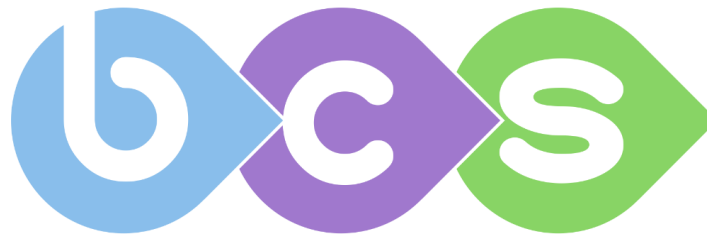


Prepared for:

Company ABC



In the following pages you'll find your customised Audit Report. It contains all of the information gathered from your IT environment summarised into one easy to read document. Upon reading, you will have a much better understanding of your IT plan and what you're spending.

YOUR CUSTOMISED REPORT

Based on our technical analysis of your IT environment, we have customised a selection of audit items spread across one or more main areas of technology. Each of these areas will give you important insight into the strengths and weaknesses of your IT plan.

YOUR AUDIT SCORE

Using the results of your audit, we calculated your overall audit score. The higher your audit score, the greater efficiency at which you are spending on technology. Our goal is to drive your audit score as close to 100 as possible.

The Comparative Analysis page allows you to easily compare your baseline plan with other plans presented in this document to see qualitative, quantitative and financial results.

HOW TO READ YOUR REPORT

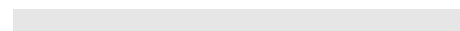
Each audit item has been color coded to make it easy to visualise your results. Red indicates an audit item that requires immediate attention, yellow indicates an audit item that needs improvement and green indicates an audit item that is satisfactory.

In addition to a Summary page, you will find dedicated pages with color coded summary statements for each individual audit item. Any audit item that isn't satisfactory is described in greater detail and its relative importance is explained in a single page infographic.

What is an audit?



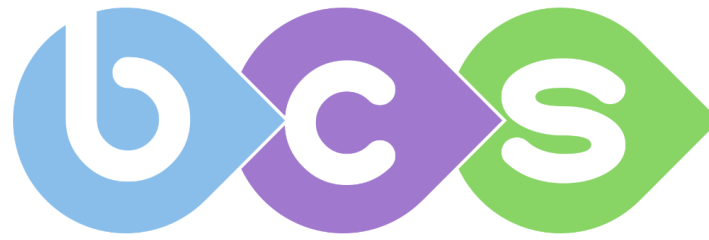
Base Plan



Summary

Detail

Library



Base Plan

Plan Type: Business Review

Technology Audit

What is an audit?

Base Plan

Summary

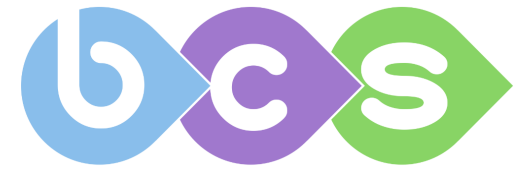
Detail

Library

Summary

Business Review

Technology Audit



BASE PLAN SUMMARY

The results of each quadrant of your base plan audit is summarised here using color coded boxes. Utilising a weighted scoring system, the results were combined and averaged into an overall audit score. Individual category scores and details for each audit item are shown in subsequent pages. Your base IT monthly expense is shown as a range and has been converted into an "effective" monthly expense based upon your audit score. This helps to level the playing field when comparing plans.



What is an audit?

