SMBsecure™ ADVANCED

Protection & Compliance Tailored for SMBs

Practical, Affordable and Effective cybersecurity suite with broad risk coverage - bundled value and made simple for a **Guaranteed ROI.**

Overview of Service

SMBsecure™ is tailored to help your small business stay secure and earn trust while remaining compliant.

SMBsecure™ is an inexpensive all-in-one fully managed service to de-risk your business with device & email attachment encryption, device lock & kill, phishing defence, cyber risk awareness education, reporting, proof of data encryption layered access controls and cybersecurity risk discovery. Easily add-on Financial Protection for Data Breach, Cyber Extortion and Business Email Compromise with the bespoke SMBsecure Cyber Warranty.

HOW IT WORKS

SMBsecure™ leverages patented technologies from leading and world class technology vendors that can be deployed in minutes to make securing data on PCs, Macs, USBs, Mobiles and Emails a **Total Breeze.** Valuable addons provide additional governance, risk and compliance (**GRC**).

MANAGED CYBERSECURITY RISK DISCOVERY

The **SMBsecure™** managed Cybersecurity Risk Discovery service identifies risk in five security areas: Network, Data, Application, Identity & Access Policies, and Social Engineering susceptibility. It also provides your business with Dark Web Monitoring & M365 and Google Workspace Account Security.

AVOID EMAILING WRONG RECIPIENTS

> More than 83% of users realize a mistake seconds after hitting Send!
Protect from the risk of confidential information being emailed to wrong people. Get users to review and confirm recipients when emails are sent.

MULTI-FACTOR AUTHENTICATION

SMBsecure™ fortifies access security on PCs, Macs and Windows Servers by verifying user logons with 2FA to **Stop a Breach Before It Occurs!** Secure against the use of weak, stolen, and re-used credentials and prevent unauthorised access for any local or remote (**RDP**) computer logons.

CYBERSECURITY AWARENESS TRAINING

SMBsecure™ offers Cybersecurity Awareness Training and Phishing Simulations to continually enhance user knowledge regarding cybersecurity risk, protocols, and overall cyber awareness within organizations - *backed with a free **Check4Phish™** service and **Dark Web Monitoring** for the user.*

PC & MOBILE DEVICE ENCRYPTION

SMBsecure™ implements the use of data encryption on PCs, Macs, USB drives and mobile devices to secure data on lost or stolen devices – *with audit-backed proof of encryption for **POPI/DPR** or security validation.*

PDF EMAIL ENCRYPTION

SMBsecure™ plugin for the classic Microsoft Outlook on Windows PC provides integrated, automatic password-protected **SecurePDF** to safeguard emailed correspondence *(file attachments)* with end-to-end encryption.
+ ***FREE*** Unified, Automatic and On-Demand password sending via SMS.

ACCESS CONTROL & AUTOMATIC INCIDENT RESPONSE

SMBsecure™ provides both admin-initiated or automatic security (defence) measures (e.g., alerts, warnings, soft or hard lockouts, network isolate, geofencing, kill, and locate functions) to prevent data exposure and unauthorized access on PCs, Macs, USB Drives, Phones, Tablets. **Boot-Level Authentication** adds a critical security layer before the Windows even boots.

+ MORE

+ Compliance Toolkit + Managed DMARC & TLS + Cyber Warranty + More

SMBsecure™

Managed Cybersecurity Risk Discovery

Holistic Risk Assessments | Analysis | Dark Web Exposures

Overview of Service

SMBsecure™ includes comprehensive scanning to discover and assess external and internal risks *plus* reporting with distilled insights for easy understanding and review.

This service enhances your cybersecurity posture and credibility with clients, suppliers, regulators and insurers. It empowers your business to take meaningful actions to mitigate key cybersecurity risks to safeguard its resilience in the wake of increasing vulnerability exploitation by attackers.

Reduce Your Business Risk with SMBsecure™.

HOW IT WORKS

This **SMBsecure™** service enhances safety for your business. Fundamental security risks that could harm your business's integrity are assessed, reported, and continually monitored for you. This service includes ongoing monitoring to identify your business's key vulnerabilities, such as open ports, easily exploitable software installed on your systems, weak passwords, dark web exposures and more.

It's more than a scan, it's a monthly service to map risks and keep your business secure!

