Identification of security issues and risks:** ATA identifies security issues such as Broken Trust and known protocol vulnerabilities.

**Delivering a sensible design and thoughtful implementation:** By following the Microsoft Solutions Framework (MSF), Microsoft Services prepares a more secure, well-thought-out design and implementation.

**Understanding and responding to attacker behaviors:** The Advanced Threat Analytics Implementation Services (ATAIS) methodology will educate you on the specific threats ATA detects and how to appropriately respond to them—allowing you to make more informed decisions on mitigations and develop your long-term threat-detection strategy.

**Development and integration of ATA-specific response planning:** Microsoft Services will help you understand the suspicious indicators discovered by ATA, the necessary response actions, and how to integrate them into your existing response plan.

* 1. Requirements

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

The following section outlines the requirements of the envisioned Solution to be deployed as part of this engagement.

* + 1. Business requirements

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.

This engagement’s business requirements address the enterprise’s unique threat-detection needs. It is imperative that [Type Customer Name Here] understands their goals and challenges. These will vary based on many factors, but some common areas that [Type Customer Name Here] might require include:

**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.**

Table : Business requirements

| Identification Code | Requirement |
| --- | --- |
| BR1 | Improve existing response plan processes. |
| BR2 | Activate a more robust threat-detection strategy. |
| BR3 | The Solution must pose minimum risk to the environment and the operational well-being of the business. |
| BR4 | Microsoft needs to review and provide input for ’s current response plan related to ATA detections. |

* + 1. User requirements

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.

The following table describes user requirements that must be considered during all phases of the engagement.

**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.

Table : User requirements

| Identification Code | Requirement |
| --- | --- |
| UR1 | [Type Customer Name Here] will identify administrators of the Solution |
| UR2 | The Solution should make use of a standard non-elevated user account. |
| UR3 | A honeytoken user account is optional for the Solution. An account for a user who has no network activities will be configured as the ATA honeytoken user. To configure the honeytoken user, you will need the security identifier (SID) of the user account, not the user name. |
| UR4 | The Solution requires a service account. |

* + 1. Operational requirements

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.

The following table describes the operational requirements that must be considered during all phases of the engagement.

**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.

Table 3: Operational requirements

| Identification Code | Requirement |
| --- | --- |
| OR1 | Microsoft needs to provide clear operational guidance to during the Envision, Plan, Build, Stabilize, and Deployment phases. |
| OR2 | Clear backup guidance needs to form part of the operational excellence of the Solution. |
| OR3 | Microsoft needs to provide clear deployment guidance so [Type Customer Name Here] can reinstall the Solution, if necessary. |

* + 1. System requirements

The following table describes the system requirements that must be considered during all phases of the engagement.

**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.

Table : System requirements

| Identification Code | Requirement |
| --- | --- |
| SR1 | Option 1: The system needs to be deployed on a virtualized platform.  Option 2: The system needs to be deployed on a physical platform. |
| SR2 | Make adequate storage available based on the technical design strategy envisioned. |
| SR3 | Make adequate hardware specifications available based on the technical design strategy envisioned. |
| SR4 | Option 1 (Lightweight Gateway): The Solution will be deployed using minimal hardware taking an agent-based approach where possible.  Option 2 (port-mirrored gateway): The Solution will be deployed in a manner which does not add additional compute resources to existing systems.  Option 3 (combination Lightweight Gateway and Port Mirrored Gateways): Where possible, the Solution will be deployed with minimal costs and impact to existing systems. |

* + 1. Security requirements

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.

The following table describes the security requirements that must be considered during all phases of the engagement.

Table : Security requirements

| Identification Code | Requirement |
| --- | --- |
| SECR1 | The education phase will prepare to understand the specific threat indicators ATA discovers. |
| SECR2 | The response plan and workshop will help to understand, identify, and prioritize the threat indicators and respond to these threats appropriately. |
| SECR3 | Communications to the administration portal should be encrypted. |
| SECR4 | Communications between the Center and the Gateway should be encrypted. |
| SECR5 | Option (port-mirrored gateway deployment): Where possible, the detection service should remain invisible (hidden) from potential attackers in a way that the detection service does not show up as a running agent on any end-state system. |

* 1. Scope of project

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.

The scope of this engagement consists of intake and review, envisioning, planning and developmental exercises, and analysis and interviews with functional area stakeholders. This culminates in the delivery of a cybersecurity implementation and execution roadmap that is tailored to [Type Customer Name Here]’s unique mission or business requirements and priorities.

The following section outlines the scope items of this engagement. Specifically, this engagement will provide an understanding of the threats that ATA can provide detection services for, assist with the creation of a response plan specific to the events that ATA might identify, and assist with the design and deployment of ATA to monitor for threats to [Type Customer Name Here]’s production AD DS environment.

* + 1. Solution components in scope

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

The following items are regarded as in-scope when preparing to design and implement ATA to provide threat-detection services in [Type Customer Name Here]’s production AD DS environment. The scope items should align to that of the agreed Statement of Work (SOW) document.

