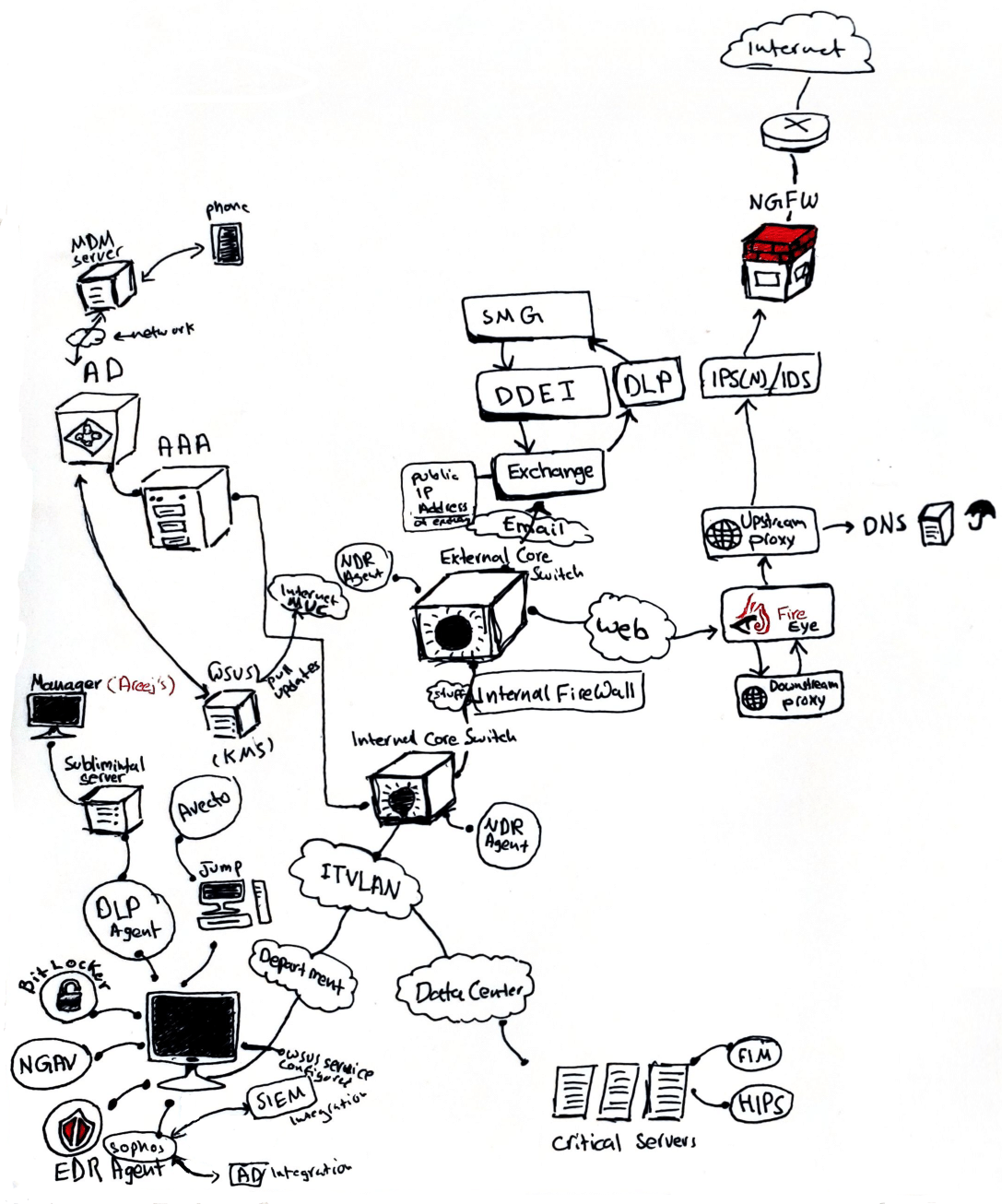


IT Platforms & Cybersecurity

# summary of solutions

|  |  |
| --- | --- |
| Solution | Brief Description |
| **SMG** | **Secure Mail Gateway** – Signature-based Email filtering |
| **DDEI** | **Deep Discovery Email Inspector** – Behavioral-based Email filtering (Sandboxing). |
| **Enterprise Vault** | Literally a “**vault**” that retains all emails for 15 years. |
| **EDR** | **Endpoint Detection & Response** – Full incident investigation for end points. |
| **TIP** | **Threat Intelligence Platform** – Collects information about new threats from all over the internet and the dark web, then analyzes collected info and produces meaningful insights. |
| **Convene** | Board Management Software. |
| **Avecto** | Enforcer of the “**Least Privilege**” security principle. |
| **DLP** | **Data Leakage Prevention** – Self Explanatory. |
| **Netwrix** | Session Monitoring, Recording, and Logging. |
| **MDM** | **Mobile Device Management** – Allows installation of business solutions into personal mobiles. |
| **VTPP** | **Venfai Trust Protection Platform** – Certificates Manager |
| **CA** | **Certificate Authority** – The bank has its own CA server. |
| **BitLocker** | Sophos, Safeguard – File encryption |
| **PGP** | **Pretty Good** **Privacy** – A solution to encrypt & decrypt and authenticate email messages (used internally). |
| **FIM** | **File Integrity Monitoring** - .. |
| **HIPS** | Host Intrusion Prevention System - |
| **Symantec** | End point protection. Next Generation Anti-virus. |
| **SEPC** | Symantec Endpoint Protection Cloud (SEPC) is mainly going to be used during clients “onboarding”, where they upload documents that need to be checked for maliciousness. |
| **Proxy** |  |
| **Netskope** |  |

# Network Archeticture



# Email Security

|  |  |
| --- | --- |
|  | **To ensure the security and legitimacy of outbound and inbound emails, three main parts of the email are checked: Header, Body, and Attachments. The header contains information about the email, the subject, the sender, receiver, etc. It also contains the “DKIM” and “DMARC” values, which are both used as digital signatures to prevent spoofing of emails.**  **Security solutions like SMG, DDEI, and DLP can take one of three actions: “Allow”, “Quarantine”, or “Delete” for each processed email. Following is the flow of external emails as they enter the Bank’s environment:** |