ESSENTIAL RISK CONTROL FOR YOUR BUSINESS

SMBsecure™ Standard and Advanced subscriptions include a managed cybersecurity risk discovery service to assess your domains and business systems for key vulnerabilities which weaken your cybersecurity posture. It focuses on several areas which can be exploited by attackers to gain unauthorised access to systems and data which, *if exploited,* can result in serious costs for your business, damage your business's reputation, or cause harm to third parties including your customers and suppliers.

HOLISTIC ASSESSMENTS

SMBsecure™ does internal and external scanning to help your business identify and address vulnerabilities and improve security posture. It reviews and itemizes risks comprehensively across a broad attack surface including *(but not limited to)* finding exposed data on the dark web's underground marketplaces, forums, and illicit websites; vulnerabilities in software and cloud applications; AI exposure; network security (open ports, misconfigurations, DNS health, etc.); financial exposure; security hygiene; data encryption status; weak, breached and re-used passwords; typo squatting; inventory of SaaS applications, presence of personally identifiable information (**PII**); and more.

M365 AND GOOGLE WORKSPACE SECURITY AUDITING

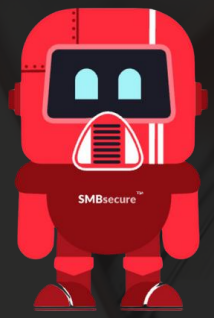
SMBsecure™ easily integrates with Microsoft 365 and Google Workspace. This empowers you to manage your Microsoft 365 or Google Workspace security posture with insightful data and reports. It assesses **MFA implementation** status for all user accounts for your tenant. The service audits and tracks logon attempt for ***suspicious activities,*** highlighting successful and failed logins neatly displayed on a **Geo Map.**

INSIGHTFUL REPORTS & REMEDIATION PLANS

SMBsecure™ managed cybersecurity risk discovery provides meaningful reports to help you understand your business's exposure to cyber events. Additionally, remediation plans are provided to help address vulnerabilities.

EASY IMPLEMENTATION

External Security scans require no installation and tests your business' public-facing systems and networks for security vulnerabilities. It is performed from the outside, simulating the perspective of an attacker. Risk Assessments quantifies the security posture of your organisation. It performs deeper analysis (internally), *plus* includes everything in the External Assessment. This requires an agent to be installed on the computer(s).



SMBsecure™

Cybersecurity Awareness Training

87% of cyber-attacks rely on social engineering and poor security hygiene to deceive users. Your User Could Be Next!

Overview of Service

Employees who lack proper cybersecurity awareness place the entire business at risk, regardless of the tools used.

SMBsecure™ includes a cybersecurity awareness program designed to improve employees' knowledge and skills to help them identify malicious activities and to exercise caution - *to help safeguard your business or practice.* Awareness training builds the **Human Firewall** as a vital defence. This improves the overall security posture of your business for mitigating cyber-attacks. It embeds security practices into your company's DNA, ensuring every employee becomes a **Vigilant Cyber Defender.**

HOW IT WORKS

SMBsecure™ cybersecurity awareness training offers easy e-learning with in-line knowledge assessments structured to fortify your frontline of defence. Training is automatically assigned, and employees are notified to complete modules to maintain a strong defence.

Topics include risk related to scams, phishing red-flags, vishing, passwords, business email compromise, identity theft, ransomware, etc.

ROI You Can See! Employees who are risk aware and vigilant help mitigate your business being scammed or attacked.

COST EFFECTIVE EDUCATION

SMBsecure™ Standard and Advanced subscriptions include a cybersecurity awareness program at Zero Extra Cost! The training is ongoing and fully managed for you, saving you money, time and resources. Training categories and topics are dynamically assigned. Our modules strategically reinforce key insights by resurfacing information to cultivate lasting learning habits.

NO MORE BORING TRAINING VIDEOS

That's right! Say goodbye to tedious - *long and boring* - training videos. **SMBsecure™** re-imagined training with a fresh approach and a captivating learning experience that actually helps your business put up its human shields against cybercrime. **Bite-sized, Science Backed Learning** empowers your team to effortlessly spot and defend against cyber threats. Quick, interactive and *on-the-go* sessions allow users to learn at their convenience. Progress isn't just tracked; it's celebrated through **Gamification.**
Phishing simulations and baiting are also conducted to test an employee's vigilance and vulnerability, and their need for additional training.

