**Ikhala TVET College Email protection solution**

Table of Contents

[Executive Summary 3](#_Toc118050063)

[Ikhala TVET College Challenges 3](#_Toc118050064)

[Scope 4](#_Toc118050065)

[Proposed Solution & Solution Overviews 5](#_Toc118050066)

# Executive Summary

It is the college’s goal to acquire best of breed email security to protect our environment. The following proposal outlines Ikhala TVET Colleges current business challenges and objectives as per the cyber security recommended solution to address these core issues.

Based on our assessment, the following priorities were outline to well-equipped the institution:

* Reduce spam and viruses getting through Microsoft
* Reduce the number of targeted impersonation emails employees receive
* Improve the ratio of time spent on IT and Security projects vs. responding to incidents

The college requires next generation cyber security solution protect more than 10 000 account companies make email safer, restore trust, and bolster cyber resilience. The recommended solution must add layered protection to block unwanted email including spam, impersonation emails and other sophisticated threats, to prevent data, monetary, and reputation loss.

The College looks to:

* Prevent losses due to malicious email and employee error
* Reduce the cost and time spent administrating and monitoring threats
* Reduce the amount of spam employees receive
* Reduce the number of targeted impersonations that employees receive

# Ikhala TVET College Challenges

Business Challenges

* The number of sophisticated email threats, including impersonation and targeted email attacks
* The burden on the IT team managing an ever-compromised email system

Desired State

* Efficient IT team
* Improved security efficacy

Ikhala TVET College Requirements

* Prevent financial loss and exposure of sensitive, proprietary information.
* Consolidate your security solutions into a single administration console to reduce complexity and save IT and security teams’ time.
* Safeguard your organization against threats aimed at email, the number one attack channel

# Scope

|  |  |
| --- | --- |
|  | Licenses |
| Perimeter Defense Plan | 500 |
| Support | 1 |
| Implementation | 0 |

# Proposed Solution & Solution Overviews

**Perimeter Defense Plan:**

|  |  |  |
| --- | --- | --- |
|  | | Recommended  Solution |
| PERIMETER  SECURITY | SEG | ● |
| URL PROTECT | ● |
| ATTACHMENT PROTECT | ● |
| IMPERSONATION PROTECT | ● |
| INTERNAL  DEFENSE | INTERNAL EMAIL PROTECT |  |
| AWARENESS TRAINING | ● |
| MANAGED AWARENESS TRAINING |  |
| CYBERGRAPH |  |
| BRAND  PROTECTION | DMARC ANALYZER |  |
| BRAND EXPLOIT PROTECT |  |
| RESILIENCE  EXTENSIONS | PRIVACY PACK |  |
| BYO THREAT INTELLIGENCE | ● |
| SECURE MESSAGING | ● |
| BROWSER ISOLATION |  |
| CLOUD ARCHIVE |  |
| SYNC AND RECOVER |  |
| EMAIL CONTINUITY |  |
| ARCHIVE FOR TEAMS |  |
| EMAIL INCIDENT RESPONSE |  |
| WEB SECURITY | ● |
| LARGE FILE SEND | ● |

Solution Features and Benefits

The College requires the following services, support, implementation, and training options rated requirements.

The **Perimeter Defense Plan must** provide a single platform for email security, user awareness and threat intelligence. Fully integrates with other security vendors’ solutions to increase intelligence and decrease down time to respond to threats.

The **Perimeter Defense Plan** includes:

* Secure Email Gateway
* URL Protect
* Attachment Protect
* Impersonation Protect
* Mimecast Intelligence
* 100+ integrations into other ecosystem partners

Secure Email Gateway with Targeted Threat Protection

**The College requires an Email Security** that provides a single platform for email security, user awareness and threat intelligence. Must fully integrates with other security vendors to increase intelligence and decrease down time to respond to threats.

The Email Security must:

* Prevent financial loss and exposure of sensitive, proprietary information.
* Consolidate security solutions into a single administration console to reduce complexity and save IT and security teams’ time.
* Safeguard your organization against threats aimed at email, the number one attack channel.

Secure Email Gateway

Stop malicious and unwanted email

**Antivirus and Anti-Spam** – Deliver comprehensive protection via multilayered engines with an optimum mix of proprietary and best-of-breed third-party technology.

**Data Loss Prevention** – Protect your sensitive and confidential information from accidental or intentional exposure with fine-grained policy controls.

**Signature Disclaimer and Management** – Achieve consistency in all email communications with email signature and disclaimer management based on Active Directory credentials.

**End User Productivity Applications** – Boost employee productivity with self-service security, email and archive access features with apps built for Outlook, mobile, Mac and Web.

**Intelligent Email Routing** – Support complex on-premises, cloud or hybrid email environments and achieve rapid email system integration or separation associated with a merger, acquisition or divestiture.