The following table details the specific items to include to support this scope.

Table : In-scope Solution components

| Solution component | Description and considerations | Scope assumptions |
| --- | --- | --- |
| Educational workshops | Microsoft will conduct three educational workshops focused on the following topic areas (one workshop for every topic area):   * Understanding of cybersecurity framework * Credential theft scenarios * ATA overview and deep dive | For appropriate personnel responsible for making decisions in the event ATA detects a threat.  For all personnel responsible for designing, deploying, and operating ATA. |
| ATA Response Planning workshops | Microsoft will conduct four workshops and two tabletop exercises to help build a response plan specific to events that ATA might identify. The workshops will cover the following topic areas (one workshop per topic area):   * Response team identification and responsibility definition * ATA event definition and classification * ATA event handling and response process definition * Organizational communication process definition | Appropriate personnel responsible for determining the following will attend each of the workshops:   * Response team identification and responsibility definition * ATA event definition and classification * ATA event handling and response process definition * Organizational communication process definition |
| ATA Response Plan document | Microsoft will provide an ATA Response Plan document, written in Microsoft Word, that will include decisions made during the ATA response planning workshops culminating in an ATA Response Plan. | The draft document will be shared with during a review meeting, at which time all feedback will be gathered. Microsoft will take this feedback and make agreed-on updates, resulting in a final version that will be delivered to . |
| ATA Design workshops | Microsoft will lead one workshop to determine the specific ATA design required to address the in-scope Solution. | All required personnel will attend these meetings. Decisions will be made during the meetings so the final design can be completed. |
| Solutions Design | Microsoft will provide a Solutions Design document written in Microsoft Word that will detail the ATA design to be deployed to meet the scope of this project. | The draft document will be shared with during a review meeting, at which time all feedback will be gathered. Microsoft will take this feedback and make agreed-on updates, resulting in a final version that will be delivered to . |
| Test Planning workshop | Microsoft will lead one workshop to define test cases specific to performing system testing and configuration validation for ATA. | For appropriate personnel required to define test cases and processes and to provide input into the test planning process. |
| Test Plan document | Microsoft will provide a Test Plan document, written in Microsoft Word, that will detail necessary testing and validation procedures that will be used to validate the system functionality of ATA. | This document will be shared with during a review meeting, at which time agreements will be made that the test cases will satisfy the validation of the deployed environment. This document will be in draft format until the test cases have been completed and all test results have been documented in the Test Plan document. |
| Implementation Guide document | Microsoft will provide an Implementation Guide document detailing the necessary steps to install and configure ATA. | The draft document will be shared with during a review meeting, at which time all feedback will be gathered. Microsoft will take this feedback and make agreed-on updates, resulting in a final version that will be delivered to . |
| Production deployment of ATA | Microsoft will assist with deploying ATA Center and up to eight hours of deployment assistance for ATA Gateway listeners that will monitor the production AD DS forest. | Microsoft will assist in deploying ATA into a production environment. |
| ATA tuning | Microsoft will assist with reviewing events that ATA identifies after the installation for up to eight hours and will help address false positive events that are captured during this time. | will assign the appropriate operational staff to work side by side with the Microsoft team to review any events that ATA captures, and to determine, follow up on, and address false positive events as they occur. |
| Operations Guide document | Microsoft will provide an Operations Guide document, written in Microsoft Word. This document will provide basic guidance on maintaining the ATA. | The draft document will be shared with during a review meeting, at which time all feedback will be gathered. Microsoft will take this feedback and make agreed-on updates, resulting in a final version that will be delivered to . |

* + 1. Out-of-scope Solution components

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.

The following scope items are regarded as out of scope in preparing for, designing, and implementing ATA to provide threat-detection services for [Type Customer Name Here]’s production AD DS environment. The scope items should align to that of the agreed SOW document.

The following table details the specific items that will not be included to support this scope.

Table 7: Solution components: Out of scope

| Solution component | Description and considerations | Scope assumptions |
| --- | --- | --- |
| Response plan | Define a complete environmental response plan for . Microsoft will provide only input into the existing response plan and process. | It is assumed that has an existing plan for responding to ATA discovery elements; Microsoft can help improve this plan. |
| Product licensing | Licenses for Windows Server 2012 R2 (Datacenter or Standard edition) | [Type Customer Name Here] is responsible for obtaining all product licenses. |
| Public key infrastructure (PKI) deployment | A PKI Solution to deploy certificates. | [Type Customer Name Here] is responsible for all PKI requirements and issuing certificates. |
| Secure Sockets Layer (SSL) certificates | Issuing certificates from an internal PKI. Certificate requirements are outlined in the software requirements section of this document. (See software requirements for each ATA role.) | is responsible for all SSL certificates required to deploy ATA. |
| Port mirroring | Configuring port mirroring. | If the use of a standard ATA Gateway is required, ATA requires that port mirroring be configured between the in-scope domain controllers (DCs) that will be monitored and the corresponding ATA Gateway. is responsible for configuring port mirroring. |
| Security information and event management (SIEM) integration | Integration of SIEM information into ATA | Configuring ATA to pull information in from a SIEM solution will be out of scope for this engagement. [Type Customer Name Here] is responsible for following the integration guidelines for the supported SIEM solutions online. |