SPACED REPITITION LEARNING

Safer teams start with smarter learning that sticks. Spaced repetition is a **powerful learning strategy** designed to change behaviour. **SMBsecure™** factors in natural memory decay to predict when information is at risk of being forgotten. **AI** monitors the user's memory stability and retrieval ability. This *"memory strength"* is reflected in a **Defence Meter** which knows when the employee may need a *Defence Boost* to stay sharp. This ensures your business's **Human Firewall** is prepared to spot phishing attempts, suspicious links, or other threats, so your team won't just learn cybersecurity best practices - *they'll remember them when it counts.*

KPI, COMPLIANCE & MANAGEMENT REPORTS

Business owners or service admins can access reports. Link these to employees' KPIs and targets for effective training adoption, or to leverage as proof for cyber insurance, security framework certifications and compliance.

USER MANAGED PERSONAL DATA EXPOSURE

SMBsecure™ monitors **Dark Web** underground marketplaces, forums, and illicit websites **24/7** *round the clock.* It also assesses **Data Breaches** for users' personal data that has been exposed. Meaningful insights and simple explanations are displayed directly to users ***plus*** provides best steps to take to keep their digital identity safe and secure. This helps to mitigate the risk of further data leaks and to protect accounts from potential compromise.

OUTLOOK SEND CONFIRMATION

SMBsecure™

SendGuard Lite 365

Employees can easily email sensitive info to wrong people by mistake - *especially with Outlook auto-complete.*

Stop Unintended Data Exposure

Overview of Service

SMBsecure™Advanced subscription includes SendGuard Lite 365, an add-in for Microsoft Outlook on Windows PC, Mac, or Web. It provides a confirmation prompt for users to verify recipients and check files attached when sending. This simple but effective prompt aims to catch mistakes typically made by users to avoid sending sensitive information to the wrong people, which can result in unintended exposure or, worse, cause a reportable data breach incident and non-compliance.

Safeguard against misdirected email and protect your business with SMBsecure™ SendGuard Lite 365.

HOW IT WORKS

This **SMBsecure™** add-in for Outlook on PC, Mac or Web enhances safety for your outbound emails which may contain sensitive or confidential information. It provides a neat and simple confirmation prompt for users to check and re-confirm recipients and attachments when sending - *before it is sent.*

Mistakes can happen - especially with Outlook auto-complete and fast-thinking.

Avoid embarrassment and data breach incidents because of misdirected emails.

AVOID SENDING TO WRONG RECIPIENTS

SMBsecure™ Advanced subscriptions include SendGuard Lite 365. This add-on for Microsoft Outlook addresses an important risk faced by many business users, where emails with sensitive information are unintentionally sent to the wrong recipients, causing embarrassment or a data breach for your business. SendGuard helps your business comply with data protection laws such as POPI, GDPR, and other regulations. Stop this type of data breach before it occurs.

> The UK ICO reported in 2022, that a massive 16.87% of data breached were due to data being emailed to the incorrect recipient.

EMAIL BACK-OUT WHEN USERS NEED IT

83% of users realise they've made a mistake just seconds after hitting Send. With SendGuard Lite 365 deployed, users will be empowered to stop an email - *immediately after hitting Send*. This allows them to go-back to make any changes, or corrections, and re-send their email.
The SendGuard automation prompt enforces a science-backed need for users to **Stop-Think-Check**, *especially when they are fast thinking.*

AVOID EMAIL RECALL - It's Unreliable

Catch mistakes and Stop the email before it's sent with SendGuard Lite 365 to avoid the need for recalling emails in the first place. Current email recall methods are unreliable and mostly do not work once the email hits receiving servers, so the best defense is to still to avoid the need to do it - and SendGuard's prompt makes this possible.

CENTRALLY MANAGED AND EASY TO DEPLOY

SMBsecure™ Administrators can centrally deploy SendGuard from the Microsoft Admin centre or they can install it on-demand from Outlook. Settings, users and license-recycling are all centrally done for you from our simple SendGuard management console.

BCC REPLYGUARD

SMBsecure™ includes BCC ReplyGuard which is designed to prevent accidental "Reply All" scenarios. It protects against the inadvertent disclosure of confidential information or embarrassment caused when the user is BCC'd. If the user is BCC'd on an email and the attempt to reply-to-all, SendGuard acts as a safety-net for them in Outlook.