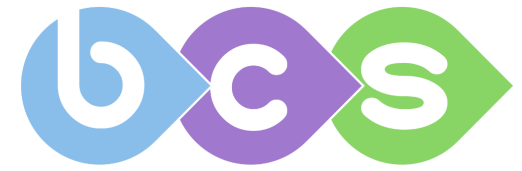
Base Plan

Summary

Detail

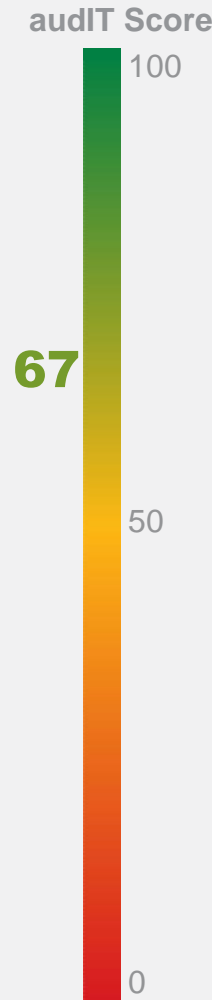
Library

Audit Detail



INFRASTRUCTURE

<p>Server</p> <p>Physical hardware is within refresh cycle and fit for purpose. All Virtual Servers have separated roles as per best practice. All OS's are supported.</p>	<p>Redundancy</p> <p>One Physical server running multiple VM's all backed up with full BDR. Suggest moving critical services to Microsoft Azure to give redundancy.</p>	<p>Workstations</p> <p>Most machines are within the refresh cycle. All running latest Windows 10 Updates. Planned upgrades are in progress for remaining.</p>
<p>Cabling</p> <p>Cabling is ageing CAT5E, however, working as expected no reported issues. Suggest getting all ports tested and look at upgrading in the future.</p>	<p>Scalability</p> <p>Currently limited by Physical Hardware. More services need to be moved to Microsoft Azure where we can expand when required without capital cost.</p>	<p>Switching</p> <p>Switchgear is fully managed, stacked and PoE capable. The configurations are fully documented using BCS Documentation tool.</p>
<p>WAN Redundancy / Failover</p> <p>Primary Connection is a Leased Line and Backup FTTC is in place for failover.</p>	<p>High Availability</p> <p>Firewall is not highly available. Suggest getting another managed UTM and run in High Availability due to how critical connection is at Head Office.</p>	<p>Managed Wireless</p> <p>No Managed Wireless in place. Access Points are running older wireless standards giving performance issues and no captive portal for Guest wireless.</p>



■ Requires Immediate Attention
 ■ Needs Improvement
 ■ Satisfactory

INFRASTRUCTURE

Infrastructure is the foundation upon which all of your technology rests. Just like with a house, it's extremely important to verify its integrity before you begin to build on top of it. Poor initial design decisions can lead to downtime, lost sales and ultimately drive up your total cost of ownership. This detailed analysis page represents an overview of the state of your Base Plan Infrastructure. Each audit item is summarised and color coded for easy identification and the results for this section are reflected in the Infrastructure audit score.



What is an audit?

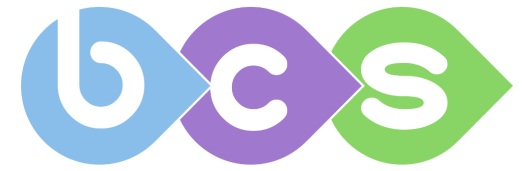
Base Plan

Summary

Detail

Library

Audit Detail



SECURITY

Security is arguably the most important section of your audit report. With so much riding on the security of your infrastructure, you can't afford to have any deficiencies. Fortunately, there's an abundance of security solutions available to help mitigate the risks and protect your data. This detailed analysis page represents an overview of the state of your Base Plan Security. Each audit item is summarised and color coded for easy identification and the results for this section are reflected in the Security audit score.