* 1. Objectives

See the preceding vision statement for the goal of this engagement. The vision statement provides context for decision-making during the later stages of this project when discussing features, cost, and delivery schedule. It is not provided to be a legally binding contract for the Solution. Any revisions of this document provide the detail scope of what will and will not be accomplished to meet the vision statement. The core features to be activated by the Solution can be characterized by the following specific goals and objectives.

* + 1. Business objectives

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

The business objectives of this engagement are to address the [Type Customer Name Here]’s unique threat detection needs with a Solution that will provide actionable telemetry. The Solution includes the following:

Implementing a threat-detection Solution that identifies and provides alerts on potential cybersecurity attacks against AD DS credentials.

Establishes a response plan for how the organization will respond to threats that the threat-detection Solution identifies.

Provides education about the common threats ATA detects and how to prioritize a response based on the threats discovered.

* + 1. Technical objectives

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

This engagement will achieve the following outlined technical objectives:

The ability to analyze data to and from the DCs by means of nonintrusive port mirroring.

After ATA has performed for the required baseline learning period (30 days), any deviations to the baseline will be flagged as potential threat indicators.

The Solution hardware and storage requirements will be configured to have maximum impact for effective detections.

* 1. Deliverables

The following table lists the key project service deliverables for this engagement.

Table 8: Engagement deliverables

| Project phase | Service deliverable name | Service deliverable descriptions | Acceptance criteria |
| --- | --- | --- | --- |
| Envision | Vision and Scope | A document that includes the project vision, all agreed-on requirements, and a Solution design approach. | The document is delivered and accurately describes the elements as described in this table. |
| Plan | ATA Response Plan | A document that provides information about the roles and responsibilities for responding to events that ATA identifies. It also includes event identification, risk classifications, and response and communications processes. | The document is delivered and accurately describes the elements as described in this table. |
| Plan | Solution Design | A document that details the technical configuration of the Solution. | The document is delivered and accurately describes the elements as described in this table. |
| Plan | Preliminary Test Plan | A document that describes the strategy and approach used to plan, organize, and manage the project’s testing activities. | The document is delivered and accurately describes the elements as described in this table. |
| Build | Implementation Guide | A document that includes step-by-step instructions for deploying ATA into a production environment. | The document is delivered and accurately describes the elements as described in this table. |
| Build | ATA System Testing | The completion of all test cases as identified in the Test Plan document and according to the in-scope Solution. | The activity is performed accurately as described in this table. |
| Build | Final Test Plan | A document that includes all final test results and notes for completing each defined test case in the document. | The document is delivered and accurately describes the elements as described in this table. |
| Stabilize | Operations Guide | A document that details how to operate and manage the ATA system. | The document is delivered and accurately describes the elements as described in this table.  This document does not contain information or processes specific to responding to a detected event. Those items are documented in the ATA Response Plan. |
| Deployment | Implementation | Implementation of the Solution. | The deployment of the Solution per the agreed-on Solution Design document. |

* 1. Acceptance criteria

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.

The following table describes the acceptance criteria for a successful engagement.

**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.

Table : Acceptance criteria

| Identification code | Requirement |
| --- | --- |
| AC1 | ATA is successfully intercepting network traffic to and from the DCs. |
| AC2 | ATA Gateways are successfully gathering entity information from the DCs. |
| AC3 | fully understands each of the threats for which ATA provides detection services. |
| AC4 | understands the ATA Response Plan and how to approach and prioritize threats ATA discovers. |
| AC5 | An ATA Response Plan that accurately reflects the plan for events that ATA might detect. |
| AC6 | Vision and Scope: A document that accurately reflects the scope of the work to be performed, requirements of the Solution, and an expected Solution design strategy that will be expanded on during the Plan phase. |
| AC7 | Solution Design: A document that accurately records the configuration of the envisioned and deployed Solution. |
| AC8 | Solution Test Plan: A document that accurately and completely reflects all test cases that need to be validated for system functionality. |
| AC9 | Solution Implementation Guide: A document that provides step-by-step instructions for implementing the in-scope Solution of ATA components. |
| AC10 | Solution Operations Guide: A document that contains operational information specific to operating and managing the ATA deployment. |
| AC11 | Informal knowledge transfers during the engagement of ATA design, implementation, and testing elements. |

* 1. Operational criteria

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.

The following table outlines the operational criteria for a successful engagement.