SMBsecure™

Plugin for Microsoft Outlook

SECUREPDF EMAIL ENCRYPTION | BCC RELYGUARD | CHECK4PHISH™

Overview of Service

Prevent the unauthorised exposure of personal/sensitive data when e-mailing.

The **SMBsecure**™ plugin for classic Outlook desktop client allows for easy encryption of emails, attachments, and invites. Secure data from Sender-to-Recipient with no files ever stored in any 3rd-party clouds. All data is always on-device. There are no requirements to make any changes to your email environment or MX records. Just Install and Go with Simple Mode or Customize it for your individual requirements! It works for any email address (mailbox) inside Microsoft Outlook on Windows PC - even Gmail!

HOW IT WORKS

SMBsecure™ Plugin for Microsoft Outlook tightly integrates with the classic Outlook email client on Windows PC, providing effortless and hassle-free end-to-end encryption of correspondence using the renowned **PDF** standard which means there's no keys, certificates or special decryption software needed by the recipient(s) - just a password and a PDF reader.

There's no need to generate encrypted PDFs separately - this plugin does it all for you inside Outlook - SIMPLE!

Securing personal data from unauthorised exposure is a critical business & compliance requirement!

TURNKEY WITH SIMPLE MODE

>A simple out-of-box experience for the recipients!

Quick implementation and ready-to-go adoption guarantee an instant ROI for your business!

Simple Mode aligns to what recipients are already familiar with when receiving encrypted correspondence from their Banks which includes a password-hint to open the Secure PDF, (e.g. use ID Number).

SEND SECURELY

Total flexibility & encryption options are offered with **SMBsecure**™.
All password encrypted Secure PDF file(s) are created using AES 256-bit encryption prior to sending, ensuring ultra-strong security to satisfy even the strictest auditor or regulator. For extra privacy, the plugin can also automatically obscure the subject line if required.

EARN TRUST

Data Subjects want their Personal Information (PI) and sensitive data to be secured and protected, including when it is emailed. Take effective steps to safeguard recipient PI with **SMBsecure**™. Using this plugin to send correspondence as encrypted Secure **PDF** by email will make your business look professional. This demonstrates that you are serious about information security and handling sensitive data, to customers, stakeholders, auditors and regulators.

REMAIN COMPLIANT

The POPI Act (**POPIA**), other statutes, or supply chain safety require your business to provide adequate safeguards for all personal and/or sensitive data, including when it is emailed. This plugin makes it a total breeze for your business to safeguard personal data when e-mailing it. An unencrypted original copy for audit and forensics is also automatically maintained inside Outlook for all encrypted email sent.

FREE SECURE PDF PASSWORD DELIVERY BY SMS

SMBsecure™ solves big challenges when using Secure **PDF** (i.e. communicating the password to unlock a Secure PDF & managing all the passwords). This plugin natively caters for embedded hint as well as automatic transmission of the Secure PDF password to the recipient(s), via email or by SMS at no extra costs - the choice is yours! ! i.e., password retrieval is made easy with ID tagging. Manage and maintain recipient passwords and preferences - *all neatly done inside Outlook!*

DMARC | SPF | DKIM | BIMI | TLS

SMBsecure™

Managed DMARC & TLS

Cyber criminals can hijack and impersonate email domains to trick and defraud users, suppliers and customers.

Your Business's Email Could Be Next!

Overview of Service

SMBsecure™Email Security Compliance is an easy to add-on vital email security service that protects your business's email domain(s) and safeguards against cyber threats such as phishing and Business Email Compromise (BEC) through impersonation attacks. This service enhances safety and credibility with users, clients and suppliers. It increases trusted delivery for your business emails, controls email sending sources, monitors for blacklisting and fortifies email security for your business email domain(s).

Protect Business Email & Improve Business Email Deliverability with SMBsecure™.

HOW IT WORKS

This **SMBsecure**™ service add-on enhances safety for your Email domain(s) and DNS records. Fundamental security risks that could harm business integrity are assessed, remediated and fully monitored for you. **Can you read XML reports?** You don't have to! This service includes ongoing monitoring and tuning for the optimised use of email authentication & security protocols.

It's more than just record changes!
> It's a monthly managed service to do it right and ensure compliance & keep your business email domain(s) secure!

