CRS

CYBER RETALIATOR SOLUTIONS

THE BUG STOPS HERE.

# CYBER RETALIATOR SOLUTIONS

2023

CRS

CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

# ABOUT US

## WHO ARE WE?

Cyber Retaliator Solutions is an Authorised IBM training Center, Redhat Training Partner and Cyber Security Distributor, Operating throughout the Globe.

Our Head Office is based in Centurion South Africa, with IBM Training Centers in Centurion, Midrand, Sandton and Cape Town.

CRS Distributes World Class Cyber Security Solutions to Stay Ahead and Stay Protected.

We have over 20 years of experience in the IBM Training and the Cyber Security space.

## AUTHORISED IBM & REDHAT TRAINING

Through our partnership with Arrow ECS - CRS delivers Authorised IBM training throughout the Globe.

RedHat Learning helps customers stay on top of industry trends by teaching innovative technologies and products to give a competitive edge.

## CYBER SECURITY DISTRIBUTION

We are a future-focused business expanding rapidly throughout Africa with our Cyber Security Solutions.

CRS Distributes World Class Cyber Security Solutions to Stay Ahead and Stay Protected.

## CYBER RISK ESSENTIALS

Cyber Risk Essentials assists in growing Organisational Awareness to Cyber-Attacks through Managed Training and Simulations.

CRS

CYBER RETALIATOR
SOLUTIONS

CYBER RETALIATOR SOLUTIONS

# CYBER SECURITY SOLUTIONS

2023

# CYBER SECURITY RANGE

CRS chooses solutions apt to current times and innovations necessary to cyber security requirements of the future.

TOPIA

Cloud-based platform to assess, prioritize, and remediate vulnerabilities in applications, assets, and operating systems.

SMBsecure™

All-in-One Fully Managed Service to De-risk your Business with Data & Email Encryption, Device Lock/Kill, Phishing Simulations, Cyber Risk Training, Reporting and Proof of Data Encryption.

BEACHHEAD®

Cloud platform to enforce encryption & access control on employee-used devices.

REAQTA
an IBM Company

MDR/EDR solution that consist of a Next Generation endpoint threat detection system Powered by AI.

CRS

Pen testing, Vulnerability and Web app scanning.

CRS
CYBER RETALIATOR SOLUTIONS

Cyber Risk Essentials assists in growing Organisational Awareness to Cyber-attacks through Managed Training and Simulations.

www.CyberRetaliatorSolutions.com

# TOPIA

Cloud-based platform to assess, prioritize, and remediate vulnerabilities in applications, assets, and operating systems.

vicarius

## 0-Day

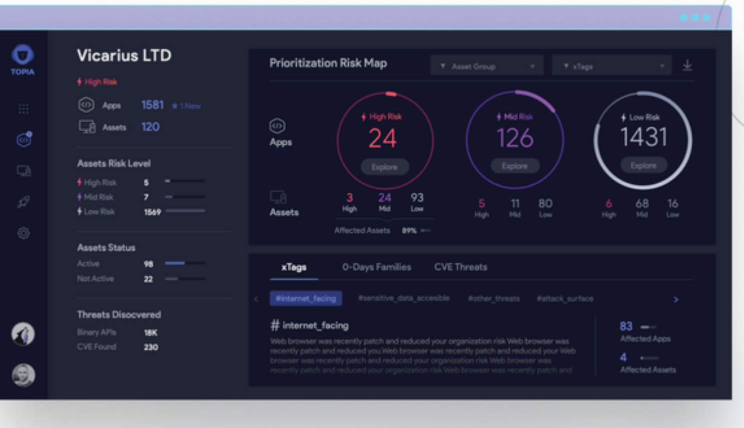
TOPIA's Zero-Day Analysis™ tool uses predictive analysis to track malware activity and predict incoming attacks. Now you can rest easy knowing you'll never get caught off-guard.

## xTags™

xTags™ help prioritize threats using contextual scoring, like prioritization parameters, access authority and activity status in order to determine the risk level of every application and asset in your organization.

## Patchless

Never think twice about deploying a patch again. TOPIA'S proprietary Patchless Protection™ tool secures threats swiftly and safely by deploying a protective force-field around high-risk, vulnerable apps.



Web browser was recently patch and reduced your organization risk Web browser was recently patch and reduced you Web browser was recently patch and reduced your Web browser was recently patch and reduced your organization risk Web browser was recently patch and reduced your organization risk Web browser was recently patch and

01

# Analyze

### Detect CVEs and binary level threats

TOPIA is the first all-in-one vulnerability management solution with the ability to analyze proprietary and niche applications for vulnerabilities without official CVEs, providing you with the full threat landscape you need. Its real-time analysis engine identifies CVE and 0-day threats by continuously analyzing third-party software applications.

### App Auto Recognition

TOPIA's Auto App Recognition tool detects installed apps across organizational assets and creates a software inventory of their most recent versions.

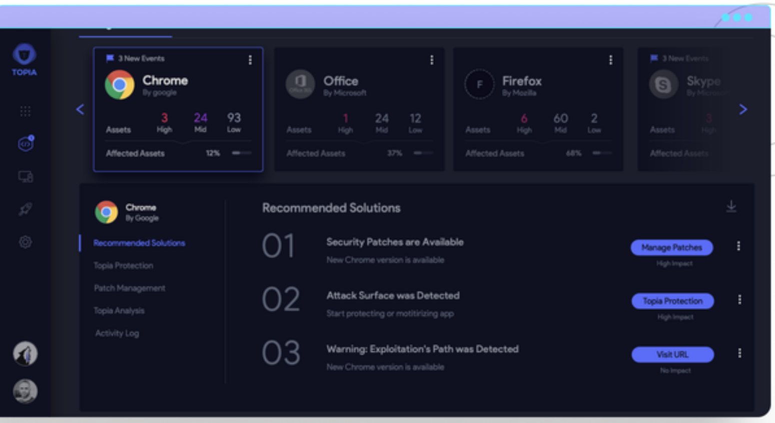
### App Threat Analysis

TOPIA's App Threat Analysis tool runs a binary analysis of all third-party apps to detect common vulnerabilities, including zero-day and CVE threats.