Table 10: Operational criteria

| Identification code | Requirement |
| --- | --- |
| OC1 | ATA administrators can access the ATA Console. |
| OC2 | The ATA Console displays detected suspicious activities on the attack timeline. |
| OC3 | ATA alerts allow administrators to interact and facilitate human acknowledgement and input. |
| OC4 | ATA makes heath state alerts available. For example, when communication between the gateway and the Center is disrupted or when the user account that is used for cataloging entities from AD expires. |
| OC5 | The Solution allows for the exclusion of short-term leased subnets, such as virtual private networks (VPNs), internal penetration testing tools subnets, or IPs. |
| OC6 | can back up and restore the ATA database and can move the database to another drive or volume. |

1. Solution design strategies
   1. Architectural design strategy

**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.

The following diagram envisions the proposed ATA architecture.



Figure 1 ATA conceptual architecture

Figure 1 illustrates the notional Solutions design that will be considered for ’s ATA deployment. It is important to note that the actual design, which meets ’s requirements and needs, will be established during Solution design workshops as a part of the project’s Plan phase.

The following table lists the items that will be used for the purposes of this design.

**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.

Table : Architectural design strategy Solution components

|  |  |
| --- | --- |
| Solution component | Rationale |
| ATA Center | An ATA Center will be deployed to provide detection services for the following forests:  **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 will be deployed to all DCs to monitor, parse, and forward all ATA-relevant network activity.  **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 will be deployed to monitor DCs in the following data center locations:  **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. Technical design strategy

This section provides details specific to the ATA requirements and configuration settings. Information in this section is provided to help drive a technical Solution design as a part of the Planning phase of this project. This information is for to review and understand so you can adequately prepare your teams for the Solution design workshop discussions.

* + 1. ATA Center

This section covers the Center requirements. Detailed design and configurations are recorded in the Solution design document. The following table lists the tasks that the ATA Center performs.

Table 12: Solution roles: Center

|  |  |
| --- | --- |
| Role | Description |
| Center | * Manages ATA Gateway configuration settings * Receives data from ATA Gateways * Detects suspicious activities and is responsible for UEBA * Supports multiple ATA Gateways * Runs the ATA Console |

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. Center hardware

The ATA Center requires a minimum 30 days of data for user behavior analytics. The following table defines the required disk space for the ATA database on a per-DC basis. If you have multiple DCs, add up the required disk space per DC to calculate the total amount of space required for the ATA database.

The number of DCs that is monitoring and the load on each of the DCs dictates the hardware requirements.

The following table outlines the base hardware requirements for the ATA Center.

Table 13: Center hardware

| Component | Center hardware requirements |
| --- | --- |
| Processor | See Center sizing section. |
| Memory | See Center sizing section. |
| Available disk space  Database storage | See Center sizing section. |
| Network | Communication between the ATA Center and the ATA Gateway is encrypted using SSL on port 443. Additionally, the ATA Console runs on Internet Information Services (IIS) and is secured using SSL on port 443. **Two IP addresses** are required. The ATA Center service will bind port 443 to the first IP address and IIS will bind port 443 to the second IP address. Also see the network ports requirements in the following table.  **Note:** Confirm a stable and effective network connection between the Center and the Gateway. See Gateway requirements for memory.  **Note:** Short-term lease subnets  Identify the subnets in which IP addresses are reassigned between devices within a very short period of time (seconds or minutes). ATA reduces the cache lifetime for all IP addresses in these subnets to accommodate the fast reassignment between devices. VPN or Wi-Fi networks are common examples of short-term lease subnets. |
| Virtualization | Installation of the ATA Center as a virtual machine is supported. |
| BIOS | The ATA database requires that [Type Customer Name Here] DISABLE Non-uniform memory access (NUMA) in the BIOS. Your system might refer to NUMA as Node Interleaving, in which case you will have to ENABLE Node Interleaving. |

* + - 1. Center sizing

The ATA Center requires a minimum of 30 days of data for user behavior analytics. The following table defines the required disk space for the ATA database on a per-DC basis. If you have multiple DCs, add up the required disk space per DC to calculate the total amount of space required for the ATA database.

Table 14: Requirements: Center sizing

| Packets per second\* | CPU (cores\*\*) | Memory (GB) | Database storage per day (GB) | Database storage per month (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) |

\* Total daily average number of packets per second from all DCs monitored by all ATA Gateways.

\*\* Includes physical cores, not hyperthreaded cores.

\*\*\* Input/output operations per second; average numbers (peak numbers)

**Notes:**

The ATA Center can handle an aggregated maximum of 400,000 frames per second from all monitored DCs.

The storage amounts indicated here are net values; you should account for future growth to make sure that the disk the database resides on has at least 20% available free space.

* + - 1. Center network ports

The following table lists the minimum ports that the ATA Center needs.

Table 15: Requirements: Center network ports

| Protocol | Transport | Port | To or from | Direction |
| --- | --- | --- | --- | --- |
| SSL (ATA communications) | 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 (optional) | TCP | 25 | SMTP server | Outbound |
| SMTPS (optional) | TCP | 465 | SMTP server | Outbound |
| Syslog (optional) | TCP | 514 | Syslog server | Outbound |

* + - 1. Center software

The following table outlines the ATA Center software requirements.