ESSENTIAL EMAIL SECURITY FOR YOUR BUSINESS

SMBsecure™ Email Security Compliance addresses vulnerabilities in your domain and business email security. It focuses on critical email authentication standards (protocols) for protecting the outbound email channel to defend against threats such as mailbox spoofing, phishing, C-Level fraud, and business email compromise (BEC).

ELEVATE YOUR EMAIL SECURITY STANDARDS

DMARC, DKIM, SPF, and **BIMI** are powerful email authentication protocols that collectively establish sender legitimacy, prevent email impersonation, and safeguard the integrity of outbound email communications. With these protocols in place, you can ensure the authenticity and integrity of the emails sent by your business, bolstering your business' trustworthiness in the digital realm. **MTA-STS** on the other hand will ensure encryption of the email channel with **TLS** to provide secure inbound email communications.

MITIGATE RISKS AND IMPROVE REPUTATION

By implementing strong email authentication measures, your business can mitigate the risks associated with cyberattacks, phishing attempts, and fraudulent emails using your email domain. Maintaining a secure email ecosystem enhances your online reputation and delivery trust among your customers, suppliers, and stakeholders. The service includes ongoing monitoring for unknown email sources, email quarantine and rejections, and blacklisting of your domain(s).

DMARC AND TLS'S CRUCIAL ROLE

DMARC unifies SPF and DKIM protocols to prevent email phishing attempts that exploit domain spoofing. **TLS** mitigates Man-In-The-Middle (MITM) attacks by ensuring encryption of inbound emails. Despite its efficacy and relatively low cost, DMARC and TLS adoption remains low due to its complexity and misconfiguration. Attackers and scammers take advantage of this fact! **SMBsecure**™ helps bridge this gap with this service by simplifying the implementation, ongoing monitoring, auditing and optimisation of DMARC and MTA-STS (TLS).

EASY IMPLEMENTATION

SMBsecure™ streamlines the implementation process of SPF, DKIM, DMARC, and MTA-STS (TLS) records. With direct assistance and guidance, we effortlessly enhance your email security posture. **SMBsecure**™ reduces the risk of phishing, BEC and improves deliverability of business emails.

SMBsecure™

POPI & Governance Toolkit

Dashboard | Manual | Training | Checklists | Templates

Overview of Service

The SA POPI Act (POPIA) regulates the processing of personal information (PI) and makes any entity processing PI *liable* for the protection & security of that personal data.

The **SMBsecure™ POPI Toolkit** is an easy to add-on resource kit in association with **POPI Comply** to provide you with affordable and practical do-it-yourself (**DIY**) POPI compliance.

This Toolkit provides an easy workflow of practical actions to help your small business comply with the lawful processing of personal information. The steps are complemented with self-assessments, training modules, checklists, templates, POPI document registers & AI Bot.

HOW IT WORKS

SMBsecure™ POPI Toolkit offers a step-by-step guide tailored for SMEs to navigate the complex landscape of POPI compliance and simplifies the process, making compliance feasible.

The Toolkit offers a centralised portal to self-assess processing activities, measure compliance levels and to get answers for specific questions and scenarios from *Compliance Kate* – our AI-powered Bot. This reduces the need for extensive research and associated cost.

Compliance with the POPI Act is mandatory for any entity processing Personal Information.

COST EFFECTIVE COMPLIANCE

SMBsecure™ POPI Toolkit addresses non-compliance with this cost-effective Do-It-Yourself resource kit for SMBs and small practices. This add-on Toolkit reduces the need for expensive consultations and engagements by consolidating, simplifying and streamlining the process and essential tasks for POPI compliance. A 30-step guided program makes keys actions pragmatic and relevant material accessible for cost-effective compliance with POPI.

RISK & VENDOR ASSESSMENT

The **SMBsecure™** POPI Toolkit provides you with the necessary tools to assess your data processing activities and to identify potential compliance risks. This helps you to prioritise actions and allocate resources effectively. It includes tools and questionnaires to help you assess the compliance of your third-party vendors and data processors (Operators), ensuring that they also align and comply with POPI requirements.