### Asset Threat Analysis

TOPIA's Asset Threat Analysis tool analyzes active and non-active assets within your organization to determine their overall exploitation and risk-level.

# TOPIA



Recommended Solutions

01 Security Patches are Available
New Chrome version is available
Manage Patches
High Impact

02 Attack Surface was Detected
Start protecting or motitirizing app
Topia Protection
High Impact

03 Warning: Exploitation's Path was Detected
New Chrome version is available
Visit URL
No Impact

## Prioritize

### Focus on the threats that matter most

An innovative prioritization engine combines the organizational infrastructure context landscape with thousands of data points and 0-days to accurately pinpoint any outstanding risk.
TOPIA's prioritization combines threats such as well-known vulnerabilities and 0-days with our proprietary xTags™ mechanisms, creating a clear-cut picture of the immediate risk as a result of both threat and exploitation.

### xTags™

TOPIA's xTags™ prioritize all detected threats based on their severity using contextual scoring, identifying the most critical threats your organization faces first.

### App & Asset Risk Scoring

TOPIA ranks the risk and severity of each app and asset in your organization based on their level of threat and exploitation.

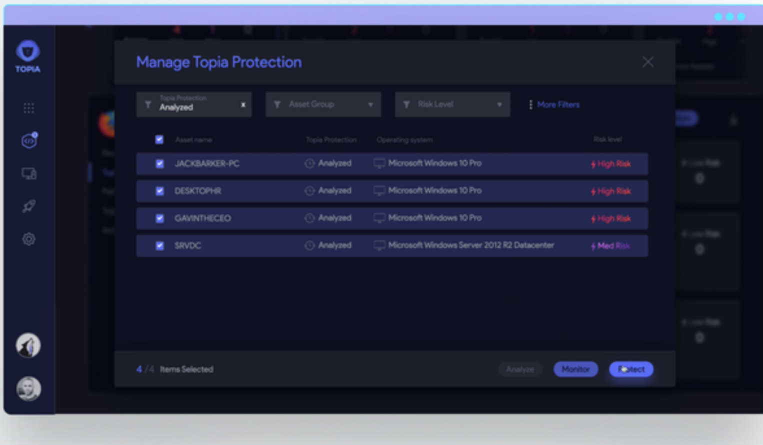
### Prioritization Mapping

TOPIA maps the prioritization of all vulnerabilities found during analysis and identifies the biggest risks facing your organization's security.

## Act

### Protect organizational assets swiftly

For each risk it analyzes, TOPIA provides a list of recommended actions to eliminate it and enable you to stay safe and resilient no matter what risk you are confronting, by patching or otherwise. In cases where there is no patch, or you do not wish to upgrade, TOPIA Patchless Protection™ will protect you without any downtime or reboot.



| ☑ | Asset name | Topia Protection | Operating system | Risk level |
|---|---|---|---|---|
| ☑ | JACKBARKER-PC | Analyzed | Microsoft Windows 10 Pro | High Risk |
| ☑ | DESKTOPHR | Analyzed | Microsoft Windows 10 Pro | High Risk |
| ☑ | GAVINTHECEO | Analyzed | Microsoft Windows 10 Pro | High Risk |
| ☑ | SRVDC | Analyzed | Microsoft Windows Server 2012 R2 Datacenter | Med Risk |

4 / 4 Items Selected

### Recommended Action Engine

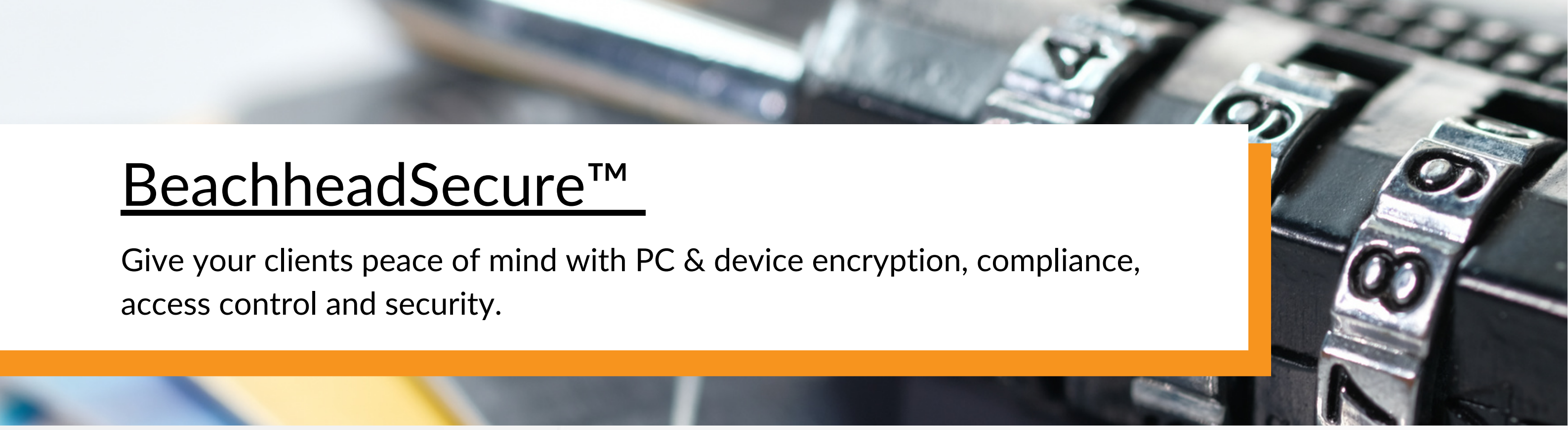
TOPIA's Recommended Action Engine provides real-time suggestions for detected vulnerabilities, allowing you to take quick action and mitigate business risk.

