
ITEC
Tiyende
SOPHOS
CYBERSECURITY LANDSCAPE 2023
Pieter Nel –Sophos Regional Head SADEC
Simbo Ntshinka – Managing Director Itec Tiyende
TEAM
purco
PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

TOP 5 VULNARIBILITIES IN CYBERSECURITY

1. Phishing attacks..

- ✓ 2022 alone, phishing attacks accounted for over 80% of reported cybersecurity incidents in the education sector across South Africa

2. Unpatched software

- ✓ Outdated software is a prime target for cybercriminals because it may contain known vulnerabilities.
- ✓ Most institutions are challenged with maintaining up-to-date software upgrades.

3. Weak passwords

- ✓ Weak passwords are a common problem.
- ✓ Passwords that are easily guessable.
- ✓ In a recent survey of South African Education Institutions, it was found that over 50% of staff and students used weak passwords for their accounts.

4. Inside threats

- ✓ Insider threats can come from employees students or anyone with access to your organisation's systems.
- ✓ In a 2022 study 68% of cyber security incidents in South African educational institutions were fount to be the result of inside threats.

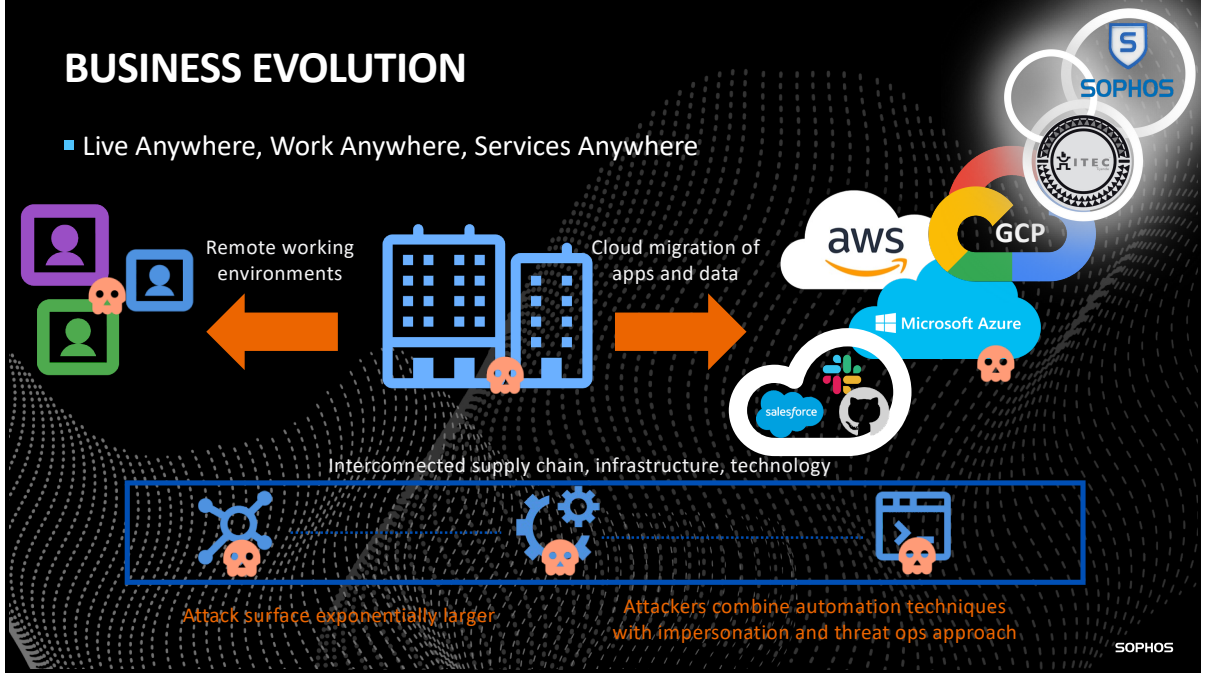
5. Malware infections

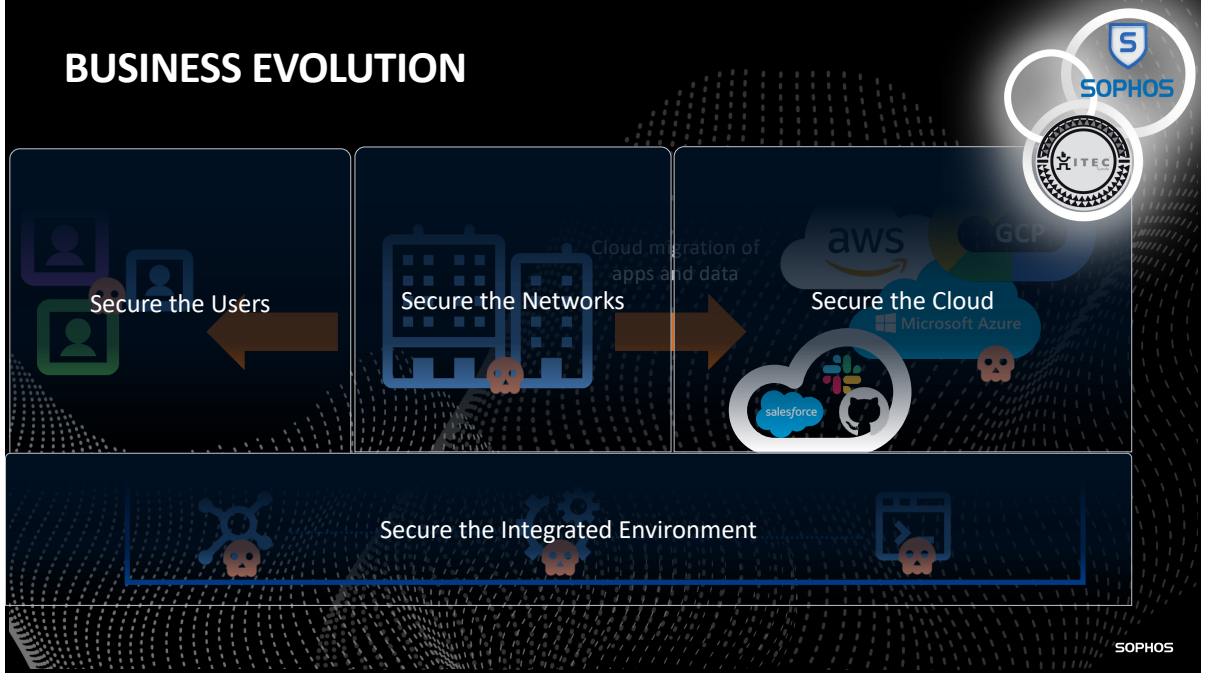
- ✓ Malware remains a persistent threat, and the Education sector is not spared of this threat.
- ✓ Malware infections increased in 2022 by 35% compared to prior years.