CHECKLISTS AND COMPLIANCE KATE

Included checklists ensure that you don't miss critical compliance requirements, helping your business stay on track throughout your compliance journey. ***Compliance Kate*** is your AI assistant to guide you with questions and scenarios pertaining to **POPIA, PAIA,** and **Data Protection.**

CUSTOMIZABLE TEMPLATES

The Toolkit provides a library of customisable templates, including privacy policies, consent forms, data processing agreements, and more. This Toolkit can save you time and resources by adapting these templates to your own specific needs, yielding a swift **ROI.**

EDUCATION AND TRAINING

A key aspect of POPI compliance is ensuring sufficient education and knowledge about POPI Act obligations, requirements and general employee awareness and personal data handling.

The Toolkit includes a repository of training modules and supplementary documentation for POPIA and PAIA (Promotion of Access to Information Act) to reduce your training costs.

Employee education modules help to expand awareness to inculcate a strong culture and deeper respect for the privacy and security of Personal Information, both internally and externally.

SMBsecure™ Cyber Warranty

Cyber events can be costly for your business, damaging to your bottom-line, and remediations require specialist expertise.

Financial Protection for Data Breach | Cyber Extortion | BEC

Overview of Service

SMBsecure™ Cyber Warranty is an easy to add-on component for risk management that protects your business's bottom-line and safeguards against remediation costs following key cybersecurity incidents by reimbursing expenses like investigations, PR fees, and potential ransom payments, etc.

This warranty offers crucial financial and operational support for three costly cyber events, including data breaches, cyber extortion, and business email compromise (**BEC**).

HOW IT WORKS

SMBsecure™ Cyber Warranty provides crucial financial and operational benefits for costs relating to stated cyber events. including data breaches, cyber extortion, and business email compromise (BEC) incidents. The Cyber Warranty can be added at any time to an Advanced Subscription, based on your company revenue tier and it meeting some *basic requirements*.

It's more than financial protection, it's also access to specialist expertise to assist with incident response, PR, regulatory triage, and remediations following a cyberattack.

Basic Requirements:

1. Company domiciled in South Africa Only.
2. The organization is not a restricted industry.
3. SMBsecure Cyber Warranty is activated and paid.
4. Have SMBsecure Advanced Plan fully implemented at the time of a Warranty Event.
5. Have minimum stated cyber controls in-place (active) at the time of a Warranty Event

ESSENTIAL FINANCIAL PROTECTION

The **SMBsecure™** Cyber Warranty reimburses expenses related to a cyber event, including:

- Investigation and remediation costs.
- Ransom payments to prevent damage.
- Data breach notification costs.
- Credit or identity monitoring for affected customers.
- Public relations expenses to manage incident fallout.
- Access to a panel of specialist expertise.
- Direct financial loss due to business email compromise.

SCOPE & BENEFITS

A **Data Breach** is an incident where sensitive, protected, or confidential data is accessed, disclosed, or stolen by unauthorised parties. The **SMBsecure™** Cyber Warranty includes Cash and Remediation for data breach limited to the maximum sum of ***R1,000,000.***

Cyber extortion is a form of cybercrime in which attackers gain unauthorised access to a victim's systems, data, or network and threaten to release, damage, or disrupt unless a ransom is paid. The **SMBsecure™** Cyber Warranty includes Cash and Remediation for cyber extortion limited to the maximum sum of ***R500,000.***

Business Email Compromise (BEC) is the unrecoverable actual direct financial loss of money as confirmed by the relevant financial institution, which belong to the business or for which the business is legally responsible, as a direct result of a Network Security Breach by a third party. The **SMBsecure™** Cyber Warranty includes Cash Payout limited to the maximum sum of ***R250,000.***

The SMBsecure™ Cyber Warranty is standardized product add-on which is not cyber insurance and is separate and independent of any cyber insurance procured.

EXPERT ASSISTANCE

The **SMBsecure™** Cyber Warranty not only provides financial support, it also provides access to professional services, PR, and cybersecurity experts who can assist with incident response and remediation following a Warranty Event. These specialist skills and services might be outside the capabilities of our or your organisation. The expertise provided can help your business avoid legal fines and penalties associated with data breaches, and non-compliance with regulations, and reputational (brand) damage.

PEACE OF MIND

Knowing that you have financial protection against the potentially devastating costs of a cyberattack. The **SMBsecure™** Cyber Warranty can provide some peace of mind and allow you to focus on your core business.