SECURITY

audit Score

100

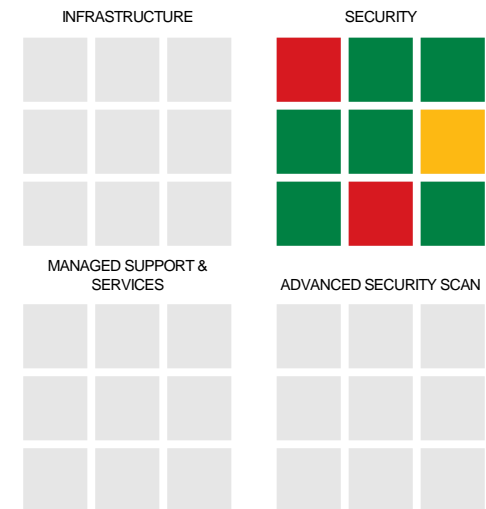
72

50

0

<p>Anti-SPAM and Virus Filter</p> <p>No Advanced Threat Protection in use. Suggest investing in ATP to ensure all emails are scanned for malware and filters are in place to stop attacks.</p>	<p>Physical Security</p> <p>Access to the building is controlled via Electronic locks. All passes are audited and visitors are given guest passes. The server room is locked.</p>	<p>Two Factor Authentication</p> <p>MFA is in place for Office 365. Suggest getting in place for Active Directory accounts to ensure total 2FA is in place.</p>
<p>Email Archiving</p> <p>Email Archiving application is in use. All email is Journalled and auditable.</p>	<p>Managed DNS</p> <p>DNS Protection is used on site. All traffic is filtered with no exceptions.</p>	<p>Password Management</p> <p>Password Manager is used for IT Accounts but not used for all staff members. Suggest this is implemented for all Staff Members.</p>
<p>Password Policy</p> <p>Password policy is in place on-site. Enforced complexity and set at 12 characters, this is reset every 6 months. MFA is also used alongside.</p>	<p>Email Encryption</p> <p>No Email Encryption is used on site. Suggest implementing Advanced Threat Protection to ensure data leaving is encrypted.</p>	<p>Endpoint Encryption</p> <p>All Laptops and Workstations are Encrypted with BitLocker. Suggest also looking at external drives and getting an Encryption policy in place.</p>

■ Requires Immediate Attention
 ■ Needs Improvement
 ■ Satisfactory

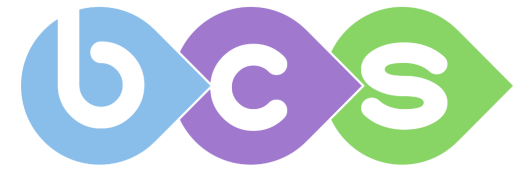


What is an audit?

Base Plan

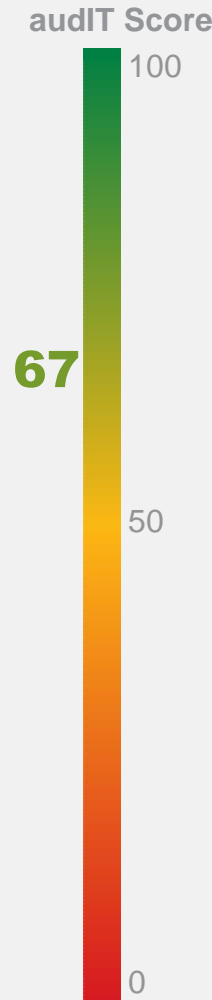
Summary **Detail** Library

Audit Detail



MANAGED SUPPORT & SERVICES

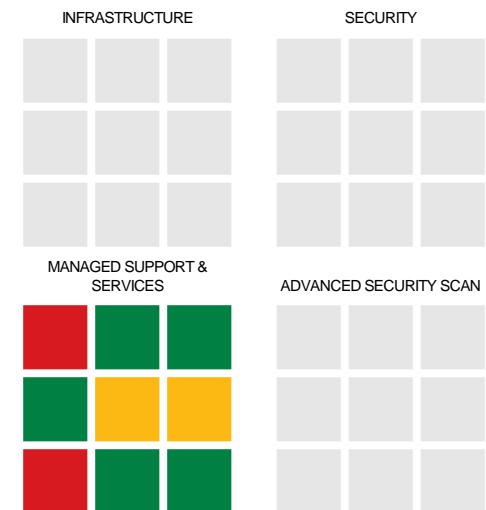
<p>Chief Information Officer</p> <p>No dedicated CIO/vCIO assigned to the business. This role is to advise and act on IT related issues/strategy at board level.</p>	<p>Proactive Maintenance</p> <p>Proactive maintenance of server(s) and workstations is automated and included in the plan.</p>	<p>Managed Backup</p> <p>Full BDR is being used on site. All servers are imaged and replicated offsite every 15 minutes.</p>
<p>Monitoring</p> <p>Monitoring of server(s) and workstations is automated with scripted remediation and included in the plan.</p>	<p>Line of Business Application(s)</p> <p>CRM is hosted on-site running on an older OS. Suggest migrating to Cloud hosted edition or migrating to Microsoft Azure "Platform as a Service".</p>	<p>Network Documentation</p> <p>Excel documents containing IPs of infrastructure however no official documentation or floor plans.</p>
<p>Mobile Device Management</p> <p>No mobile device management (MDM) is in use for smartphones with email accounts configured.</p>	<p>Help Desk Support</p> <p>Remote Help Desk Support is included for all supported endpoints and services.</p>	<p>Inventory & Asset Management</p> <p>Inventory & Asset Management is automated, included at no additional cost and reviewed quarterly.</p>



■ Requires Immediate Attention
 ■ Needs Improvement
 ■ Satisfactory

MANAGED SUPPORT & SERVICES

Managed Support & Services is the most efficient way to minimise reactive support and proactively manage your infrastructure. In exchange for a fixed monthly fee, outsourcing support helps improve operations while reducing your overall expense. This detailed analysis page represents an overview of the state of your Base Plan Managed Support & Services. Each audit item is summarised and color coded for easy identification and the results for this section are reflected in the Managed Support & Services audit score.

