IT SECURITY GAP ANALYSIS FROM KYTEC

Kytec

Kytec has created a framework and process to identify security risk in mid to large businesses and Government organisations. Kytec will gather information in two stages, then present recommendations on how security can be improved and business risk reduced.

Who can benefit from the Kytec Gap Analysis?

Security risk impacts a variety of roles because ultimately, IT security risk translates into business risk.

The Kytec Gap Analysis will have benefits for anybody who is responsible for IT security, and anybody impacted by IT security:

- **CIO**
- **IT Manager**
- **CISO**
- **Senior Executives including CFO**
- **The Board**

Customers, Partners and Suppliers also have a stake in your security as they need their information to be protected.

IT security risk translates into business risk.

The growing need for improved security

Security breaches are increasing year on year and the financial cost of these breaches is escalating. In particular, Ransomware attacks are becoming more prolific and debilitating. They have become a regular news story.

Accelerating the need for improved security is the increasing number of workers that are working at home or in remote locations; applications and data being decentralised across multiple clouds and locations and the increasing complexity of product-based 'point' security solutions that have the potential to create gaps and vulnerabilities.

Objectives of the Kytec Gap Analysis

1

To identify vulnerabilities in process and information flow that could lead to security breaches, resulting in direct financial loss, loss of information/IP, damaged reputation, no access to resources and data and penalties from lack of compliance.

The Gap Analysis aims to mitigate against the three primary attack vectors - Email, web & end point.

2

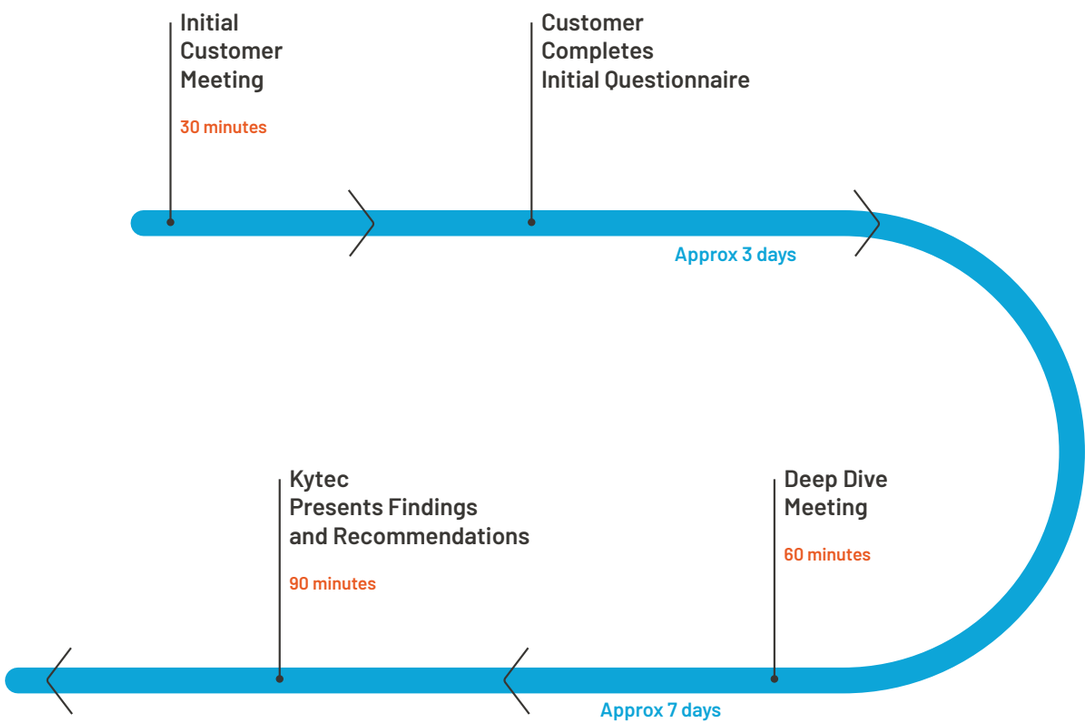
Assist in the fulfilment of common compliance requirements.
(ASD, ISO 27001, NIST and PCI-DSS)

3

Help organisations to understand their current state (security posture), their ideal state and provide recommendations on the best pathway to the ideal state.

Benchmarking is provided against best practice and industry norms.

The Gap Analysis Process



The first step in the Gap Analysis process is to fully understand your IT infrastructure, business priorities and main areas of risk. We work with all relevant stakeholders.