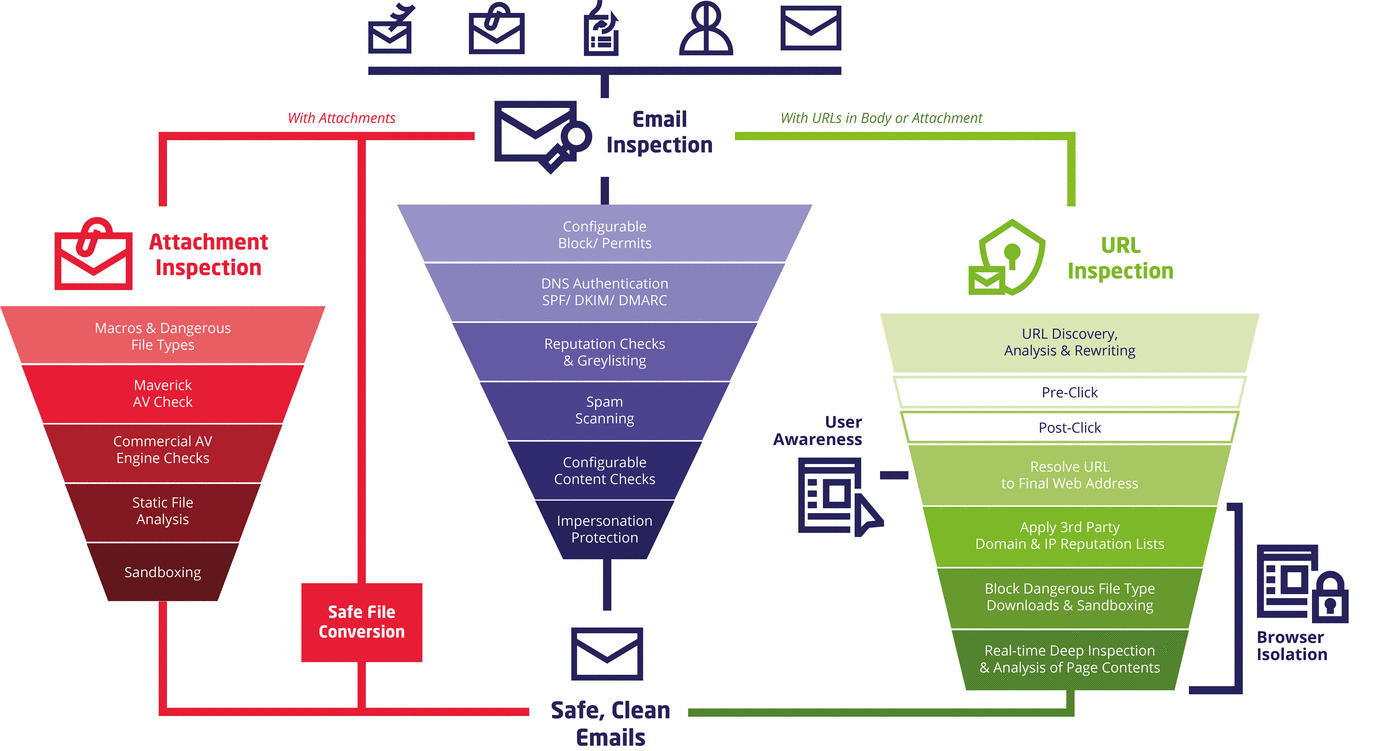
**Targeted Threat Protection**

Protect against impersonation, ransomware, and business email compromise attacks

**Impersonation Protect** – Protect against social engineering attacks, including business email compromise, CEO fraud and phishing, targeting your employees.

**URL Protect** – Protect your organization and employees against malicious websites containing malware, phishing and other threats through URL rewriting and on-click deep site inspection.

**Attachment Protect** – Defend against infection from weaponized attachments often used in ransomware, keylogger, Trojan and spyware attacks with multilayered inspection, including advanced static and dynamic analysis.



Email security Intelligence

Respond to threats faster and more effectively with email security Intelligence. Designed to give a deeper understanding of the cyber threats your organization faces, Mimecast Threat Intelligence provides you with expert analysis of detected attacks. The service provides threat data and analytics specific to your organization, either through an intuitive, web-based dashboard or via the Mimecast API Threat Feed.

The Intelligence solution must deliver the following information:

* Contextual, showing your organization’s security performance and trends.
* Actionable, designed to help take a more proactive approach to new and emerging threats.
* Easily consumable, so the insights can be used to communicate with other stakeholders in your organization.
* Instructive, designed to help you better understand the threats your organization faces.

**Email security solution:** Must have a threat Intelligence API to feed threat data into a third-party tool .

**Basic Support**

* Access to online support portal to manage all cases
* Twelve business-hour response SLA
* Online Mimecast Community
* Robust knowledge base
* In-product reporting
* Phone support routing during a P1 critical issue