SMBsecure™
For Windows Server MFA

ENFORCED TWO-FACTOR AUTHENTICATION FOR ANY:

DOMAIN | LOCAL | THIRD-PARTY ACCOUNT ON WINDOWS SERVER

Overview of Service

Windows Servers are highly vulnerable to Brute Force, RDP and Account attack.

SMBsecure™ for Windows Server simplifies multi-factor authentication (**MFA**) implementation on Windows Servers. It provides easy setup, strong login verification through 2FA codes, and support for local, remote, online, and offline logins. The solution improves Server security and compliance with reporting and auditing capabilities.

HOW IT WORKS

SMBsecure™ for Server enforces multi-factor authentication (**MFA**) to add a critical layer of protection to Windows Server security beyond passwords. It requires both credentials and a time-sensitive code from an authenticator app for authorised users to access the server.

Hardening Access to Servers is now a Critical Control!

SIMPLE SETUP

The solution is designed to be easy to set up and use, simplifying the process of implementing 2FA for Windows Server logons.

ZERO-TRUST USER VERIFICATION

MFA adds an additional layer of security to the login process by requiring users to provide a second form of authentication, typically a code generated by an authenticator app, in addition to their password alone.

MFA & PASSWORD POLICY FOR NON-DOMAIN SERVERS

Maybe you are already using MFA for domain-accounts synced to M365, but what about all those local accounts **NOT synced with M365?!** This yields very high risks for exploit and server compromise. **SMBsecure™** can selectively implement MFA for all or local accounts only. It can also enforce a password policy to reform authentication posture on non-domain servers, including password length, strength, complexity and account lock-out.

SECURE LOCAL AND REMOTE LOGONS

The MFA implementation works for both local and remote logons, ensuring that users go through the MFA process regardless of their location.

OFFLINE AND ONLINE ACCESS

The MFA codes can be used for both online and offline logins, providing flexibility and security even when the server is not connected to the internet. Administrators can also use an offline Recovery Code, if needed!

SUPPORT FOR AUTHENTICATOR APPS

The solution supports multiple authenticator apps, such as Google Authenticator and Microsoft Authenticator, allowing users to choose their preferred app for generating 2FA codes. No MFA fatigue here!

CENTRALLY AUDIT, REVIEW & REPORT MFA

Easily assess (in real-time) the use & status of **SMBsecure™** MFA across ALL User Accounts on computers (including blind spot local accounts) to report and prove **SMBsecure™** managed 2FA is used as a vital authentication control for Governance, Risk & Compliance (**GRC**).

SMBsecure™

SA Cyber Joint Standard Compliance

SMBsecure™ provides a comprehensive suite of tools and services that addresses key requirements of the FSCA Cyber Joint Standards.

Overview of Service

SMBsecure™ is tailored to help your small business stay secure and earn trust while remaining compliant.

SMBsecure™is an inexpensive all-in-one fully managed service to de-risk your business with device & email attachment encryption, device lock & kill, phishing defence, cyber risk awareness education, reporting, proof of data encryption, layered access controls, MFA and cybersecurity risk discovery. Easily add-on Financial Protection for Data Breach, Cyber Extortion and Business Email Compromise with the bespoke SMBsecure Cyber Warranty.

HOW IT WORKS

SMBsecure™ leverages patented technologies from leading and world class technology vendors that can be deployed in minutes to make securing your data on PCs, Macs, USBs, Mobiles and Emails a Total Breeze. Addons provide additional GRC for FSPs.

IT GOVERNANCE AND RISK MANAGEMENT

- **Risk Discovery:** The managed Cybersecurity Risk Discovery service focus on assessing and identifying risks and provides insightful attack surface management which directly addresses FSCA requirements for risk assessment and management.
- **Reporting:** Reporting capabilities provide audit trails and documentation necessary for demonstrating compliance to the FSCA.
- **Cyber Warranty:** This add-on provides financial protection against key cyber events, which is an element of risk management.

PROTECTION OF SENSITIVE INFORMATION

- **Device Encryption:** This feature directly addresses the FSCA's mandate to protect sensitive data on devices, especially in cases of loss or theft.
- **PDF Email Encryption:** Protects sensitive information sent via email correspondence (*attachments*), fulfilling data protection requirements.
- **Misdirected email governance:** This feature prevents sensitive information being sent to the wrong recipients.