After an initial discussion, Kytec will send a questionnaire to gather an initial set of information in five key areas:

1. **Gateway security controls**
2. **Network**
3. **Endpoint**
4. **Administrative (policy/training)**
5. **Compliance, regulatory and risk**

Kytec will then use this information to structure a meeting, either face to face or via Webex, where we will deep dive into your environment and collect more detailed information.

Kytec will then collate all the collected information, create a set of key issues and recommendations and present these back to you.

An add-on option, is to run a vulnerability assessment which creates an inventory of all the devices in your network, including shadow IT, and provides a health check – for example, have all relevant patches been applied, are all operating systems up to date? It provides total visibility into your network and IT infrastructure.

Kytec is a Cisco Gold Partner and we believe that a single vendor solution is the most efficient and effective, however, we can recommend a solution that leverages your existing investment, ie, a multi-vendor solution.

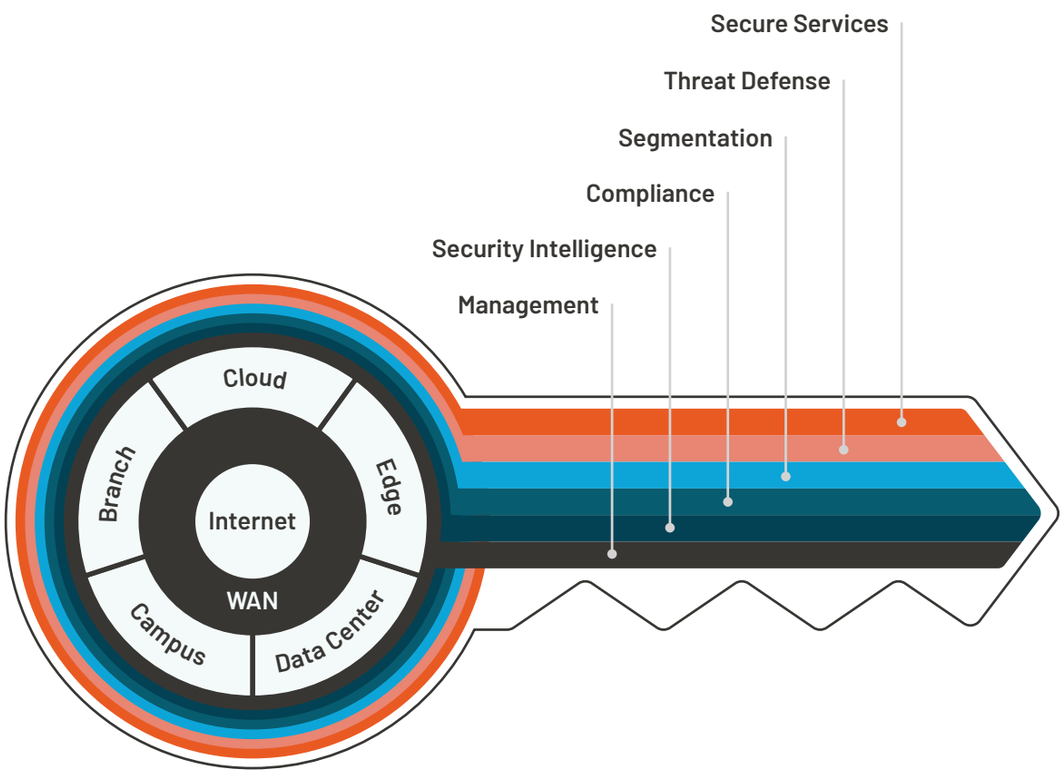
When providing recommendations, we aim to reduce complexity and operational expenses, we enable least privilege access to internal resources and plan for optimum protection against malware.

Kytec aims to reduce complexity and operational expenses, enables least privilege access to internal resources.

The SAFE Methodology

Kytec uses the SAFE methodology which is an architectural approach, leveraging the network, that focuses on addressing risks and threats by identifying the required capabilities, based on business, information and process flows. **SAFE** is vendor agnostic and focuses on function rather than product.

Capabilities can be viewed as building blocks.