### Real-Time Patch Management

TOPIA's Real-Time Patch Management gives you the power to close patching gaps on a moment's notice with quick and easy patch deployment.

### Patchless Protection™

TOPIA's Patchless Protection™ tool secures high-risk apps rapidly and blocks incoming exploitation attempts using proprietary in-memory protection.



# BeachheadSecure™

Give your clients peace of mind with PC & device encryption, compliance, access control and security.

## Easy, unified, web-managed mobile device security

BeachheadSecure™ Management System is a single, configurable, web-based console with device modules that can be added in any mix or quantity for iPhone & iPads, Android devices, Windows & Mac PCs and USB storage devices. This unique system allows you to remotely secure the vulnerable devices in your organisation – including those owned by employees.

**Who needs this? Your clients do.**

Data security is no longer an optional (or discretionary) MSP service. Ever-increasing (and complex) threats put your client's integrity and business continuity at risk. Businesses can be ruined by a single data exposure, insider threat, breach, or a compliancy violation...and once that happens, it's too late. BeachheadSecure is the proven and trusted platform that ensures your clients' business continuity through robust security enforcement.

BEACHHEAD®

| Benefits of BeachheadSecure | |
|---|---|
| Enforced Encryption | Ensures compliance to legal obligations & stakeholder mandated information security guidelines. |
| Quarantine & Data Lock | Mitigate the risk of data exposure to any unAuthorised user or thief when a device is lost, stolen or impounded or kept or the internet. |
| Remote Wipe | Kill access to sensitive or confidential data when a device is reported stolen or as needed. Mission Impossible, made possible! |
| Device Auditing & Compliance Reporting | Leverage device telemetry for forensic, auditing or reporting purposes for any of your secured devices, be it Windows or Mac PCs & laptops, encrypted USB storage, and Android and iOS phones and tablets. One-button "Compliancy Report" to demonstrate security and compliance for client custodial data. |
| Data Isolation | Securely shield data between users on Windows PCs so when you need to give your PC to the "IT Guy", be assured your data remains inaccessible to them - unless you choose to provide access! |
| Mobile Wi-Fi Provisioning | Automatically and simply set up access to your organizational Wi-Fi connections on phones and tablets without users ever knowing the password. Also remotely decommission Wi-Fi access to prevent employees, volunteers & contractors leaving the organization with continued access to the network without disruption caused to current Wi-Fi users |
| Instant Lock | Immediately eliminate access to phone and tablet devices if lost, stolen or impounded. |

# BeachheadSecure® PCs & MACs

## Advanced Security for Windows & Mac PCs

***Layered encryption, remote & automatic access-control for compliance and true PC data security***

now includes Windows Security Management 10.2023

BeachheadSecure is an advanced web-based platform that makes it simple to enforce and manage encryption and access control on remote Windows & Mac PCs, USB Storage, Phones & Tablets and Windows Servers. BeachheadSecure protects organizations against insider risk, poor user security hygiene, compliancy violations and lost & stolen devices.

All things mobile.
BeachheadSecure
Phones
PCs & Laptops
Servers
Tablets / Pads
Macs
USB Drives

### Encryption is just the beginning: RiskResponder measures & immediately responds to risk events as they happen

Encryption must be easy to manage and enforced under all conditions. You also need to be able to prove encryption is in place in the event that a device is lost, stolen or otherwise compromised.

While encryption should be a cornerstone of your security strategy, it alone cannot protect data in circumstances where user credentials are compromised.

Insider risk, lost credentials, and poor security hygiene all can undermine the best cybersecurity practices. Therefore, it's critical that you control access to sensitive data on PCs and Macs – remotely and instantly.

With the BeachheadSecure administration console, you can do so with a simple button push. Or better yet, let BeachheadSecure's **RiskResponder®** measure risk in real-time and protect data instantly and automatically with pre-determined responses if risk exceeds acceptable thresholds – even when no one's looking.

### RiskResponder: a deeper dive

RiskResponder lets you determine when a PC's environmental or behavioral conditions

constitute a risk, and allows you to pre-determine the appropriate and automatic countermeasure(s) as that risk escalates. Depending on the risk factors, these customized responses can range from simple notifications to your IT team, to a customizable message to the user, to complete and immediate revocation of access to your sensitive data. This risk assessment and deployment of pre-determined countermeasures will happen automatically and immediately, before members or your team (or even a SOC) has any clue there's a problem, 24/7/365. RiskResponder is your eyes and ears into the security conditions of your inventory of PCs and Macs, wherever they may be.

BeacheadSecure currently includes RiskResponder safeguards for addressing the following issues:

- ***Consecutive Invalid Logins:*** May suggest brute force or socially engineered attacks on device credentials
- ***Out of Contact:*** The device is no longer checking in, suggesting hardware is in unAuthorised hands
- ***GeoFence Perimeter Violations:*** The device has moved outside of acceptable preset boarders
- ***Network-Borne Attacks:*** UnAuthorised sites are attempting to access PC data
- ***Security Software Tampering:*** UnAuthorised changes to local security tools (e.g. firewall, AV, encryption)

Beachhead will continue to build RiskResponder safeguards. What other PC environmental or behavioral conditions concern you? We'd love to hear your thoughts.

Currently-available automated responses/countermeasures for meeting any level of risk include: logging the event, sending alert(s) to IT team member(s) or security vendors, running a script, displaying a message to the PC user, shutting the computer down and removing the user's access to data (both at the file level and with lockout from BitLocker). Once a risk is removed, recovery to normal PC operation is achieved with literally a button push on the administration console.

### 2FA (Two-Factor Authentication)

Optionally, BeachheadSecure includes an enforceable 2FA (two-factor authentication) during the Windows boot process. A QR code is generated by the BeachheadSecure agent, which can be scanned by your preferred mobile security authentication application (e.g. Google, Microsoft Authenticator). The application will generate a pin code that is required at the PC boot screen. This second verification provides assurance that only Authorised users will access your PC and its sensitive data!