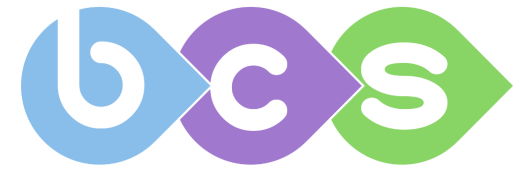


What is an audit?

Base Plan

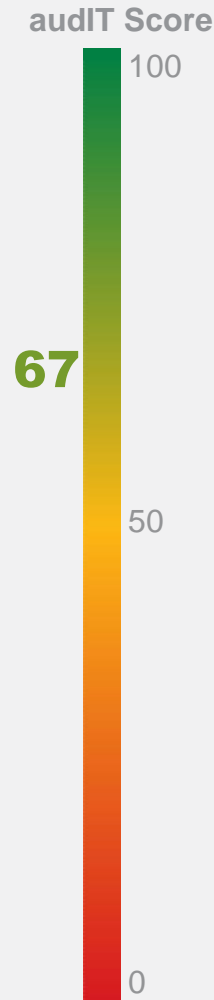
Summary
Detail
Library

Audit Detail



ADVANCED SECURITY SCAN

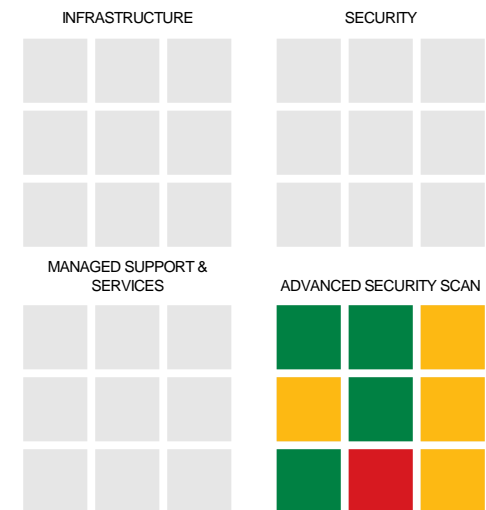
Anti-Virus Anti-Virus is corporately managed by a cloud based subscription and all endpoints are up to date.	Active Directory Security Active Directory is secure. No legacy accounts or computers. All machines are domain joined and secure sessions are enforced to the Domain Controller.	Network Vulnerabilities Our advanced scan has notified there are potentially unsecured ports left open on some network computers.
Security Policy Security Policies are robust and well managed. However, there is no process to review the policies after a certain time window and validate them.	Domain Computer Policy Machines are set to automatically lock, this reduces risk of users leaving machines unlocked and access for unauthorised people possible.	Windows & Application Updates Windows is up to date however applications are not. Need to ensure CRM applications and other installed apps are updated to ensure no vulnerabilities.
Security Awareness Training All users undertake security training as part of their onboarding. This ensures there is a base level of knowledge throughout the company.	Dark Web Monitoring No dark web monitoring is in place; compromised credentials found on the Dark Web.	Patching Windows updates are deployed however this is in an unmanaged fashion. All patches are installed and devices set to install all updates automatically.



■ Requires Immediate Attention
 ■ Needs Improvement
 ■ Satisfactory

ADVANCED SECURITY SCAN

Building on the basic security aspect of the report, this more in-depth section takes a look at security policy, application maintenance and potential network vulnerabilities. The report also highlights any shortfalls in end-user Cyber Security Awareness Training. This is something that in today's threat landscape, represents a significant risk to overall network security. This audit also looks at any PII (Personal Identifiable Information), that has been compromised and is available to cybercriminals via the Dark Web, including but not limited to: names, addresses and passwords.



What is an audit?