SOPHOS

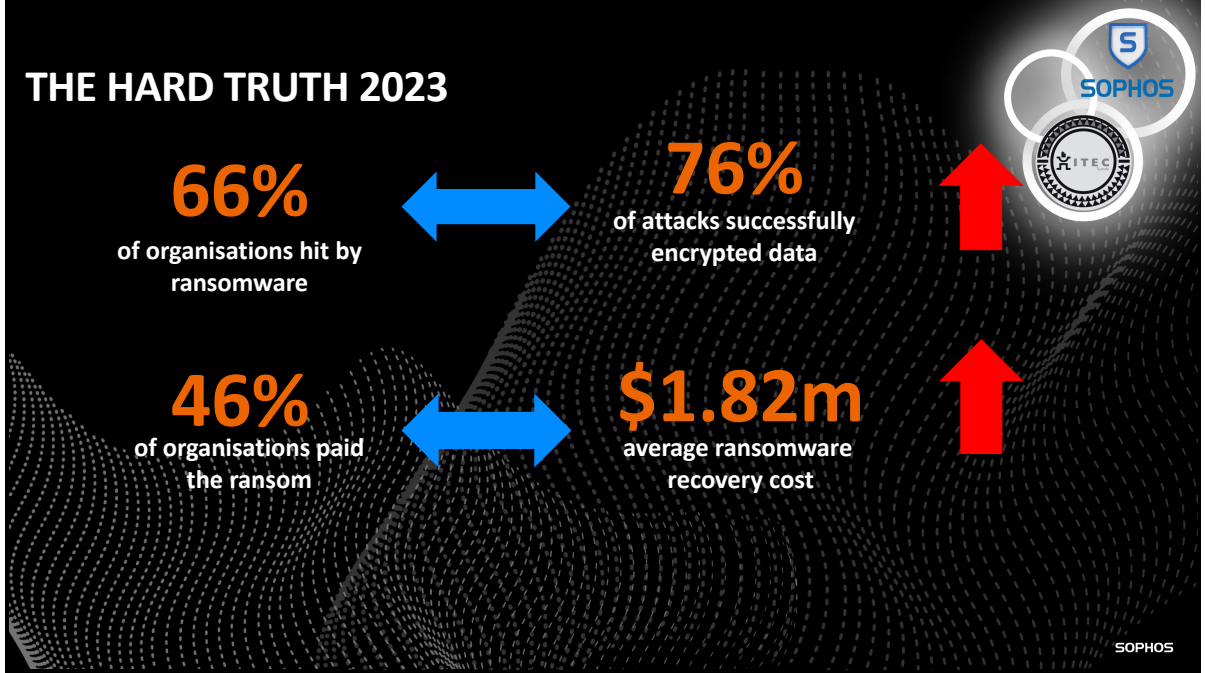
BUSINESS EVOLUTION

- Live Anywhere, Work Anywhere, Services Anywhere

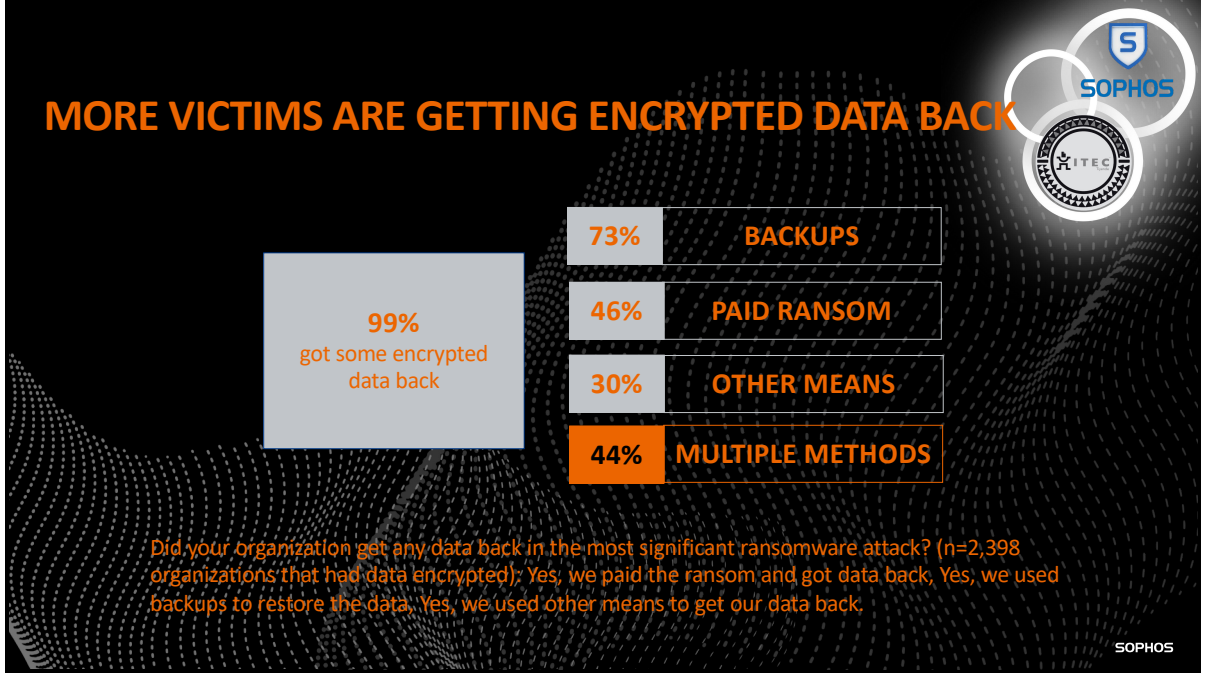



BUSINESS EVOLUTION
SOPHOS
ITEC
Secure the Users
Secure the Networks
Cloud migration of apps and data
aws
GCP
Secure the Cloud
Microsoft Azure
salesforce
Secure the Integrated Environment
SOPHOS


THE REALITY OF RANSOMWARE
SOPHOS
ITEC
SOPHOS


THE HARD TRUTH 2023
66%
of organisations hit by ransomware
76%
of attacks successfully encrypted data
46%
of organisations paid the ransom
$1.82m
average ransomware recovery cost
SOPHOS
SOPHOS

MORE VICTIMS ARE GETTING ENCRYPTED DATA BACK



Did your organization get any data back in the most significant ransomware attack? (n=2,398 organizations that had data encrypted). Yes, we paid the ransom and got data back, Yes, we used backups to restore the data, Yes, we used other means to get our data back.

