Confidential

Bitdefender

Client Redacted

Cybersecurity Review Essentials Workshop.

Bitdefender APAC Pte Ltd
109 North Bridge Rd, #05-21, Singapore 179097

Document version
1.0

Document Control.

Version	Changes	Author	Reviewer	Date
0.1	Initial Draft	Bintang Wanda		13 October 2025
1.0	Final Report	Bintang Wanda	Niko Akatyev	16 October 2025

Document Distribution.

Name	Company	Email	Date
Client Employee	Client Redated	employee@clientreacted.com	16 October 2025

Table of Contents

1. Executive Brief

1.1 Introduction

Client Redacted ('Client Redacted') engaged Bitdefender with an objective to assess the state of their baseline security and identify top practical improvements that help them address relevant threats and reduce cybersecurity risks.

Small businesses with lean IT and security teams suffer similar cybersecurity challenges to their larger peers and competitors with extensive budgets and an army of security and risk management professionals. Client Redacted leverages 16 digital tools to run their innovative business, providing a larger target for ransomware and other threat actors.

Client Redacted is a small logistics business with fewer than 10 employees. Despite its size, the company serves several large clients as well as a number of smaller companies. As a result, it handles trade-sensitive information belonging to its larger clients and personal data relating to its smaller clients. Cybersecurity is therefore one of the company's growing priorities. It is essential for maintaining the trust of its larger clients, fulfilling its responsibilities in protecting personal data, and mitigating the risk of operational disruptions.

Between 9 October 2025 – 16 October 2025, Bitdefender performed a Cybersecurity Review Essentials Workshop (CREW) based on key best-practice controls derived from CSA Cyber Essentials, MAS Cyber Hygiene, UK Cyber Essentials, and Bitdefender Cyber Hygiene. The primary objective of this assessment is to evaluate the organization's current level of cybersecurity hygiene and deliver practical, actionable recommendations to address identified gaps in a comprehensive and effective manner. The results of the CREW also serves as a way to educate Client Redacted about relevant cyber threats and immediate measures they can take to reduce risks.

The scope of the CREW focuses on collecting insights through a structured self-assessment completed by the Client's primary Information Security contact, followed by a targeted workshop with that representative and additional stakeholders as needed. CTO, HR, and Legal joined the workshop session. The information gathered during these stages forms the basis of an actionable report detailing the organization's current cybersecurity posture and practical recommendations.

This report is comprised of three (3) key sections:

1. A gap assessment of essential cybersecurity controls, helping to safeguard both the company and its customers.
2. Practical recommendations to improve essential cybersecurity controls.

3. Summary of the relevant threats and top measures to reduce cybersecurity risks. Client Redacted can share that summary for the entire organization in order to improve knowledge about cybersecurity.

1.2 Summary

Based on the information collected during the questionnaire review and workshop, Bitdefender had the following top observations.

The company's strengths are:

1. The organization maintains a centralized inventory for laptops.
2. The organization enforced Multi-Factor Authentication (MFA for administrative accounts of their core systems, Google Workspace and HubSpot.
3. Endpoint protection with behavioral detection is deployed across corporate devices.
4. Standard hardening templates are applied to new workstations and servers.

The following is the top list of improvements that Client Redacted can start with as a checklist for immediate implementation. Client Redacted should address lower efforts, higher impacts tasks first.

ID	Finding	Business Impact	Efforts	Impact	Related Category	Owner
1	Enforce MFA for all critical systems including Xero, Docusign, AWS, and GitHub.	Reduce 90% of successful attacks such as stolen credentials that are major cause of breach for SMBs.	*Low*	*High*	*User Access Control*	DevOps, Legal
2	Disable offboarded employees from Google Workspace and limit administrative accounts to maximum two users (primary and backup).	Prevent unauthorized access to internal data by offboarded employees. Reduce the risk of the compromise of unmanaged and overprivileged accounts. Optimize cost of Google Workspace licenses by removing non-existent users.	*Low*	*High*	*User Access Control*	CTO
3	Identify and track critical systems and servers.	It is only possible to protect what is known. Identify critical systems and servers to apply fundamental security to them such as MFA, EDR installation, and hardening.	*Medium*	*Medium*	*Assets*	DevOps

4	Develop an incident response playbook for a most probable incident, a workstation compromise, and practice incident response.	It is not if but when an incident happens. Respond to incidents confidently and earn clients trust avoiding to be in 60% of SMBs that close or file bankruptcy after experiencing a breach.	*Medium*	*Medium*	*Incident Response*	CTO
5	*Sample Report*.				*Backup*	DevOps
6	*Sample Report*				*Security Awareness*	Finance

The detailed assessment results are elaborated in section 3.1. Detailed Gap Assessment Results.

2. Methodology

Bitdefender adopts industry best practices and methodologies and Bitdefender cybersecurity expertise to build methodology and approach for all security services. Bitdefender's CREW follows a structured approach in order to achieve a clear evaluation of the current state of the Client's environment and provide actionable recommendations.

2.1 Stages

The CREW is conducted as a project to assess organization's cybersecurity capabilities and controls, and align them with the organization's larger business goals in order to secure the organization and drive the business forward. The entire project is performed using a three (3) stage **approach** that is outlined in Figure 1. In order to provide an accurate assessment of Client's state for each of the areas covered by Cyber Essentials Domains, Bitdefender's analytical **methodology** is powered by three (3) assessment techniques which are outlined in Figure 2 below.