# BEACHHEADSECURE'S OUTLOOK ENCRYPTION APPLICATION

Software to secure any outgoing emails.
As powerful or simple as you need it!

Add-in for Outlook to allow sending emails (body/attachment/invites) as encrypted, in a way that is easy for the sender and simple for the recipient.

## Secure Outgoing Email Without Hassle

Tightly integrated with the Outlook email client on Windows PC makes for effortless and hassle-free encrypted email sending 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 viewer like Acrobat Reader which is widely used and totally free.

## Password Management

This app caters for automatic transmission of the PDF password to the recipient via Email or SMS - the choice is yours. You can send the actual password or a password-hint instead.

Passwords can be automatically generated for Recipients or it can be manually assigned using custom passwords.

Importantly, this app provides for a personal password list as well as the use of a shared "organization-wide" (admin-controlled) password list.

## Send Securely

Data Subjects want their Personal Information (PI) and sensitive data to be secured and protected, including when it is emailed.

All password encrypted PDF file(s) are created using AES 256-bit encryption prior to sending, ensuring the app employs strong security to satisfy even the strictest auditor or regulation.

## Earn Trust

Do the right thing for your business by taking real and effective) steps to safeguard personal/sensitive information, including when it is emailed.

Using this app to send email as encrypted will make your business look professional to stakeholders and will demonstrate that you are serious about information security and sensitive data handling, even to auditors and regulators.

## Remain Compliant

Laws require your business to provide proper protections and safeguarding of all personal and/or sensitive data, including when it is emailed.

The app boasts some outstanding features and functions making it a total breeze for your business to implement and for employees to use (immediately). This software will yield an instant return-on-investment (ROI) for your business.

## Bank Grade Email Encryption

A simple and intuitive app installed as an add-in for Microsoft Outlook on any Windows PC to send emails as encrypted, in a way that is easy for the sender and simple for the recipient, using the PDF standard.

Encrypt the full message body and attachments, or encrypt attachments-only either in their native format (for editing), or have it automatically converted to PDF.

**De-Risk Your Business**

TRAINING | PHISHING | SMISHING | VISHING

# CYBER RISK ESSENTIALS

## What is Cyber Risk Essentials?

Cyber Risk Essentials is a managed service to assist organisations with cyber awareness in a world of ever evolving threats.

The Service includes Instructor-Led training, Real-world Simulations and supplementary training to grow cyber awareness.

## Why Choose Cyber Risk Essentials?

- Single Managed Platform, managed and hosted by CRS.
- Managed Phishing, Smishing and Vishing Simulations
- Detailed Reporting
- Organisational Risk Analysis
- Virtual / In-Classroom Instructor-led Training
- Gamified Learning Experience
- White-Labelled Content
- Employee Self Development
- Ability to Integrate into an LMS
- Highly Scalable
- Wide Range of Training modules
- Phishing, Smishing and Vishing Simulations

## IMPROVE YOUR ORGANISATIONAL AWARENESS WITHOUT WORRY.

### Training

1

Send your organisation on instructor led cyber awareness training

### Test

2

Deploy a Phishing, Vishing, or Smishing Simulation

### Asess

3

Assess the Organisational risk for phising and cyber awareness

### Train

4

Train them on the EC-Council AWARE LMS to become more Aware

### Test

5

Deploy another phishing simulation to determine effectiveness

POWERED BY CRS AND EC-Council aware When Everyone Protects

TRAINING | PHISHING | SMISHING | VISHING

# CYBER RISK ESSENTIALS

## An Early Warning System Against the Next Phishing Attack

Building organizational memory by building subconscious competency and human firewall to protect your enterprise.

### Outstanding Features

- Real-time phishing simulations
- Security awareness trainings
- Customizable campaigns
- Integratable Learning Management System (LMS)
- Enhanced Reporting
- Unlimited Simulations
- Certificates of completion for courses

### Why Choose Cyber Risk Essentials?

According to online reports, susceptibility to phishing emails drops almost 20% after a company runs just one simulation.

So people do learn, awareness does rise, and risks do reduce with an intelligent solution like Aware.

### A Managed Solution to your Cyber Awareness Requirements

One-Stop Solution to All Possible Security Awareness Training Concerns.

- No instructor's involvement required
- Acquired knowledge assessment and proper reporting
- Get general security awareness topics
- Organisational Risk Assessment

POWERED BY CRS CYBER RETALIATOR SOLUTIONS AND EC-Council aware When Everyone Protects

# SMBsecure™

Patented technology, deployed in minutes, makes securing your organisational data on Windows and Mobiles a total breeze!

## Get Data Security & Compliance as part of your everyday data processing

Uses patented technologies for any standard: POPIA, GDPR, PCI-DSS

ENCRYPT

SAFEGUARD

PROTECT

DEFEND

**All-in-One** Fully Managed Service to De-risk your Business with Data & Email Encryption, Device Lock/Kill, Phishing Simulations, Cyber Risk Training, Reporting and Proof of Data Encryption.

### Data-on-Device Encryption

Make use of encryption methods native to your operating system to ensure the most seamless and most secure means of encryption for your data at rest on your PC & Mobile Device. On Windows PCs, you get persistent Bitlocker for Volume level encryption, as well as fully managed key control, backup & retrieval with real-time encryption risk monitoring for your convenience.

### Outlook Email Encryption

When sending email containing any personal or sensitive data from Microsoft Outlook on your PC, as the Sender you are the ***"Responsible Party"*** so send it using secure end-to-end encryption in password-protected portable document format (PDF), just like the banks do! The Outlook plugin allows flexible options to send data securely to avoid 3rd party data exposure, earn trust from customers & stakeholders by demonstrating effective security, and remain compliant with the Protection of Personal Information Act (**POPIA**), VAT Act, and other requirements which require safe custody of consumer/customer data.

### Device Lock/Kill

- Kill device immediately if stolen,
- Quarantine data access until correct access can be confirmed,
- Fully managed cloud initiated controls.