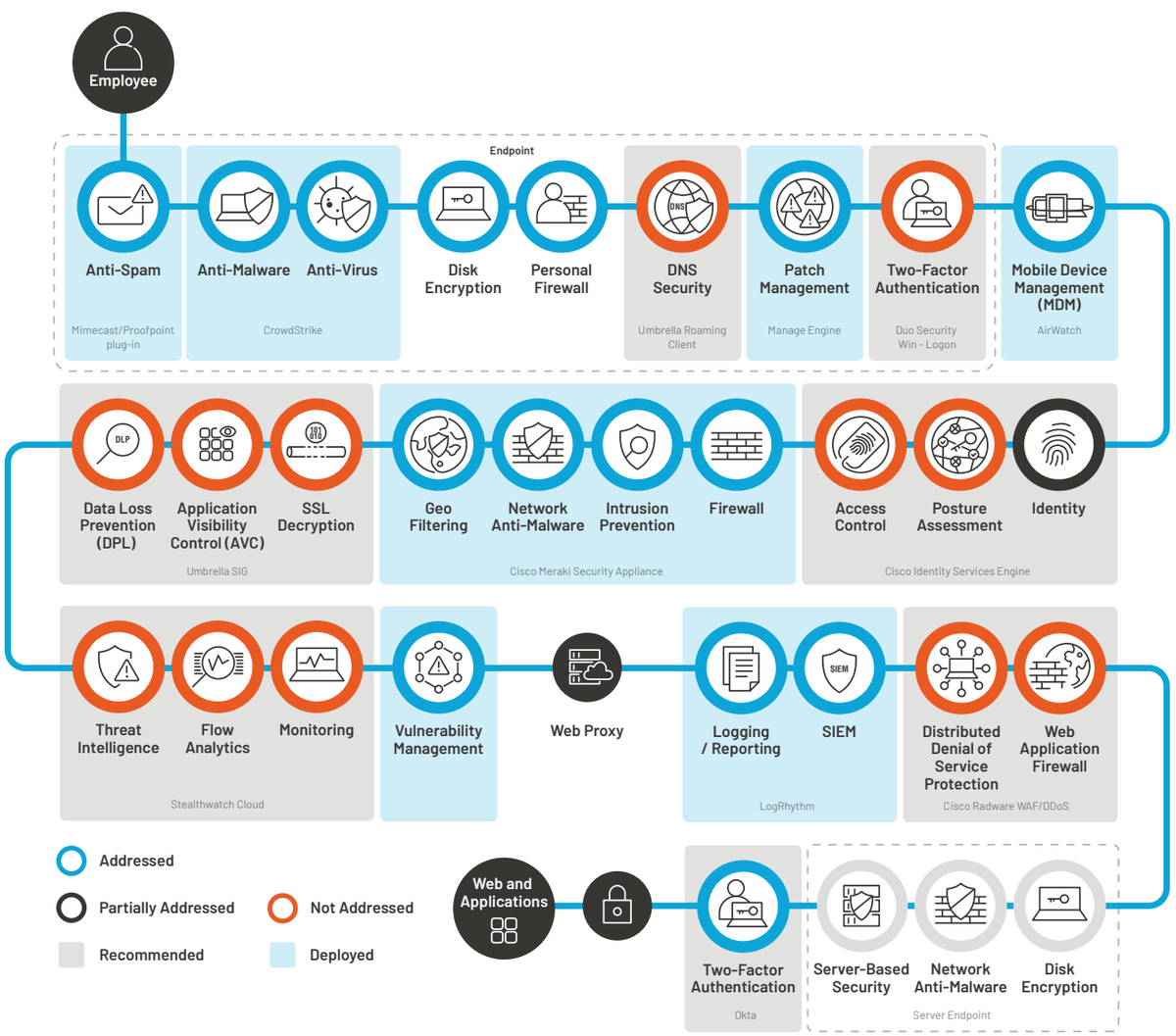


As part of the Gap Analysis, we will work with you on a critical business flow, and using the **SAFE** methodology, we will identify the capabilities required to secure this flow.

Business flow with gaps/vulnerability

A sample flow is shown below, with vulnerabilities highlighted.