Table 16: Requirements: Center software

| Component | Center software requirements |
| --- | --- |
| Certificates | ATA Center requires certificates for the following services:   * IIS: Web server certificate * ATA Center service: Server authentication certificate |
| Operating system | Windows Server 2012 R2 Standard or Datacenter editions |
| Domain or workgroup membership | The ATA Center can be installed on a server that is a member of a domain or workgroup |
| User account | **Local administrator** (non–**domain joined)**  **Standard user account (domain joined)**: Added to local administrator, ATA administrators |
| Components | The following components are installed and configured during the ATA Center installation:   * IIS * MongoDB * ATA Center service and ATA Management IIS site * Custom performance monitor data collection set * X.509 certificate will be recommended and issued by an internal PKI. Self-signed is only recommended for testing purposes. |
| Browser support | The ATA Console is accessed through a browser. The following browsers are supported:   * Internet Explorer 10 * Google Chrome 40 * Minimum screen width resolution of 1700 pixels |
| Microsoft updates | Make sure that all Microsoft updates have been installed on the server. |

* + 1. ATA Gateways

ATA has two components, the ATA Center and the ATA Gateway. This section discusses the gateway requirements.

You can deploy ATA using a combination of gateway configurations: ATA Gateways only, ATA Lightweight Gateways only, or both ATA Gateways and ATA Lightweight Gateways. The ATA Lightweight Gateway is recommended over the ATA Gateway whenever possible, as long as the DCs comply with the ATA Lightweight Gateway sizing table (below). Most DCs can, and should, be covered with the ATA Lightweight Gateway unless your domain controllers don't fit with the requirements in the sizing table.

Table 17: Solution roles: Gateway

| Role | Description |
| --- | --- |
| The ATA Gateway and Lightweight Gateway both have the same core functionality. | * Capture and inspect DC network traffic (port-mirrored traffic in the case of an ATA Gateway and local traffic of the domain controller in the case of an ATA Lightweight Gateway) * Receive Windows events from SIEM or Syslog servers, or from DCs using Windows event forwarding * Retrieve data about users and computers from the AD domain * Resolve network entities (users, groups, and computers) * Transfer relevant data to the ATA Center. * Monitor multiple DCs from a single ATA Gateway, or monitor a single DC for an 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. Lightweight Gateway hardware and sizing

An ATA Lightweight Gateway can monitor a single DC, depending on the amount of network traffic the DC generates.

The ATA Lightweight Gateway requires a minimum of 2 cores and 6 GB of RAM installed on the DC. For optimal performance, set the **Power Option** of the ATA Lightweight Gateway to **High Performance**. The ATA Lightweight Gateway can be deployed on DCs of various loads and sizes, depending on the amount of network traffic to and from the DCs and the resources installed on the DC. The following table provides sizing details.

Table 18: Requirements: Lightweight Gateway hardware

| Packets per second\* | CPU (cores)\*\* | Memory (GB)\*\*\* |
| --- | --- | --- |
| 1,000 | 2 | 6 |
| 5,000 | 6 | 16 |
| 10,000 | 10 | 24 |

\*Total number of packets per second on the DC that the ATA Lightweight Gateway is monitoring.

\*\*Total amount of nonhyperthreaded cores that the DC has installed. While hyperthreading is acceptable for the ATA Lightweight Gateway, when planning for capacity count actual cores and not hyperthreaded cores.

\*\*\*Total amount of memory installed on the DC.

**Notes:**

If the DC does not have the necessary resources the ATA Lightweight Gateway requires, the DC performance will not be effected, but the ATA Lightweight Gateway might not operate as expected.

The ATA Lightweight Gateway can be installed on a DC running Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.

The DC can be an RODC.

The DC cannot be server core.

The ATA Lightweight Gateway monitors local traffic on all of the DC’s network adapters. After deployment, you can use the ATA Console to change which network adapters are monitored.

* + - 1. Lightweight Gateway network ports

The following table lists the minimum ports that the ATA Gateway requires configured on the management adapter.

Table 21: Requirements: Lightweight Gateway network ports

| Protocol | Transport | Port | To or from | Direction |
| --- | --- | --- | --- | --- |
| DNS | TCP and UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | All devices on the network | Outbound |
| NetBIOS | UDP | 137 | All devices on the network | Outbound |
| SSL | TCP | 443 or as configured for the Center service | ATA Center:  Center Service IP Address  IIS IP Address | Outbound |
| Syslog (optional) | UDP | 514 | SIEM server | Inbound |

**Notes:**

As part of the resolution process that the ATA Lightweight Gateway performs, the NetBIOS and NT LAN Manager (NTLM) over remote procedure call (RPC) ports need to be open inbound on network devices from the ATA Lightweight Gateways.