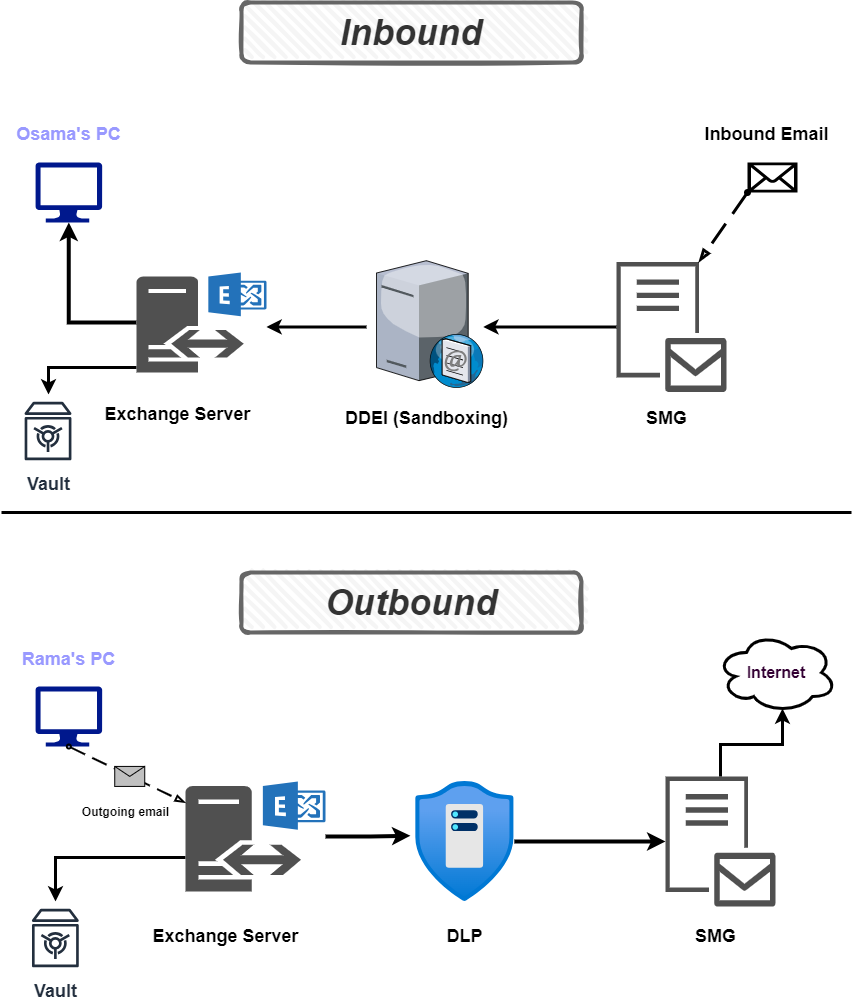


Figure 1: Flow of Inbound Emails

|  |  |
| --- | --- |
|  | **Symantec Messaging Gateway (SMG) is a Threat detection and an Anti-spam solution. For the most part, it is “signature-based”. It inspects every outgoing and incoming email in four main areas:**   * **Reputation: This focuses on the domain of the sender and whether it is malicious or legit. SMG maintains a huge database that can be either local, global, or a mix of the two. The global database is provided by Symantec and contains a list of globally malicious domains. The local database can be crafted locally, from the bank itself.** * **Extension of attachments: A list of allowable extensions can be created. Emails will be quarantined if they contain attachments not in the list. “Unrated attachments” that are encrypted or cannot be inspected will be quarantined.** * **Authority: Is the receiver of the email authorized to receive this email? Is the sender allowed to send this email?** * **Header: This is a check against the DKIM & DMARC values in the header of the email. Those are email authentication methods that use a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain. This check helps prevent external spoofing of Arab Bank domains.** |

|  |  |
| --- | --- |
|  | **Deep Discovery Email Inspector (DDEI) is a behavioral-based threat detection solution. It throws every incoming email into a “sandbox”, in where extensive analysis of the content of the email and attachments happens. DDEI is very efficient and really fast, it can process an entire email within just 1 millisecond. Following are some of the key use cases of DDEI:**   * **Web filtering and URL time-of-click analysis.** * **Malware identification via machine learning.** * **Custom sandbox, anti-evasion tech, behavioral analysis, ML-based C&C.** * **Supports Mitre ATT&CK framework for effective threat detection and response.** * **Spam & content filtering, and DLP.**   **DDEI’s custom sandboxes use virtual images to match system configurations, drivers, applications, and languages. Difficult to evade, they include a “safe live mode” to analyse downloads, URLs, C&C, and more. They identify ransomware, backup modification, and encryption. DDEI also uses machine learning inside the sandbox to enhance detection.** |

|  |  |
| --- | --- |
|  | **Every email, whether incoming or outgoing, is stored in a “vault” for later investigations. This vault is configured to retain emails for 15 years. An email sent 10 years ago could easily be found in less than 10 minutes. “Enterprise Vault” is the solution that provides such capabilities. For each employee, it creates a dedicated “journaling” mailbox, in where all emails are indexed and categorized properly. The quota of the journaling mailbox is UNLIMITED.** |

|  |  |
| --- | --- |
|  | **AB uses Windows Exchange Server, which is responsible for handling email traffic for the entire bank. When an email passes through SMG and DDEI, it is then sent to the Exchange Server, which then sends it over to the email agent (Outlook) for users to read. Additionally, it sends a copy of the email to the “Enterprise Vault” to retain emails.** |