SOPHOS

THE CYBERSECURITY CHALLENGE

Cybersecurity – is so complex, so difficult, and moves so fast that most organizations simply can't manage it effectively on their own.

Cyberthreats Are Accelerating in Volume and Sophistication

- 57% of organizations report an increase in the number of attacks over the past year[1]
- 78% increase in the number of organizations hit by ransomware last year[1]
- "It's nearly impossible for organizations to outrun threat actors and keep themselves, their customers, and employees safe" – IDG

Cybersecurity Tools Are Overwhelmingly Costly and Complex

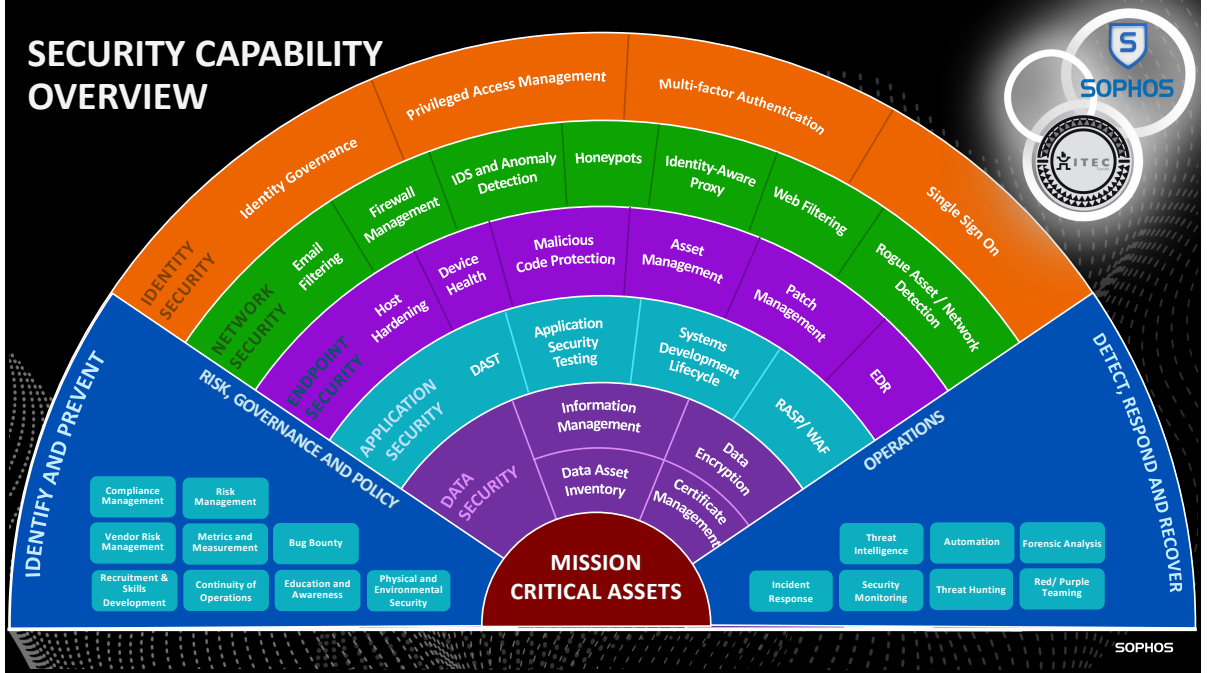
- The average organization has more than **46 cybersecurity monitoring tools** in place
- Most sec ops teams are **drowning in alerts**
- The average organization spends **$7.5K on cybersecurity** per employee[2]

