

# DefCyte is a GDPR compliant e-mail phishing detection and inbox security solution



Remote working is on the rise, and attackers are now trying to exploit e-mail communication more than ever. E-mail phishing attacks increased 667 percent after the COVID-19 outbreak in 2020. As the users will become more mobile, it should be expected that the numbers will continue to grow. Parallel to this increase, it is also becoming challenging to block these malicious e-mails as they are becoming more targeted and specific to the end-user. Research shows that phishing has become the most dynamic and adaptive threat type organisations face.

DefCyte provides a complete view of threats arising from phishing attacks. The users can report e-mails that they suspect is suspicious. Machine learning-based classification algorithm provides an extensive real-time view into threats. Recently initiated sites and domains are easily blocked before being identified as malicious by the traditional secure e-mail gateway solutions. The platform provides unmatched visibility for malicious e-mails reaching the end-users. Once an e-mail is identified as malicious, the system can delete the e-mail from all user mailboxes.

Phishing simulation and user awareness training are also provided as built-in modules to enable organisations to prepare better for phishing attacks.

DefCyte is based on the CloudCyte platform. CloudCyte is a multi-tenant, containerised SaaS platform for protecting users, networks and applications from cyber threats. The system allows end-users and MSSP's to deploy the solution in minutes. On-premise deployment on VMWARE/Hyper-V and Cloud-based deployment on Kubernetes is supported.

## Detect

Detect the threats from malicious e-mails and protect users.

## Enforce

Enforce adaptive policies across the entire infrastructure regardless of technology, user and device.






## Enable

Enable a better user experience supporting both desktop and mobile platforms.

## Automate

Utilise dynamic policies with automated actions for identifying and deleting malicious e-mails.

## Product Benefits

-  **Real-time threat intelligence.**
-  **Increased user awareness.**
-  **Identification of targeted phishing attacks.**
-  **Deploy in minutes with no maintenance overhead.**
-  **Integration with existing security solutions for automated and centralised response.**

## DefCyte at a Glance

### • VISIBILITY

Identify phishing attacks bypassing the existing security controls.

### • PROTECTION

Policy enforcement and baselining with in-depth threat discovery.

### • AUTOMATION

Policies enable automated actions for malicious activity. Malicious e-mails can be deleted from all user mailboxes.

### • GDPR COMPLIANCE

Only the metadata collected from the e-mail is analysed, enabling complete GDPR compliance.

### • RETURN ON INVESTMENT

Reduce administrative overhead, risks, and improve infrastructure management.

## Technical Features

The end-user module is deployed in minutes through Office 365 and Microsoft Exchange.

Advanced metadata analyses by extracting domain and matched keywords from e-mail header and body.

Complete GDPR compliance by supporting only metadata reporting.

Centralised investigation for reported e-mails.

**Support for automated actions:**

- SMS
- e-mail
- SNMP
- Execute command

Identification of newly registered domains, phishing sites and e-mails exploiting zero-day attacks.

Automatic deletion of e-mails flagged as malicious.

Built-in templates for phishing attacks, simulations and user awareness training.

Active Directory integration support.

Reporting based on HTML, pdf and csv formats.

## Modules



### DefCyte Simulation

DefCyte Simulation enables the testing of end-user awareness for phishing attacks.



### DefCyte Training

DefCyte Training helps an organisation to train its employees for increased awareness.



### DefCyte Sight

DefCyte Sight classifies e-mails and detects suspicious e-mails through the built-in intelligence network.



### DefCyte Analyzer

DefCyte Analyzer enables robust inbox security. The end-users can perform a security check and report suspicious e-mails with just one click on any incoming e-mail.

## Hardware Requirements for On-Premise Deployments

Scale	Server
0-10000 Users	1x 6 Core CPU, 16 GB RAM, 250 GB HDD
10001-25000 Users	2x 6 Core CPU, 32 GB RAM, 500 GB HDD
25000+ Users	For every 25000 Users using one server is recommended.

### Platform Support

- Office 365
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft Outlook 2013-2019
- Microsoft Outlook for IOS
- Microsoft Outlook for Android
- Microsoft Outlook for MAC

## About CyberCyte

CyberCyte is a UK based cybersecurity company that provides a framework of solutions based on the Circle of Zero Trust for identity management, network access control, and DNS security. Our integrated security solutions enable enterprises, governments and service providers to protect their users and digital assets seamlessly with minimum operational overhead..

Davidson House, Kings Road Reading UK RG1 4EU

+44 118 900 1422

[www.cybercyte.com](http://www.cybercyte.com)