### Phishing Simulations & Security Awareness Training

- Secure your first line of defence, the **Human Layer**,
- Be prepared by learning to identify phishing scams which mimic real-life attack,
- Automatic training so you don't fall prey to scams designed to steal your (or your customers') information and money,
- Improve your Human Firewall with breach prevention techniques and strategies,
- Fully managed so you don't have to do anything

  ***Become AWARE to Avoid Being a Victim.***

**SMBsecure™ provides value-added Protection for Small and Medium Businesses.**

*Now you can build and maintain trust, compliance, and competitive advantage!*

Distributed by

CRS
CYBER RETALIATOR SOLUTIONS

**Find out more at smbsecure.co.za or email info@CyberRetaliatorSolutions.com**

# IBM Security ReaQta offers a unique, forward-thinking approach to endpoint security.

REAQTA
an IBM Company

The solution uses exceptional levels of intelligent automation, taking advantage of AI and machine learning, to help detect and remediate sophisticated known and unknown threats in near real-time. With deep visibility across endpoints, the solution combines expected features, such as MITRE ATT&CK mapping and attack visualizations, with dual-engine AI and automation to propel endpoint security into a zero trust world.

## Why ReaQta?

1

Continuously learns as AI detects and responds autonomously in near real-time to new and unknown threats

2

Helps secure isolated, air-gapped infrastructures, as well as on-premises and cloud environments

3

Maps threats against the MITRE ATT&CK framework and uses a behavioral tree for easy analysis and visualizations

4

Offers a bidirectional API that integrates with many popular security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools

5

Provides heuristic, signature and behavioral techniques in its multilayered defense

6

Allows users to build custom detection strategies to address compliance or company-specific requirements without the need to reboot the endpoint

7

Simplifies and speeds response through guided or autonomous remediation

8

Offers automated, AI-powered threat detection and threat hunting including telemetry from indicators that can be customized for proprietary detection and granular search

9

Makes remediation available with automated or single-click remote kill

10

Provides deep visibility with NanoOS, a unique hypervisor-based approach that works outside the operating system and is designed to be invisible to attackers and malware

# Unique Features of ReaQta

REAQTA
an IBM Company

ReaQta leverages exceptional levels of intelligent automation and AI to help detect and remediate known and unknown threats in near real time.

### Autonomous AI-powered endpoint detection and response (EDR)

– Uses continuous self-learning AI and machine learning to build an evolving baseline that protects endpoints from threats without requiring daily updates

– Future-proofs your organization with autonomous prevention of ransomware, fileless and in-memory attacks, both online and offline

– Supercharges gaps left by traditional security antivirus (AV) solutions with enhanced detection, visibility and control

### High threat resolution

– Increases your understanding of threats in your environment mapped against tactics and techniques in the MITRE ATT&CK framework

– Helps reduce investigation time from minutes to seconds with threat intelligence and analysis scoring

– Uses prevalence monitoring to remove the guesswork needed to understand the impact and spread of infected artifacts across your organization

### Enterprise automation

– Helps you quickly implement new automations and functionality into your existing workflows using ReaQta API and integrations

– Integrates with SIEM and SOAR tools

### Managed detection and response (MDR)

– Provides 24x7 monitoring, tracking and resolution of critical alerts while keeping you informed

– Helps you identify and track even the most sophisticated actors and run advanced threat hunting campaigns using both AI and our team's deep experience in intelligence

and analysis

– Contains and remediates threats as soon as they're detected, minimizing your business risk and reducing damages and interruption of services

### Complete hunt and response features

– Provides a user-friendly threat hunting platform with preconfigured hunt parameters that don't require database query knowledge

– Offers complete remediation guidance and clickthrough response automation to help you contain any situation within seconds

### Compliance monitoring

– Delivers full visibility into user behavior and application usage to enhance your organization's compliance policies and enforce standards

– Allows users to build custom detection strategies to address compliance or company-specific requirements using DeStra (Detection Strategy) scripting, without the need to reboot the endpoint

– Enables users to activate updates across the organization without endpoint intervention or downtime

### Deployment in any environment

– Provides options for cloud and on-premises infrastructures and works in fully isolated air-gapped environments with no need for daily signature updates

– Installs in seconds without complex integrations, becomes operational within minutes and coexists seamlessly with existing AV software with zero conflicts

– Leaves no impact on the endpoint during deployment, daily operations and even after responding to a live incident

CRS
CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

# Sophos XDR

## Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X is the industry's only XDR solution that synchronizes native endpoint, server, firewall, email, cloud and O365 security. Get a holistic view of your organization's environment with the richest data set and deep analysis for threat detection, investigation and response for both dedicated SOC teams and IT admins.

### Answer IT operations and threat hunting questions

Quickly get answers to business-critical questions. Both IT admins and cybersecurity professionals will see real value added when they are performing day-to-day IT operations and threat hunting tasks.

### Start with the best protection

Intercept X stops breaches before they can start. Which means you get better protection and spend less time investigating incidents that should have been automatically stopped. You also have access to detailed threat intelligence giving you the necessary information to take rapid, informed actions.

### Know where to focus

Hone in on the important issues with a prioritized list of suspicious detections and vulnerable configurations that includes key information for further investigation. Choose from a library of pre-written templates to ask a wide variety of IT ops and threat hunting questions or create your own.

### Minimize investigation and response time

AI-guided investigations enable you to quickly understand the scope and cause of an incident and minimize time to respond. Access devices for real-time state and up to 90 days of historic data or 30 days historic data in the data lake.

### Cross-product visibility

Get maximum visibility of your organization with native integration of Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix and Microsoft Office 365 data.

### Multi-platform, multi-OS support

Inspect your environment whether in the cloud, on-premises or virtual across Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure deployments.