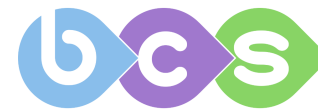
Base Plan

Summary

Detail

Library

ANTI-SPAM & VIRUS FILTER



SINCE 2001, THE THREAT LANDSCAPE HAS DRAMATICALLY CHANGED

from unorganized, electronic vandalism to funded, organized theft of personal data, intellectual property and financial information. Protection against these threats begins with modern software and workstations running the latest operating system. Today, many offices allow employees to bring their own devices to the office. While this increases flexibility and productivity and helps lower costs, it also makes your data more vulnerable to attack. Proactively managing all endpoints and ensuring that they are up to date and supported is of paramount importance to your IT infrastructure.

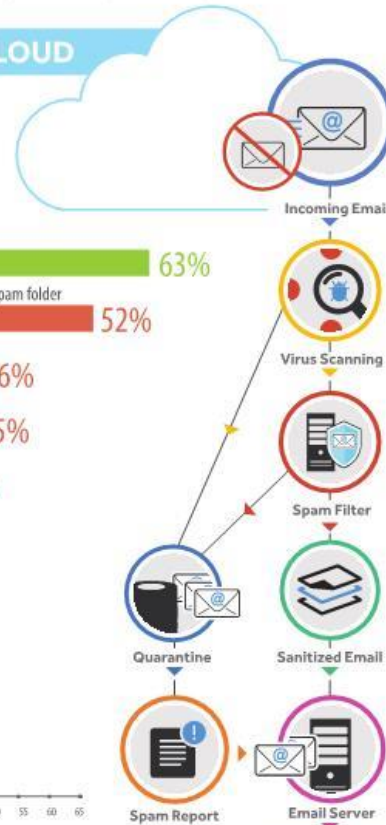
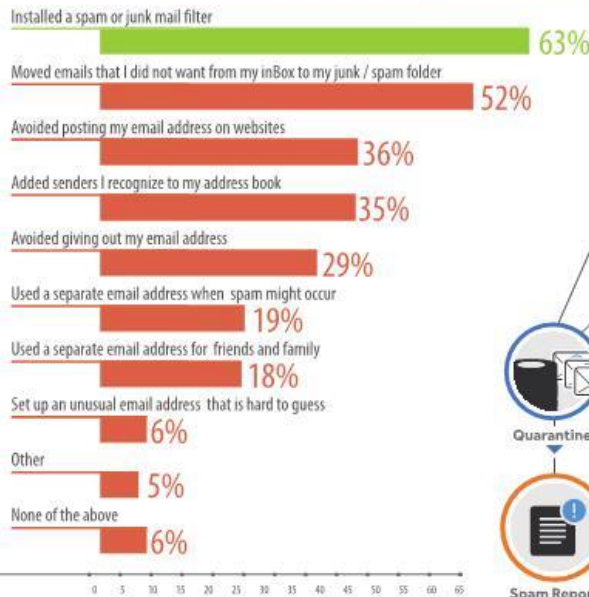


WHY IS THIS IMPORTANT?

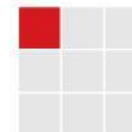
One of the main ways viruses and other malware infiltrate a network is through email. With so much riding on the high availability of an electronic communication system, it is important to add a 3rd party layer of filtered protection. Most filters will allow for the simple release of quarantined messages and include a daily report of held email for review. You should consider a filter separate from your email server or hosted provider. That way, if there is any type of outage and email can't be delivered, your anti-SPAM filter will hold the messages and deliver them when the server becomes available.

CLOUD

HOW DO YOU KEEP YOUR INBOX FREE OF SPAM?



SECURITY



END POINTS



What is an audit?