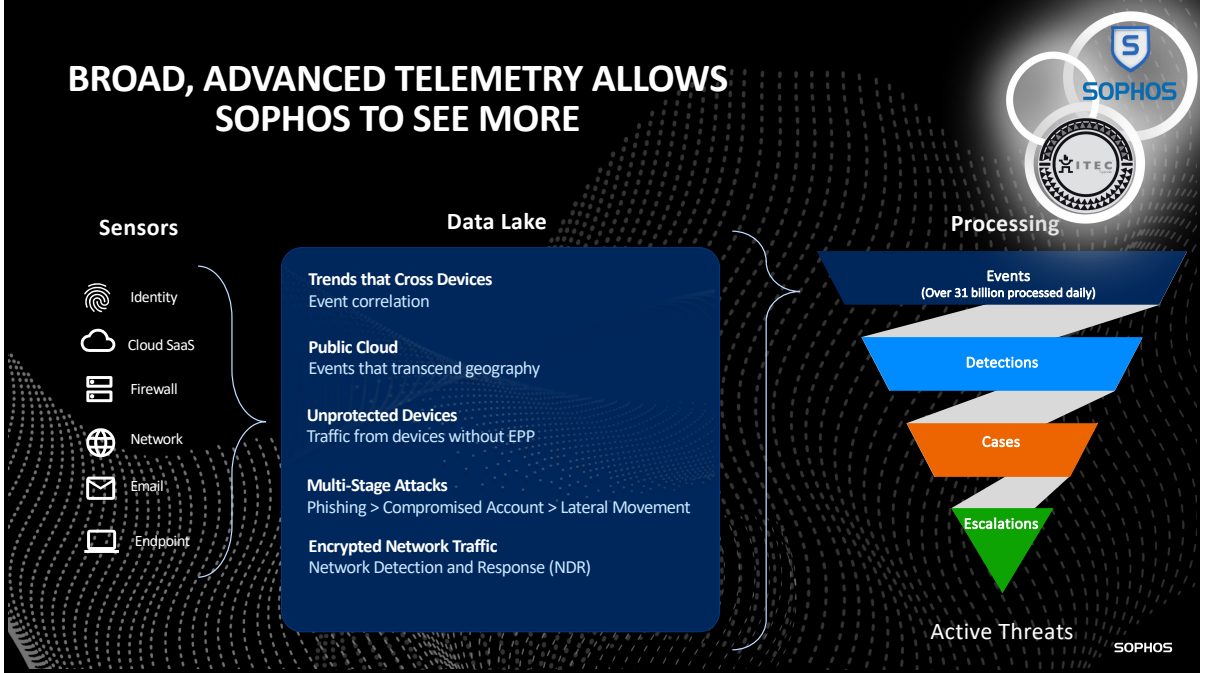
Hiring and Retaining Cybersecurity Experts Has Become Fiercely Competitive

- The number of unfilled cybersecurity jobs worldwide **grew 350%** between 2013 and 2021
- In the US there are 1 million cybersecurity workers and **750,000 cybersecurity openings**
- Security Analysts cost $100-150K per year, and the annual cost to maintain a SOC is $2.86M[3]

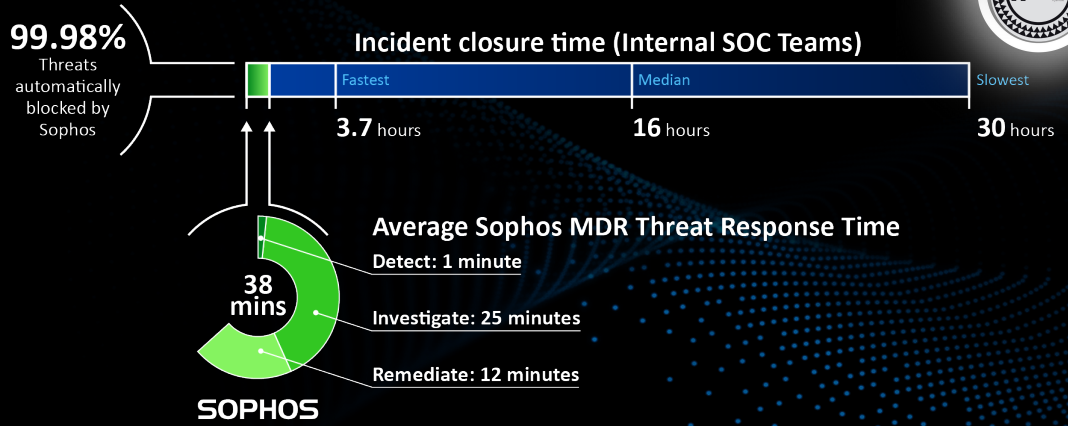
[1] *The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos*
[2] *Statista: https://www.statista.com/outlook/tmo/cybersecurity/worldwide*
[3] *Ponemon Institute: "The Economics of Security Operations Centers: What Is the True Cost for Effective Results?"*