### Highlights

- Answer business critical IT operations and threat hunting questions
- Leverage a prioritized list of detections and AI-guided investigations
- Remotely take remedial actions on devices of interest
- Get a holistic view of your organizations' IT environment and drill into granular detail when needed
- Native endpoint, server, firewall, email, cloud, mobile and O36 integrations
- Access a library of pre-written, customizable template use cases

## Use cases

### IT Operations

- Why is a machine running slowly?
- Which devices have known
- vulnerabilities, unknown services or
- unauthorized browser extensions?
- Are there programs running
- that should be removed?
- Identify unmanaged, guest and IoT devices
- Why is the office network connection
- slow? Which application is causing it?
- Look back 30 days for unusual activity
- on a missing or destroyed device
- Locate mobile devices that are unpatched or have out of date software

### Threat hunting

- What processes are trying to make a network
- connection on non-standard ports?
- Show processes that have recently
- modified files or registry keys
- List detected IoCs mapped to the
- MITRE ATT&CK framework
- Extend investigations to 30 days without
- bringing a device back online
- Use ATP and IPS detections from the
- firewall to investigate suspect hosts
- Compare email header information,
- SHAs and other IoCs to identify
- traffic to a malicious domain
- Identify users with multiple failed
- authentication attempts

## What's included?

| | Extended Detection and Response (XDR) |
|---|---|
| Cross-product data sources | ✓ |
| Cross-product detection, investigation & response | ✓ |
| Prioritized detections list & AI-guided investigations | ✓ |
| Sophos Data Lake | ✓ |
| Data lake retention period30 days | |
| Real-time state information | ✓ |
| On-disk data retention periodUp to 90 days | |
| Threat hunting & IT ops template library | ✓ |
| Intercept X protection capabilities | ✓ |

For further details on licensing please see the Intercept X and Intercept X for Server license guides.

# Intercept X

Intercept X Advanced, Intercept X Advanced with XDR,
Intercept X Advanced with MTR

Sophos Intercept X is the industry leading Endpoint Security solution that reduces the attack surface and prevents attacks from running. Combining anti-exploit, anti-ransomware, deep learning AI and control technology it stops attacks before they impact your systems. Intercept X uses a comprehensive, defense in depth approach to endpoint protection, rather than relying on one primary security technique.

## Stop Unknown Threats

Deep learning AI in Intercept X excels at detecting and blocking malware even when it hasn't been seen before. It does this by scrutinizing file attributes from hundreds of millions of samples to identify threats without the need for a signature.

## Block Ransomware

Intercept X includes advanced anti-ransomware capabilities that detect and block the malicious encryption processes used in ransomware attacks. Files that have been encrypted will be rolled back to a safe state, minimizing any impact to business productivity.

## Prevent Exploits

Anti-exploit technology stops the exploit techniques that attackers rely on to compromise devices, steal credentials and distribute malware. By stopping the techniques used throughout the attack chain Intercept X keeps your organization secure against file-less attacks and zero-day exploits.

## Reduce the Attack Surface

Control which apps and devices can run in your environment, block malicious websites and potentially unwanted apps (PUAs) before they reach user or device.

## Synchronized Security

Sophos solutions work better together. For example, Intercept X and Sophos Firewall will share data to automatically isolate compromised devices while cleanup is performed, then return network access when the threat is neutralized. All without the need for admin intervention.

## Highlights

- Stops never seen before threats with deep learning AI
- Blocks ransomware and rolls back affected files to a safe state
- Prevents the exploit techniques used throughout the attack chain
- Reduces the attack surface with app, device and web control
- Performs threat hunting and IT ops security hygiene with XDR
- Provides 24/7/365 security delivered as a fully managed service
- Easy to deploy, configure and maintain even in remote working environments

## Extended Detection and Response (XDR)

Sophos XDR provides better accuracy and reduced workload for organizations performing threat hunting and IT ops security hygiene. Starting with industry leading protection reduces unwanted noise, and a prioritized list of detections paired with AI-guided investigations makes it easy to know where to start and quickly act. Native endpoint, server, firewall, email, cloud, mobile and O365 integrations are available in the data lake, or pivot to the device for real-time state and up to 90 days of historical data.

## Managed Threat Response (MTR)

24/7/365 threat hunting detection and response service that's delivered by a team of Sophos experts. Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, where, when, how and why.

## Straightforward Management

Intercept X is managed via Sophos Central, the cloud-management platform for all Sophos solutions. It's a single pane of glass for all of your devices and products, making it easy to deploy, configure and manage your environment even in remote working setups.

## AI and Expert Powered Data

Combining deep learning AI and the cybersecurity knowledge of SophosLabs experts, Intercept X gives organizations the best of both worlds with industry leading threat intelligence.

## Technical Specifications

Intercept X supports Windows and macOS deployments. For the latest information please read the Windows system requirements and Mac datasheet.

# Sophos Intercept X for Mobile

## Mobile Threat Defense (MTD) for Android, iOS and Chrome OS devices

Intercept X for Mobile protects users, their devices, and corporate data from known and never-before-seen mobile threats by leveraging our market leading Intercept X deep learning engine. It is all managed seamlessly through Sophos Central, alongside the entire Sophos portfolio of next-generation cybersecurity solutions.

### Device security

Sophos Intercept X for Mobile continuously monitors device health and notifies you if a device is compromised so you can take remediating action or automatically revoke access to corporate resources. Device security advisors detect jailbreaking or rooting and can inform the user and admin of necessary operating system updates.

### Network security

Establish a first line of defense at the mobile network level on Android and iOS. Network connections are examined in real time to check for suspicious characteristics that may identify an attack. This helps mitigate the risk of Man-in-the-Middle (MitM) attacks. Web filtering and URL checking stops access to known bad sites on mobile devices, while SMS phishing detection spots malicious URLs.

### Application security

Sophos Intercept X for Mobile detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Users and admins are notified if the threat status of a device changes. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.

### Centralized deployment, configuration, and reporting

Sophos Intercept X for Mobile can be centrally configured from Sophos Central, which hosts our Unified Endpoint Management (UEM) platform. Deployment can occur via existing app stores with user enrolment, or the app can be pushed using existing UEM's such as Sophos Mobile or third-party Enterprise Mobility Management (EMM) tools.