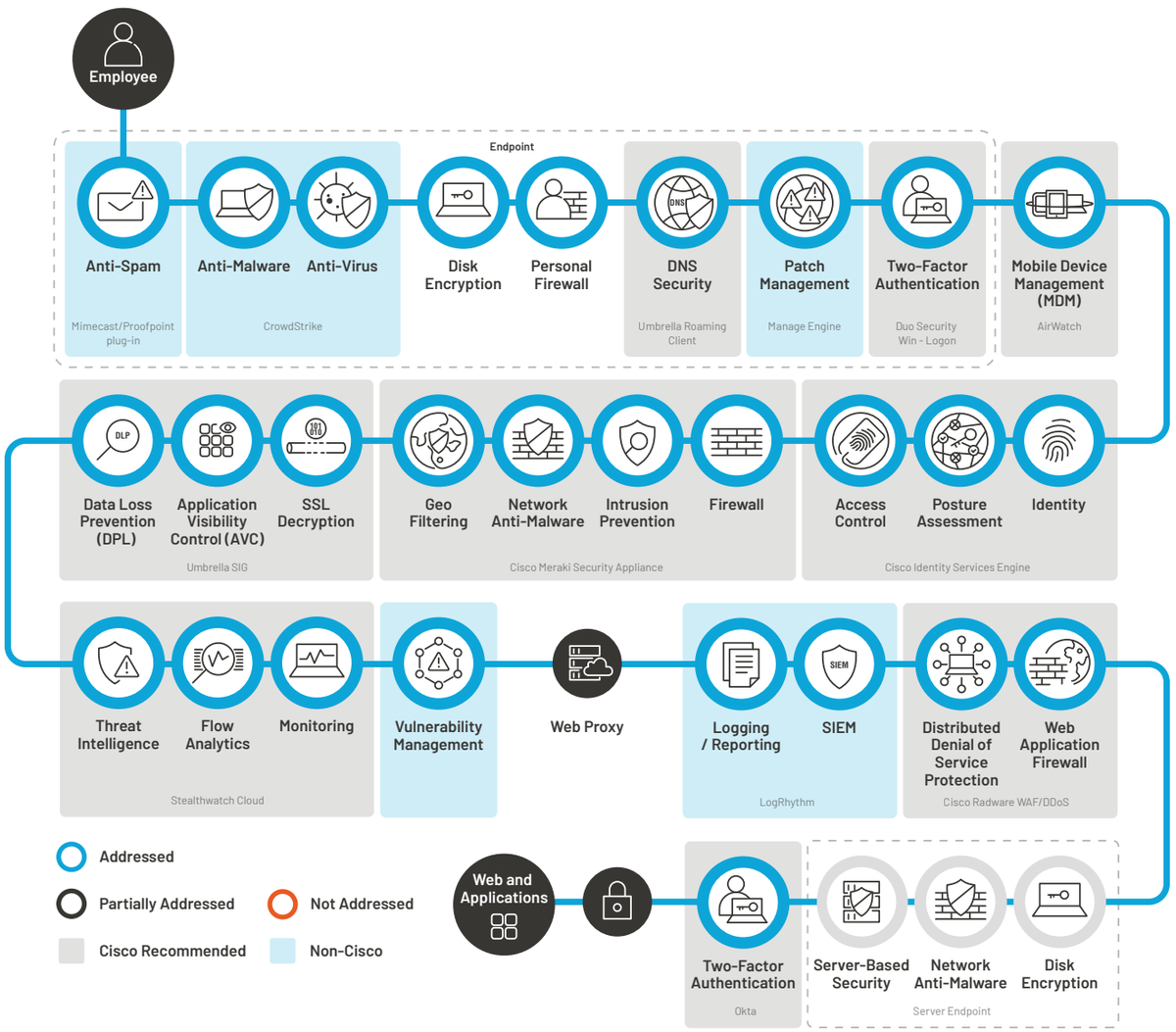
The flow below this shows that the vulnerabilities have been addressed.



Business flow with recommendations addressing gaps

Analysis of the business/information flow above highlighted a number of vulnerabilities, including DNS security, lack of two factor authentication, data loss prevention, DDoS protection and access control. All of which represent risk to the business.

By implementing recommendations from Kytec, the business/information flow is now fully secure. This is shown in the flow diagram below.



Developing a Zero Trust Security Model – Considerations

1

Do you have a clear identity and access management (IAM) strategy aligned with your business needs with full implementation and integration of a multi-factor authentication (MFA) solution supported by risk-based policies?

2

Do you have an up-to-date asset inventory that distinguishes between managed and unmanaged devices, providing a hygiene check as part of an integrated IT and security function?

3

Do you have a trusted device policy that prompts users to update their devices against measured vulnerabilities — within a managed process — and reports on out-of-policy devices?

4

Do you control user access through a centrally managed policy that identifies and acts upon exceptions?

5

Do you have a business-aligned zero-trust strategy supported by an architecture and set of processes that enables users to seamlessly access both on-premise and cloud applications?

"Zero Trust means organisations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access."

Why work with Kytec?

Kytec is a Cisco Gold Partner with accreditation in all architectural specialisations, including security. Our people are our greatest asset, both in terms of technical expertise and experience and relentless customer focus.

We focus on the needs and priorities of our customers and ensure we deliver tangible business benefits.

www.kytec.com.au
sales@kytec.com.au

cisco Partner

Kytec