* + - 1. Gateway hardware

An ATA Gateway can monitor multiple DCs, depending on the network traffic to and from the DCs.

Table 19: Requirements: Gateway hardware

| Component | Gateway hardware requirements |
| --- | --- |
| Processor | See Gateway sizing section. |
| Memory | See Gateway sizing section.  **Note:** The ATA Gateway uses its memory to buffer captured data and send it to the Center. The default setting is 1,000,000 entities and is configurable. Depending on the load of the DC connected to the gateway, this can generate a tremendous amount of data.  **Caution:** If communication between the Center and the Gateway is disrupted, the Gateway will cache in memory, and 1,000,000 entities can take up to 5 GB of memory. Once this limit is reached it will stop collecting network traffic until communication is restored with the Center. Depending on the DC load, this can be hours or minutes. |
| Available disk space | See Gateway sizing section: Table : Requirements: Gateway sizing |
| Network | The Gateway requires two or more network adapters.  **Management adapter**—will be used for communications on the company network. This adapter should be configured with the following:   * Static IP address including the default gateway. * Preferred and alternate Domain Name System (DNS) servers. * “DNS suffix for this connection” should be the DNS name of the domain being monitored.   **Capture adapter**—will be used to capture traffic to and from the DCs:   * Configure port mirroring for the capture adapter as the destination of the DC network traffic. * Configure a static non-routable IP address for your environment with no default gateway and no DNS server addresses. For example, 1.1.1.1/32. * This confirms that the capture network adapter can capture the maximum amount of traffic and that the management network adapter is used to send and receive the required network traffic.   **Note:** Short-term lease subnets  Identify the subnets in which IP addresses are reassigned between devices within a very short period of time (seconds or minutes). ATA reduces the cache lifetime for all IP addresses in these subnets to accommodate the fast reassignment between devices. VPN or Wi-Fi networks are common examples of short-term lease subnets. |
| Virtualization | Installing the ATA Gateway as a virtual machine is supported when the DCs being monitored are also running as virtual machines on the same virtualization host. |

* + - 1. Gateway sizing

An ATA Gateway can monitor multiple DCs, depending on the network traffic of the DCs being monitored.

Table 20: Requirements: Gateway sizing

| Packets per second\* | CPU (cores\*\*) | Memory (GB) |
| --- | --- | --- |
| 1,000 | 1 | 6 |
| 5,000 | 2 | 10 |
| 10,000 | 3 | 12 |
| 20,000 | 6 | 24 |
| 50,000 | 16 | 48 |

\* Total number of packets per second from all DCs the ATA Gateway is monitoring, during the busiest hour of the day.

\*\*Total amount of DC port-mirrored traffic cannot exceed the capacity of the capture NIC on the ATA Gateway.

\*\* Hyperthreading must be disabled.

* + - 1. Gateway network ports

The following table lists the minimum ports that the ATA Gateway requires configured on the management adapter.

Table 21: Requirements: Gateway network ports

| Protocol | Transport | Port | To or from | Direction |
| --- | --- | --- | --- | --- |
| LDAP | TCP and UDP | 389 | Domain controllers | Outbound |
| LDAP over SSL (LDAPS) | TCP | 636 | Domain controllers | Outbound |
| LDAP to Global Catalog | TCP | 3268 | Domain controllers | Outbound |
| LDAPS to 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 | All devices on the network | Outbound |
| NetBIOS | UDP | 137 | All devices on the network | Outbound |
| SSL | TCP | 443 | ATA Center:   * Center Service IP Address * IIS IP Address | Outbound |
| Syslog (optional) | UDP | 514 | SIEM server | Inbound |

* + - 1. Gateway software

The following table outlines the gateway software requirements.

Table 22: Requirements: Gateway software

| Component | Center software requirements |
| --- | --- |
| Certificates | ATA Gateway requires certificates for the following services:   * A certificate supporting **Server Authentication** is required to be installed in the computer store of the ATA Gateway in the local computer store. This certificate must be trusted by the ATA Center. |
| Operating system | Windows Server 2012 R2 Standard or Datacenter edition. |
| Domain or workgroup membership | The ATA Gateway can be installed on a server that is a member of a domain or workgroup. |
| User accounts | **Local Administrator (Non–domain joined)**  **Standard user account (Domain joined)** – Added to local admin, ATA Administrators  **Standard service account** – Used to query Active Directory for indexing and object or entity cataloging. (Domain connectivity)  **Honeytoken account** – SID to be used (Optional) |
| Components | The following components are installed and configured during the installation of the ATA Gateway:   * KB 3047154 (Do not install KB 3047154 on a virtualization host. This might cause port mirroring to stop working properly.) * ATA Gateway service * Microsoft Visual C++ 2013 Redistributable * Custom Performance Monitor data collection set |
| Microsoft updates | Run Windows Update and make sure all **Important** updates have been installed. Before installing ATA Gateway confirm that the following update has been installed, [KB2919355](https://support.microsoft.com/en-us/kb/2919355/). If the update is not installed, install the update before installing the ATA Gateway service. |