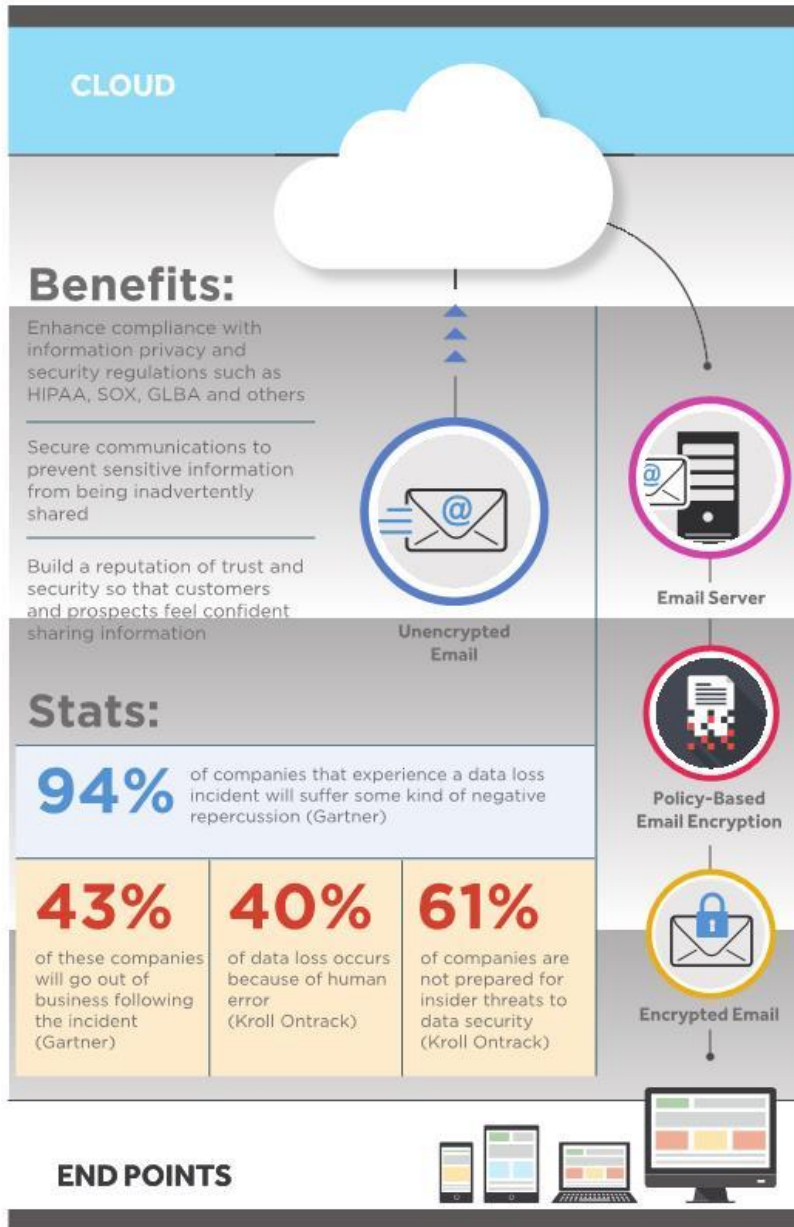
Base Plan

Summary

Detail

Library

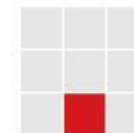
EMAIL ENCRYPTION



WHY IS THIS IMPORTANT?

Most emails are currently transmitted in clear text which means they are susceptible to eavesdropping and the subsequent disclosure of personally identifiable information (PII). Email encryption is encryption of email messages to protect the content from being read by entities other than the intended recipients and it may also include authentication. You should never send PII such as social security numbers, driver's license numbers or passwords using unencrypted email.

SECURITY



What is an audit?

Base Plan

Summary

Detail

Library

DARK WEB MONITORING



CLOUD

HOW ARE CREDENTIALS COMPROMISED?

What Can an Attacker Do with Compromised Credentials?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

Monitoring

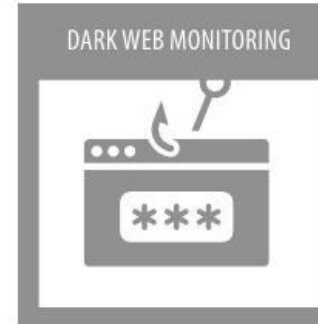
Phishing

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

Web Attacks

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

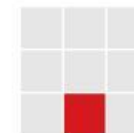
END POINTS



WHY IS THIS IMPORTANT?

Your business is at constant risk of a security breach. When identity information is accessed and stolen, it is often traded on the "Dark Web". This underbelly of the Internet is shrouded in mystery, hidden from most search engines and can only be accessed by a special web browser. Dark Web monitoring, or cyber monitoring, allows you to monitor your personal information and receive notifications if your credentials, passwords or other personally identifiable information is found online. Dark Web monitoring is also the best way to check on the effectiveness of your security awareness training program.

ADVANCED SECURITY SCAN



What is an audit?

Base Plan

Summary

Detail

Library