Figure 1. Staged Approach

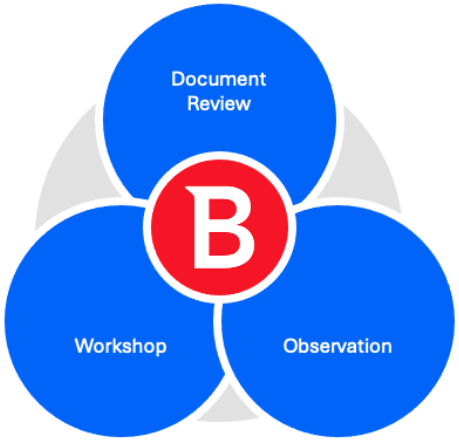

Figure 2. Assessment Techniques

2.1 Framework

Cyber Essentials

There are few essential cybersecurity controls mentioned by CSA Cyber Essentials, MAS Cyber Hygiene, UK Cyber Essentials, and Bitdefender Cyber Hygiene that must be in place to prevent majority of cyberattacks in the wild. The CREW checks the state of those essential controls and provides recommendations how to address them with minimum efforts.

Cyber Essentials Domains	
Assets	It is only possible to protect what defenders know about. The organization must identify all assets and relevant information that they store and process. The organization must grade the criticality of assets.
User access control	Control of access to data and services and what level of access person and non-person entities have. Normal users and administrative accounts are managed differently. Every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorized access to or use of such account. All administrative accounts must implement multi-factor authentication (MFA).
Secure configuration	The organization must set up computers and systems including cloud/SaaS securely to minimize ways that a cyber-criminal can find a way in. The security standards must be define and documented at least for critical systems.
Malware protection	Measures to identify and immobilize viruses or other malicious software before it has a chance to cause harm.
Incident response	It is not “if” but “when” the incident happens. The organization must be ready to respond an incident. A documented and practiced incident response plan is essential for effective incident response.

Security update management	Prevention of exploitation of vulnerabilities by cyber criminals when they find them in software as an access point to the organization’s systems.
Firewalls and security groups	Configuration of the network to limit exposure and restrict all unauthorized network traffic.
Backup	Data backups are critical for enabling quick recovery from cybersecurity incidents such as ransomware or malware, and physical disruptions such as system failures, theft, or natural disasters.
Security awareness	Employees are the first line of defense in the organization and the weakest link in the security chain, as cyber attackers increasingly use social engineering techniques to target them for their agenda. Therefore, it is essential for all employees to be well-trained to identify these techniques, mitigate them, and report any suspected incidents promptly

3. Gap Assessment Results

Based on Bitdefender's assessment of the information collected and shared with our consultants between 9th October 2025 – 13th October 2025, Bitdefender observes that Client Redacted implemented several fundamental cybersecurity controls, but it needs to establish its consistent application across critical systems and data as cyber criminals only need to find one loophole to own it all.

3.1. Detailed Gap Assessment Results

Bitdefender's observations of Client's cybersecurity state of each Cyber Essentials Domains are as follows. Recommendations using the verb "shall" indicate important actions that the organization needs to address as soon as possible. Recommendations using the verb "should" indicate actions that the organization may implement when the available resources allow this, or when the urgency increases in the future.

Category	Current State	Recommended Actions to Address Gaps
Assets	Document reviews of the IT Policy, combined with responses from the self-assessment questionnaire, indicate that the organization has established foundational processes for identifying and managing some IT assets for laptops of employees. A key strength observed is that the organization maintains a centralized inventory covering laptops of employees. The organization tracks partially some business applications. However, the organization does not identify and track consistently other important assets such as servers, cloud resources, network equipment, removable media, and remaining business applications. The ownership and classification metadata are not captured for core systems, supporting traceability and accountability.	Phase 1: Identify and track critical systems and servers. Phase 2: Etstablish and document a process to identify assets at the organization and grade their criticality. Phase 3: Expand the scope of the centralized asset inventory to include all hardware (e.g., switches, access points), software, and cloud-native services. Phase 4: Integrate asset inventory with configuration and endpoint management tools to enable automated discovery and reduce manual effort.

Category	Current State	Recommended Actions to Address Gaps
User Access Control	Based on the review of the Access Management Standard and supporting documentation, Client Redacted has established several foundational access control requirements. The documentation clearly specifies that multi-factor authentication (MFA) is enforced for administrative accounts, demonstrating a strong control for protecting privileged access. However, during the workshop session, Bitdefender identified that several Legal and Marketing systems did not have MFA enabled for users and administrators. During the review of provided materials, Bitdefender did not identify clearly defined processes or controls for identifying and managing inactive or dormant user accounts. The absence of a documented mechanism to routinely remove or disable unused accounts may lead to prolonged retention of unnecessary access, which increases the risk of unauthorized system entry.	Phase 1: Enable MFA for all administrators. Remove legacy accounts of employees who left the company. Phase 2: Limit the number of administrators per system. There should be maximum tow administrators, primary and backup. Enforce MFA for all critical systems including Xero, Docusign, AWS, and GitHub. Phase 3: Define explicit requirements for handling dormant accounts, including criteria (e.g., inactivity thresholds), monitoring procedures, and timelines for deactivation. Enforce MFA for all users in all systems where it is supported.
Secure Configuration	*Sample Report*	*Sample Report*
Malware Protection	*Sample Report*	*Sample Report*
Incident Response	*Sample Report*	*Sample Report*
Security Update Management	*Sample Report*	*Sample Report*
Firewalls and Security Groups	*Sample Report*	*Sample Report*
Backup	*Sample Report*	*Sample Report*

Category	Current State	Recommended Actions to Address Gaps
Security Awareness	*Sample Report*	*Sample Report*

~ End of Report ~
October 2025, Bitdefender APAC Pte Ltd