* + 1. Port mirroring

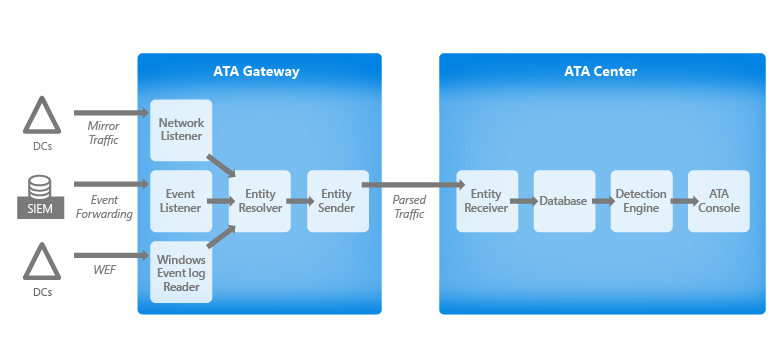


Figure 2: ATA network capture data flow

The main data source ATA uses is deep-packet inspection of the network traffic to and from ’s DCs. If you are not implementing an ATA Lightweight Gateway, you must configure port mirroring for ATA to see the network traffic. Port mirroring copies the traffic on one port, known as the *source port*, to another port, known as the *destination port*. ATA works with Solutions that can mirror traffic—if the traffic can be port-mirrored to ATA, it can be used to analyze threats to ’s system. To configure port mirroring, refer to the vendor's documentation.

[Type Customer Name Here]’s DCs and ATA Gateways can be either physical or virtual.

The following are common methods for port mirroring and some considerations:

**Switched Port Analyzer (SPAN):** Copies network traffic from one or more switch ports to another switch port on the same switch. Both the ATA Gateway and DCs must be connected to the same physical switch.

**Remote Switch Port Analyzer (RSPAN):** Empowers an organization to monitor network traffic from source ports distributed over multiple physical switches. RSPAN copies the source traffic into a special RSPAN-configured virtual LAN (VLAN). This VLAN needs to be trunked to the other switches involved. RSPAN works at Layer 2.

**Encapsulated Remote Switch Port Analyzer (ERSPAN):** A Cisco proprietary technology working at Layer 3. With ERSPAN, the user can monitor traffic across switches without the need for VLAN trunks. ERSPAN uses generic routing encapsulation to copy monitored network traffic. ATA currently cannot directly receive ERSPAN traffic. For ATA to work with ERSPAN traffic, a switch or router that can decapsulate the traffic needs to be configured as the ERSPAN destination where the traffic is decapsulated. The switch or router then needs to be configured to forward it to the ATA Gateway using either SPAN or RSPAN.

* + 1. Port mirroring considerations

Table 23: Port-mirroring considerations

| ATA Gateway | Domain controller | Considerations |
| --- | --- | --- |
| Virtual | Virtual on same host | The virtual switch needs to support port mirroring.  Moving one of the virtual machines to another host by itself might break the port mirroring. |
| Virtual | Virtual on different hosts | Make sure your virtual switch supports this scenario. |
| Virtual | Physical | Requires a dedicated network adapter, otherwise ATA will see all of the traffic coming in and out of the host—even the traffic it sends to the ATA Center. |
| Physical | Virtual | Make sure your switch, whether physical or virtual, supports port mirroring based on the following scenario:   * If the virtual host is on the same physical switch, you will need to configure a switch level span. * If the virtual host is on a different switch, you will need to configure RSPAN or ERSPAN.\* |
| Physical | Physical on the same switch | Physical switch must support SPAN/port mirroring. |
| Physical | Physical on a different switch | Requires physical switches to support RSPAN or ERSPAN.\* |

\*ERSPAN is only supported when decapsulation is performed ATA analyzes the traffic.

**Note:** Port mirroring is an new feature in Hyper-V virtual switch in Windows Server 2012. Thus, the virtualization hosts need to run, at minimum, Windows Server 2012 for the Center and Gateways to make use of this feature in Hyper-V as guests.

* + 1. SIEM integration

The following guidelines must be taken into consideration:

Configure one of your ATA Gateway servers to listen and accept events forwarded from the SIEM or Syslog server.

Configure your SIEM or Syslog server to forward specific events to the ATA Gateway.

Do not forward all the Syslog data to the ATA Gateway.

ATA supports UDP traffic from the SIEM or Syslog server.

ATA supports the following SIEM vendors:

RSA Security Analytics

HP Arcsight

Splunk

IBM QRadar

Refer to SIEM/Syslog server's product documentation for information on how to configure forwarding of specific events to another server.

If does not use a SIEM/Syslog server, can configure the Windows DCs to forward Windows Event ID 4776 to be collected and analyzed by ATA. Windows Event ID 4776 provides data regarding NTLM authentications.

More insight and guidance will be provided as part of the operational guidance document of this engagement.