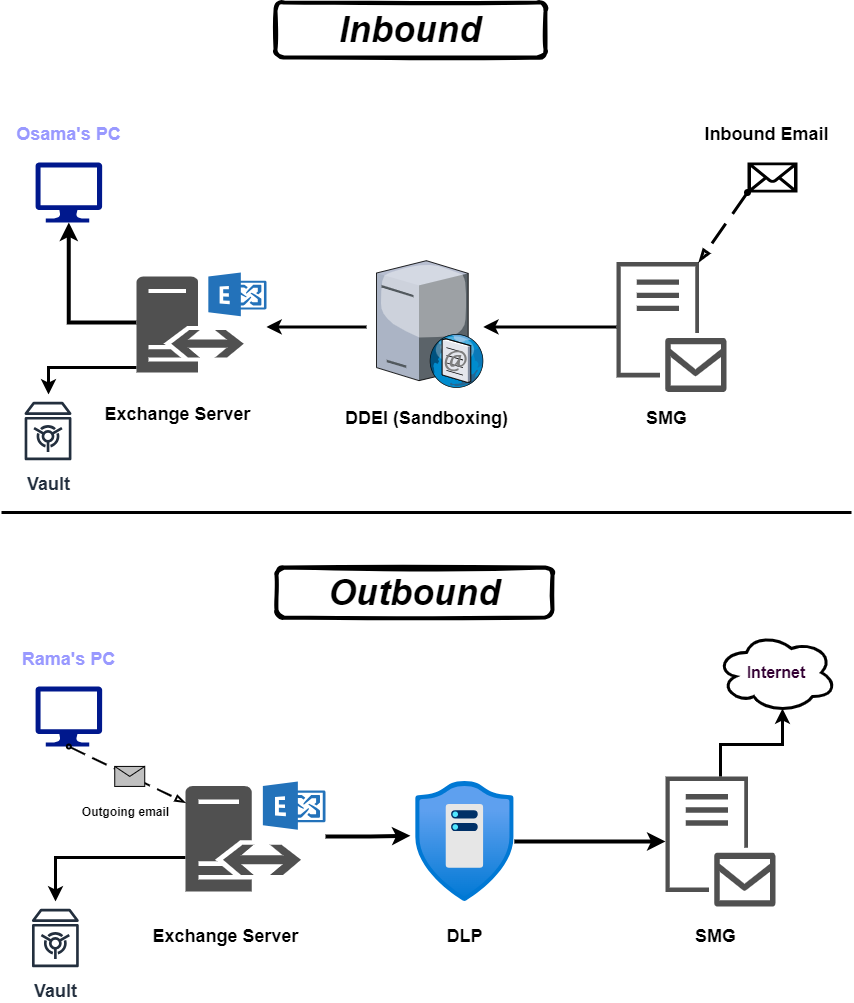


Figure 2: Flow of Outgoing Emails

# End Point Protection

|  |  |
| --- | --- |
|  | **HIPS.** |

|  |  |
| --- | --- |
|  | **EDR vs NDR vs XDR.** |

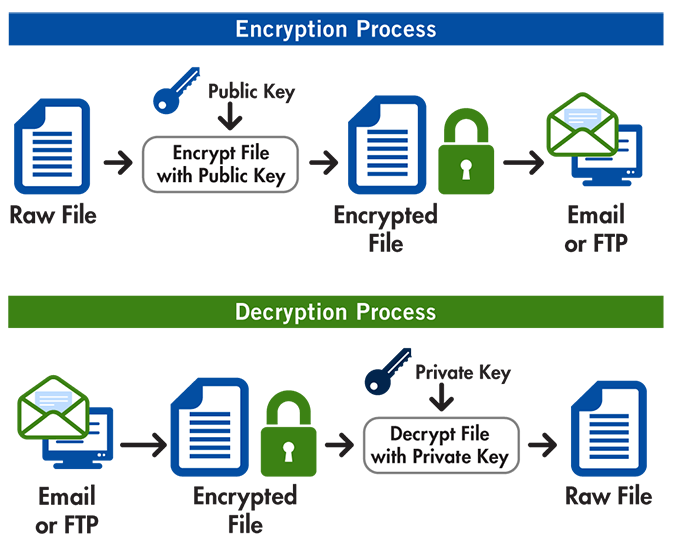
|  |  |
| --- | --- |
|  | **MDM** |

# Patch Management

|  |  |
| --- | --- |
|  | **WSUS** |

# Licenses & Certificates

|  |  |
| --- | --- |
|  | **VTPP** |



|  |  |  |
| --- | --- | --- |
| Team | Allowed to Access | Denied Access to |
| **HR** | Can only access the HR servers | Can't ping any server in the company |
| **IT** | Can access all IT & HR servers. | – |
| **Security** | Can only access IT / HR servers 1 and 3 | Cannot access IT / HR server (2) |