### Conditional access with Synchronized Security

Synchronized Security enables your defenses to work together as a system to be more coordinated than the attackers. Threat status information can be shared with Sophos Wireless access points to ensure all threats on devices are fully remediated before access to sensitive networks is granted.

### Highlights

- Protection for Android, iOS, and Chrome OS devices
- Deploy using Sophos Mobile or alternate UEM products
- Leverages Intercept X deep learning on Android
- Comprehensive Man-in-the-Middle (MitM) threat detection
- Award-winning mobile threat defense
- Microsoft Intune conditional access
- Available from the Apple App
- Store and Google Play Store

CRS
CYBER RETALIATOR SOLUTIONS

SOPHOS

www.CyberRetaliatorSolutions.com

# Sophos Managed Detection and Response

## 24/7 Threat Detection and Response

Sophos MDR is a fully managed 24/7 service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

## Ransomware and Breach Prevention Services

The need for always-on security operations has become an imperative. However, the complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organizations to successfully manage detection and response on their own.

With Sophos MDR, our expert team stops advanced human-led attacks. We take action to neutralize threats before they can disrupt your business operations or compromise your sensitive data. Sophos MDR is customizable with different service tiers, and can be delivered via our proprietary technology or using your existing cybersecurity technology investments.

## Cybersecurity Delivered as a Service

Enabled by extended detection and response (XDR) capabilities that provide complete security coverage wherever your data reside, Sophos MDR can:

Detect more cyberthreats than security tools can identify on their own
Our tools automatically block 99.98% of threats, which enables our analysts to focus on hunting the most sophisticated attackers that can only be detected and stopped by a highly trained human.

Take action on your behalf to stop threats from disrupting your business
Our analysts detect, investigate, and respond to threats in minutes — whether you need full-scale incident response or help making accurate decisions.

Identify the root cause of threats to prevent future incidents
We proactively take actions and provide recommendations that reduce risk to your organization. Fewer incidents mean less disruption for your IT and security teams, your employees, and your customers.

## Compatible with the Cybersecurity Tools You Already Have

We can provide the technology you need from our award-wining portfolio, or our analysts can leverage your existing cybersecurity technologies to detect and respond to threats.

Sophos MDR is compatible with security telemetry from vendors such as Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace, and many others. Telemetry is automatically consolidated, correlated, and prioritized with insights from the Sophos Adaptive Cybersecurity Ecosystem (ACE) and Sophos X-Ops threat intelligence unit.

### Highlights

- Stop ransomware and other advanced human-led attacks with a 24/7 team of threat response experts
- Maximize the ROI of your existing cybersecurity technologies
- Let Sophos MDR execute full-scale incident response, work with you to manage security incidents, or deliver detailed threat notifications and guidance
- Improve cyber insurance coverage eligibility with 24/7 monitoring and endpoint detection and response (EDR) capabilities
- Free up your internal IT and security staff to focus on business enablement

CRS
CYBER RETALIATOR SOLUTIONS

SOPHOS

www.CyberRetaliatorSolutions.com

## MDR That Meets You Where You Are

Sophos MDR is customizable with different service tiers and threat response options. Let the Sophos MDR operations team execute full-scale incident response, work with you to manage cyberthreats, or notify your internal security operation teams any time threats are detected. Our team quickly learns the who, what, when, and how of an attack. We can respond to threats in minutes.

## Key Capabilities

### 24/7 Threat Monitoring and Response

We detect and respond to threats before they can compromise your data or cause downtime. Backed by six global security operations centers (SOCs), Sophos MDR provides around-the-clock coverage.

### Compatible with Non-Sophos Security Tools

Sophos MDR can integrate telemetry from third-party endpoint, firewall, identity, email, and other security technologies as part of Sophos ACE.

### Full-Scale Incident Response

When we identify an active threat, the Sophos MDR operations team can execute an extensive set of response actions on your behalf to remotely disrupt, contain and fully-eliminate the adversary.

### Weekly and Monthly Reporting

Sophos Central is your single dashboard for real-time alerts, reporting, and management. Weekly and monthly reports provide insights into security investigations, cyberthreats, and your security posture.

### Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE automatically prevents malicious activity and enables us to search for weak signals for threats that require human intervention to detect, investigate, and eliminate.

### Expert-Led Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own. The Sophos MDR operations team can also use third-party vendor telemetry to conduct threat hunts and identify attacker behaviors that evaded detection from deployed toolsets.

### Direct Call-in Support

Your team has direct call-in access to our Security Operations Center (SOC) to review potential threats and active incidents. The Sophos MDR operations team is available 24/7/365 and backed by support teams across 26 locations worldwide.

### Dedicated Incident Response Lead

We provide you with a Dedicated Incident Response Lead who collaborates with your internal team and external partner(s) as soon as we identify an incident and works with you until the incident is resolved.

### Root Cause Analysis

Along with providing proactive recommendations to improve your security posture, we perform root cause analysis to identify the underlying issues that led to an incident. We give you prescriptive guidance to address security weaknesses so they cannot be exploited in the future.

### Sophos Account Health Check

We continuously review settings and configurations for endpoints managed by Sophos XDR and make sure they are running at peak levels.

### Threat Containment

For organizations that choose not to have Sophos MDR perform full-scale incident response, the Sophos MDR operations team can execute threat containment actions, interrupting the threat and preventing spread. This reduces workload for internal security operations teams and enables them to rapidly execute remediation actions.

### Intelligence Briefings: “Sophos MDR ThreatCast”

Delivered by the Sophos MDR operations team, the “Sophos MDR ThreatCast” is a monthly briefing available exclusively to Sophos MDR customers. It provides insights into the latest threat intelligence and security best practices.

### Breach Protection Warranty

Included with Sophos MDR Complete one-, two-, and three-year licenses, the warranty covers up to $1 million in response expenses. There are no warranty tiers, minimum contract terms, or additional purchase requirements.