* 1. Constraints

**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.

Table : Constraints

| Identification code | Explanation |
| --- | --- |
| C1 | Windows Server 2008 or later DCs required. (2008 R2 is using an ATA Lightweight Gateway) |
| C2 | Physical versus virtual DCs will dictate where the Gateway servers will be located as part of the envisioned Solution and Solution design. |
| C3 | Stable network connection between the Gateway and the Center. See network requirements on the Gateway and Center. |
| C4 | Meet port-mirroring requirements to reach DCs in scope of this engagement. We recommend reaching all DCs for maximum threat discovery and detection capabilities. |
| C5 | Change controls for server implementations. |
| C6 | The internal PKI needs to issue certificates to the Center and the Gateway for the dashboard portal and communications between the Center and the Gateway. |

* 1. Usage analysis

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.

The following section outlines the ATA usage analysis.

* + 1. User profiles

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.

Table : User Profiles

|  |  |
| --- | --- |
| User type | Explanation |
| ATA administrators | This is a built-in group and should contain the administrators of the ATA Center and Gateway. |
| ATA user | A user account and password with read access to all objects in the domains that will be monitored. |
| ATA honeytoken user | **Optional:** A user account of a user who has no network activities. The SID is used in the ATA configuration. ATA may be configured to provide detection services for multiple honeytoken accounts. |

* + 1. Usage scenarios

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.

Table : Usage scenarios

| Identification code | Explanation |
| --- | --- |
| US1 | ATA is successfully configured and intercepting network communications from the DCs |

1. Appendix
   1. Overview: How ATA provides detection services

**Step 1:** **Analyze**—After installation, by using preconfigured, nonintrusive port mirroring, all AD-related traffic is copied to ATA while remaining invisible to attackers. ATA uses deep-packet inspection technology to analyze all AD traffic. It can also collect relevant events from SIEM and other sources.

**Step 2:** **Learn**—ATA automatically starts learning and profiling behaviors of users, devices, and resources, and then uses its self-learning technology to build an Organizational Security Graph. The Organizational Security Graph is a map of entity interactions that represent the context and activities of users, devices, and resources.

**Step 3:** **Detect**—After building an Organizational Security Graph, ATA can then look for any abnormalities in an entity’s behavior and identify suspicious activities—but not before those abnormal activities have been contextually aggregated and verified.

ATA uses years of world-class security research to detect known attacks and security issues taking place regionally and globally.

ATA will also automatically guide you, asking you simple questions to adjust the detection process according to your input.

**Step 4:** **Alert**—While the hope is that this stage is rarely reached, ATA is there to alert you of abnormal and suspicious activities. To further increase accuracy and save you time and resources, ATA not only compares the entity’s behavior to its own, but also to the behavior of other entities in its interaction path before issuing an alert. This dramatically reduces the number of false positives, freeing you up to focus on the real threats.

At this point, it is important for the information presented in the reports be clear, functional, and actionable. The simple attack timeline is similar to a social media feed on a web interface and surfaces events in an easy-to-understand way.

* 1. Key potential benefits of the ATA technology

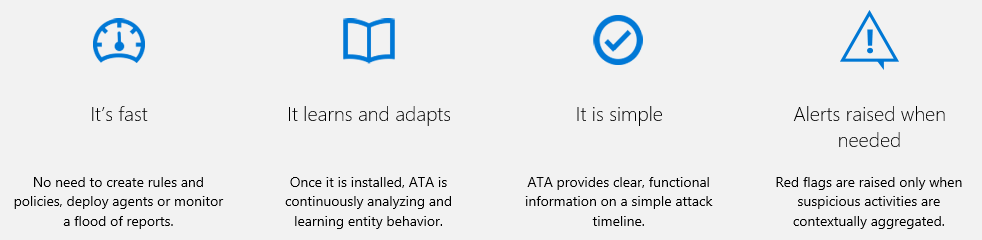


Figure : Key potential benefits

**Detect:** Using its proprietary algorithm, ATA works around the clock to help you pinpoint suspicious activities in your systems by profiling and knowing what to look for. ATA also identifies known advanced attacks and security issues.

**Focus:** The constant reporting of traditional security tools, and sifting through them to locate the important and relevant alerts, can get overwhelming. The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline. This can give you the power of perspective on who, what, when, and how. ATA also provides recommendations for investigation and remediation for each suspicious activity.

**Adapt:** ATA continuously learns from the behavior of organizational entities (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly evolving enterprise. As attacker tactics get more sophisticated, ATA helps you adapt to the changing nature of cybersecurity attacks with continuously learning behavioral analytics.

**Reduce:** Traditional IT security tools are often not equipped to handle the rising amounts of data, turning up unnecessary red flags and distracting you from the real threats. With ATA, these alerts happen once suspicious activities are contextually aggregated to its own behavior as well as to the other entities in its interaction path. The detection engine also automatically guides you through the process, asking you simple questions to adjust the detection process according to your input.

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