CYBERSECURITY AND CYBER RESILIENCE

- **Multi-Factor Authentication (MFA):** Essential for securing access to systems and preventing unauthorized access, a key component of *cybersecurity*.
- **Cyber Awareness Training and Phishing Simulations:** Enhances employee awareness of cyber threats, reducing the risk of successful phishing attacks and social engineering to build up the **Human Firewall**.
- **Access Control:** Provides tools to manage and restrict access to sensitive data and systems, mitigating risks of unauthorized access.
- **Managed DMARC & TLS:** This add-on assists in securing email communications, reducing the risk of email spoofing, phishing & BEC.

COMPLIANCE WITH POPIA & JS

- **POPI & Cyber Joint Standards Toolkits:** These add-ons directly help with compliance to the POPI Act and Cyber Joint Standard regulations - a requirement for all FSPs - and mandated by the FSCA.
- **Proof of Data Encryption:** Provides the necessary documentation to demonstrate compliance with FSCA data protection requirements.

OVERALL VALUE FOR FINANCIAL SERVICE PROVIDERS

SMBsecure™ simplifies and enhances cybersecurity for small and mid-sized FSPs, helping to meet several key requirements of the FSCA Joint Standards. It inexpensively offers broad coverage for compliance that includes data protection, risk management, and employee training. This leads to lower risk, improved compliance, and increased business resilience and trust.

SMBsecure™

For SA Medical Practices

Patient Confidentiality | Data Security | Compliance

Overview of Service

Medical Practices are targets for cyber criminals to obtain personal information. Exposed personal information places patients at risk of financial losses stemming from identity theft, scams, and fraud.

SMBsecure™ is a neat and affordable solution bundle for data protection stipulated by HPCSA, Medical Aids and the POPI Act,

This solution employs necessary security measures and controls to mitigate risks of unauthorised data access and exposure. It is tailored to help medical practices and healthcare practitioners stay secure and earn trust while remaining compliant.

HOW IT WORKS

SMBsecure™ is an All-in-One service to de-risk your medical practice with Data-on-Device Encryption, Device Access Controls, Secure PDF Email Encryption, Device Lock/Kill, Cyber Risk Awareness Education, Reporting and Proof of Data Encryption.

Beyond your consent form, the SMBsecure™ POPI Toolkit is an add-on DIY resource kit to help you comply with the POPI Act.

Securing personal data from unauthorised exposure is a critical HCP & compliance requirement!

COMPLY WITH SOUTH AFRICAN HPCSA

The Health Professions Council of South Africa (**HPCSA**) prescribes your ethical guidelines and good practice. The right of patients to privacy, security and confidentiality must be protected at all times. Therefore, effective safeguards against unauthorised use and the secure transmission of confidential patient information must be assured. All patient and clinical records stored on computer drives are to be encrypted and access to the device is controlled by a password to prevent unauthorised access to this information (**patient personal data**).

The HPCSA stipulates that any electronic transmissions which include patient personal data (e.g. emails, prescriptions, and laboratory results) must be secured. It is the responsibility of healthcare practitioners to ensure that non-healthcare personnel do not violate patient confidentiality. When it comes to the processing of patient information, the HPCSA states that a healthcare practitioner (**HCP**):

1. **Must** be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by computer, e-mail or other electronic means.
2. **Must** make sure that their own computer terminals or any other communication devices are secure at all times. If they send data by email or any electronic format, they should satisfy themselves, as far as is practicable, that the data cannot be intercepted or seen by anyone other than the intended recipient. Healthcare practitioners should note that information sent through the Internet may be intercepted.
3. **Should** include details of the security measures taken such as data encryption and authentication controls with the informed consent documentation for telemedicine practice.

MEDICAL AIDS AND POPIA REQUIREMENTS for Healthcare

Both the POPI Act (**POPIA**) and Medical Aid administrators demand proper safeguards of patient personal data.

Where an email is being sent with files which contain or include personal information (patient personal data), it must be password encrypted. A practice must ensure that any communication with patient personal information sent to a medical aid administrator is sent securely.

Necessary security measures must be in-place - *with proof* - on your computers and mobile devices to mitigate unauthorised access and data exposure. Ensure that if a device is stolen it can be locked or killed, removing all access to the perpetrator. These protections must also apply to your operators (e.g. debt collectors).

Sources: https://www.hpcsa.co.za/ | https://www.discovery.co.za
https://smbsecure.co.za/popia/