SOPHOS


SECURITY CAPABILITY OVERVIEW
SOPHOS
ITEC
IDENTITY SECURITY
Identity Governance
Privileged Access Management
Multi-factor Authentication
Single Sign On
NETWORK SECURITY
Email Filtering
Firewall Management
IDS and Anomaly Detection
Honeypots
Identity-Aware Proxy
Web Filtering
Rogue Asset / Network Detection
ENDPOINT SECURITY
Host Hardening
Device Health
Malicious Code Protection
Asset Management
Patch Management
EDR
APPLICATION SECURITY
DAST
Application Security Testing
Systems Development Lifecycle
RASP/ WAF
DATA SECURITY
Information Management
Data Asset Inventory
Data Encryption
Certificate Management
MISSION CRITICAL ASSETS
IDENTIFY AND PREVENT
RISK, GOVERNANCE AND POLICY
Compliance Management
Risk Management
Vendor Risk Management
Metrics and Measurement
Bug Bounty
Recruitment & Skills Development
Continuity of Operations
Education and Awareness
Physical and Environmental Security
DETECT, RESPOND AND RECOVER
OPERATIONS
Threat Intelligence
Automation
Forensic Analysis
Incident Response
Security Monitoring
Threat Hunting
Red/ Purple Teaming
SOPHOS


BROAD, ADVANCED TELEMETRY ALLOWS SOPHOS TO SEE MORE
SOPHOS
ITEC
Sensors
Identity
Cloud SaaS
Firewall
Network
Email
Endpoint
Data Lake
Trends that Cross Devices
Event correlation
Public Cloud
Events that transcend geography
Unprotected Devices
Traffic from devices without EPP
Multi-Stage Attacks
Phishing > Compromised Account > Lateral Movement
Encrypted Network Traffic
Network Detection and Response (NDR)
Processing
Events
(Over 31 billion processed daily)
Detections
Cases
Escalations
Active Threats
SOPHOS

LEADING DETECTION AND RESPONSE TIMES



Sophos Breach Protection Warranty

At Sophos, we make your cybersecurity our responsibility. The Sophos Breach Protection Warranty is included at no additional charge with our Sophos MDR Complete subscription. It covers up to $1 million in response expenses for qualifying customers.

Trusted Protection for Complete Peace of Mind

More organizations trust Sophos for MDR than any other security vendor. With the Sophos Breach Protection Warranty, Sophos MDR Complete customers enjoy the reassurance and peace of mind that comes with having financial coverage if a breach happens.

Clear, Comprehensive Coverage

- Automatically provided – no need to apply
- Included with one-, two-, and three-year subscriptions
- Included with new and renewal license purchases
- Covers endpoints, servers, and devices running Windows and macOS
- No warranty tiers that restrict coverage
- No additional license purchase requirements

Included with Sophos MDR Complete

The warranty is included automatically and at no additional charge with new purchases or renewals of Sophos MDR Complete annual subscriptions. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

Up to $1 Million in Response Expenses

The warranty covers response expenses following a ransomware incident within an environment protected by Sophos MDR Complete:

- Up to $1,000 per breached machine
- Up to $1 million in total response expenses
- Up to $100,000 ransom payment (as part of per-device limit)

Reflecting the reality of today's operating environments, breached machines include endpoints, servers, and Windows and macOS devices. The warranty covers a wide range of incurred expenses, including data breach notification, PR, legal, and compliance.

Warranty Overview

- Up to $1 million in total response expenses
- Up to $100,000 for ransom payment (as part of per-device limit)
- Up to $1,000 per breached machine
- Covers a range of incurred expenses, including data breach notification, PR, legal, and compliance

For full terms and conditions of the warranty, visit www.sophos.com/legal

SOPHOS


ITEC
Tiyende
&
SOPHOS
Cybersecurity delivered.
SOPHOS
ITEC


ITEC
Tryende
SOPHOS
Q & A
purco
PURCHASING CONSORTIUM
SOUTHERN AFRICA NPC
ISO 9001:2015 certified company