## Sophos Service Tiers

| | Sophos Threat Advisor | Sophos MDR | Sophos MDR Complete |
|---|---|---|---|
| 24/7 expert-led threat monitoring and response | ✔ | ✔ | ✔ |
| Compatible with non-Sophos security products | ✔ | ✔ | ✔ |
| Weekly and monthly reporting | ✔ | ✔ | ✔ |
| Monthly intelligence briefing: “Sophos MDR ThreatCast” | ✔ | ✔ | ✔ |
| Sophos Account Health Check | | ✔ | ✔ |
| Expert-led threat hunting | | ✔ | ✔ |
| Threat containment: attacks are interrupted, preventing spread<br>Uses full Sophos XDR agent (protection, detection, and response) or Sophos XDR Sensor (detection and response) | | ✔ | ✔ |
| Direct call-in support during active incidents | | ✔ | ✔ |
| Full-scale incident response: threats are fully eliminated<br>Requires full Sophos XDR agent (protection, detection, and response) | | | ✔ |
| Root cause analysis | | | ✔ |
| Dedicated Incident Response Lead | | | ✔ |
| Breach Protection Warranty<br>Covers up to $1 million in response expenses | | | ✔ |

## Sophos MDR Included Integrations

Security data from the following sources can be integrated for used by the Sophos MDR operations team at no additional cost. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

XDR

### Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and Microsoft integrations

Included in Sophos MDR and Sophos MDR Complete Pricing

Fw

### Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm

Product sold separately; integrated at no addtional charge

### Microsoft Graph Security

Microsoft Defender for Endpoint Microsoft Defender for Cloud
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity

Identity Protection (Azure AD)
Microsoft Azure Sentinel
Office 365 Security and Compliance Center
Azure Information Protection

Ep

### Sophos Endpoint

Block advanced threats and detect malicious behaviors — including attackers mimicking legitimate users

Included in Sophos MDR and Sophos MDR Complete Pricing

Em

### Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks

Product sold separately; integrated at no addtional charge

### Office 365 Management Activity

Provides information on user, admin, system, and policy actions and events from Office 365 and Azure Active Directory logs

Cld

### Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform

Product sold separately; integrated at no addtional charge

### 90-Days Data Retention

Retains data from all Sophos products and any third-party (non-Sophos) products in the Sophos Data Lake

### Third-Party Endpoint Protection

Compatible with...

Microsoft
CrowdStrike
SentinelOne
Trend Micro

Trellix
BlackBerry (Cylance)
Symantec (Broadcom)
Malwarebytes

CRS
CYBER RETALIATOR SOLUTIONS

SOPHOS

## Add-On Integrations

Security data from the following third-party sources can be integrated for use by the Sophos MDR operations team via the purchase of Integration Packs. Telemetry sources are used to expand visibility across your environment, generate new threat detections and improve the fidelity of existing threat detections, conduct threat hunts, and enable additional response capabilities.

### NDR Sophos Network Detection and Response

Continuously monitor activity inside your network to detect suspicious actions occurring between devices that otherwise are unseen

Compatible with any network via SPAN port mirroring

### Firewall

Compatible with...

Palo Alto Networks
Fortinet
Check Point
Cisco
SonicWall

### Identity

Compatible with...

Okta
Duo
ManageEngine

### Public Cloud

Compatible with...

AWS Security Hub
AWS CloudTrail
Orca Security
Google Cloud Platform Security

### Email

Compatible with...

Proofpoint
Mimecast

### Network

Compatible with...

Darktrace
Tinkst Canary
Skyhigh Security

### 1-Year Data Retention

## Sophos MDR Guided Onboarding

For an additional purchase, Sophos MDR Guided Onboarding is available for remote onboarding assistance. The service provides hands-on support for a smooth and efficient deployment, ensures best practice configurations, and delivers training to maximize the value of your MDR service investment. You are provided a dedicated contact from the Sophos Professional Services organization who will be with you through your first 90 days to make sure your implementation is a success. Sophos MDR Guided Onboarding includes:

### Day 1 - Implementation

Project kickoff

Configure Sophos Central and review of features

Build and test deployment process

Configure MDR integrations

Configure Sophos NDR sensor(s)

Enterprise-wide deployment

### Day 30 - XDR Training

Learn to think and act like a SOC

Understand how to hunt for indicators of compromise

Gain an understanding of using our XDR platform for administrative tasks

Learn to construct queries for future investigations

### Day 90 Security Posture Assessment

Review current policies for best practice recommendations

Discuss features that are not in use that could provide additional protection

Security assessment following NIST framework

Receive summary report with recommendations from our review

CRS CYBER RETALIATOR SOLUTIONS

SOPHOS

## | PENETRATION TESTING

## | VULNERABILITY SCAN

## | WEB APPLICATION SCANNING

## | PROFESSIONAL SERVICES

01 SCOPING

02 DISCOVERY, RECONNAISSANCE, AND INFORMATION GATHERING

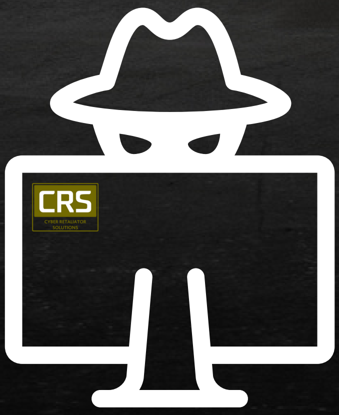
03 NETWORK ENUMERATION AND SCANNING

04 VULNERABILITY MAPPING

05 EXPLOITATION

06 CLEAN UP

07 REPORTING



# CONTACT US:

## IBM Training

+(27) 12 023 1959
Training@CyberRetaliatorSolutions.com

## Distribution

+(27) 12 023 1959
CRSCyberSales@CyberRetaliatorSolutions.com

## Head Office Address:

6D Longdale Street, Midstream Estate, Centurion, South Africa, 1692
Office Line: (+27) 12 023 1959

## Visit our website:

www.CyberRetaliatorSolutions.com