

# Co-sell Xylos Secure Modern Workplace Endpoint Management Workshop

# Xylos



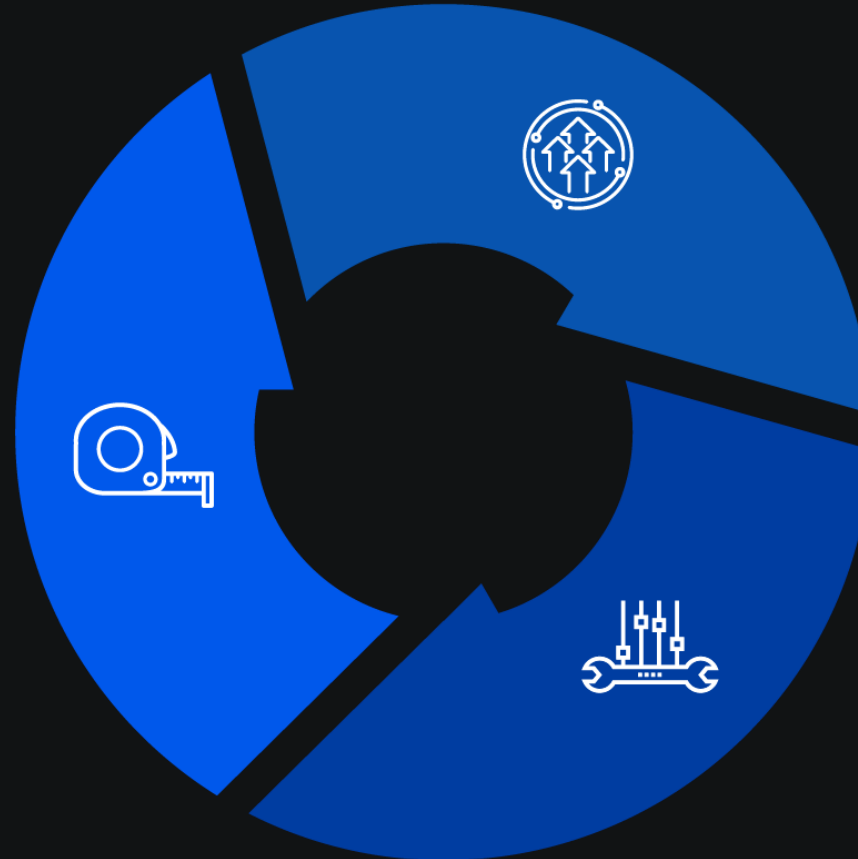
Tony Verhaegen & Paul Peersman

*We believe successful solutions require a human perspective,  
a strategic approach, a solid understanding of data and technology as well as a  
strong execution.*

# The Xylos security approach

## ASSESS

- Baseline measuring
- Establish endpoint overview
- Define building blocks
- Create roadmap



## IMPROVE

- Implement technology, procedures, policies
- Improve resilience, lower risk

## MANAGE

- Follow up compliance
- Maintain resilience level, both for technology and people

# Interviews & workshops

## Questionnaires



### Device Management Objectives and Requirements

Please provide information about the device management objectives and requirements.

| Question  | Answer  | Comment |
|---|---|---------|
| What are the top device management challenges you are facing? | <input type="checkbox"/> Challenge to prevent security threats from entering the enterprise environment caused by mobile access to corporate applications and data.<br><input type="checkbox"/> No remote access to on premise LOB applications from mobile devices.<br><input type="checkbox"/> Challenge to comply with data privacy and information protection regulations (like HIPAA and GDPR).<br><input type="checkbox"/> No tools to manage lost or stolen devices and to prevent corporate data leakage.<br><input type="checkbox"/> Mobile Device types and operating systems fragmentation makes it difficult for IT to provide a consistent user experience and to secure corporate applications and data across all these platforms.<br><input type="checkbox"/> Other, please specify |         |

|   |   |  |
|---|---|--|
| Does your organization provide company phones and/or tablets to employees?                              | <input type="checkbox"/> Yes, please specify<br><input type="checkbox"/> No |  |
| Are employees allowed to access corporate email, data, or applications from personal phones or tablets? | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                 |  |
| Do employees have remote access to corporate applications and data from their company Windows laptop?   | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                 |  |
| Do employees have remote access to corporate applications and data from                                 | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                 |  |

### Device Management

Please provide information about your device management environment:

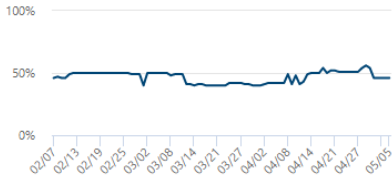
| Question  | Answer   | Comment |
|---|--|---------|
| What, if any, Mobile Device Management (MDM) solutions have you currently deployed?   | <list MDM products>  |         |
| Are Windows 10 devices currently managed with Microsoft Endpoint Configuration Manager?   | <input type="checkbox"/> Yes<br>Version: <version?><br><input type="checkbox"/> No |         |
| Can your IT team manage all work devices from a single console?   | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |
| Do your current solutions let you control settings on personal devices used by employees for work (BYOD)?   | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |
| Can your IT team automatically deploy company-required apps and updates to personal devices used for work and managed by IT?                                  | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |
| Do employees have access to optional, company-approved apps they can download to the devices they use for work?   | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |
| Can your IT team control employee access to company data?   | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |
| Can IT protect company data in managed apps (including Office Mobile apps) used on personal devices, including employee's devices that are not managed by IT? | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |
| Can you provide self-service functions to employees for managing aspects of their access and mobile devices, such as password reset or device enrollment?     | <input type="checkbox"/> Yes<br><input type="checkbox"/> No                        |         |

# Technical assessments

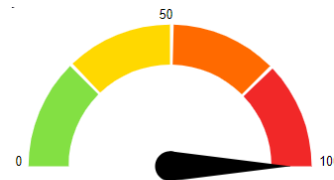
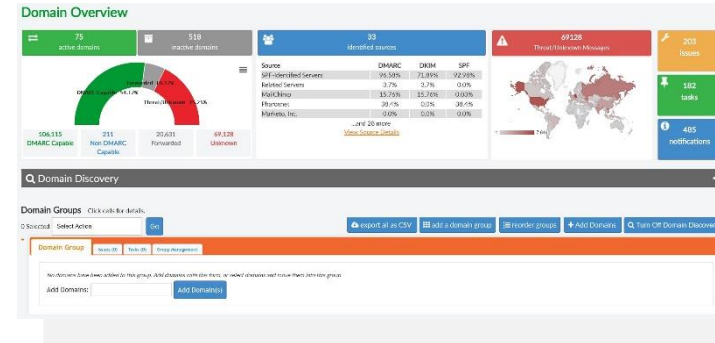
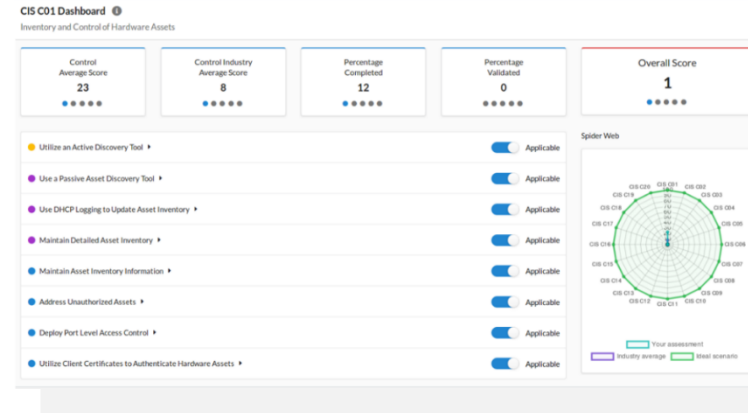
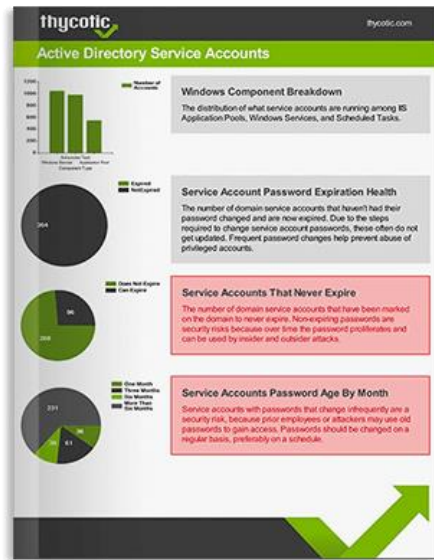
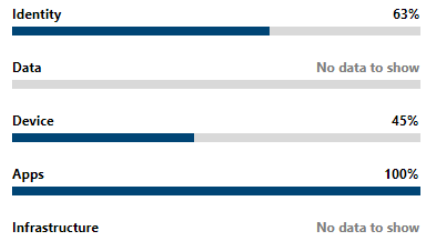


## Secure Score: 46%

379/820 points achieved

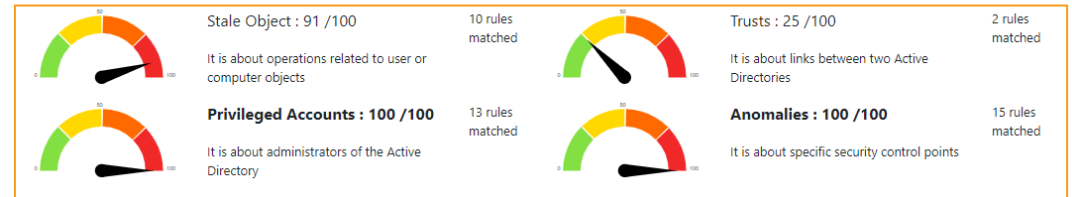


Breakdown points by: Category



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better



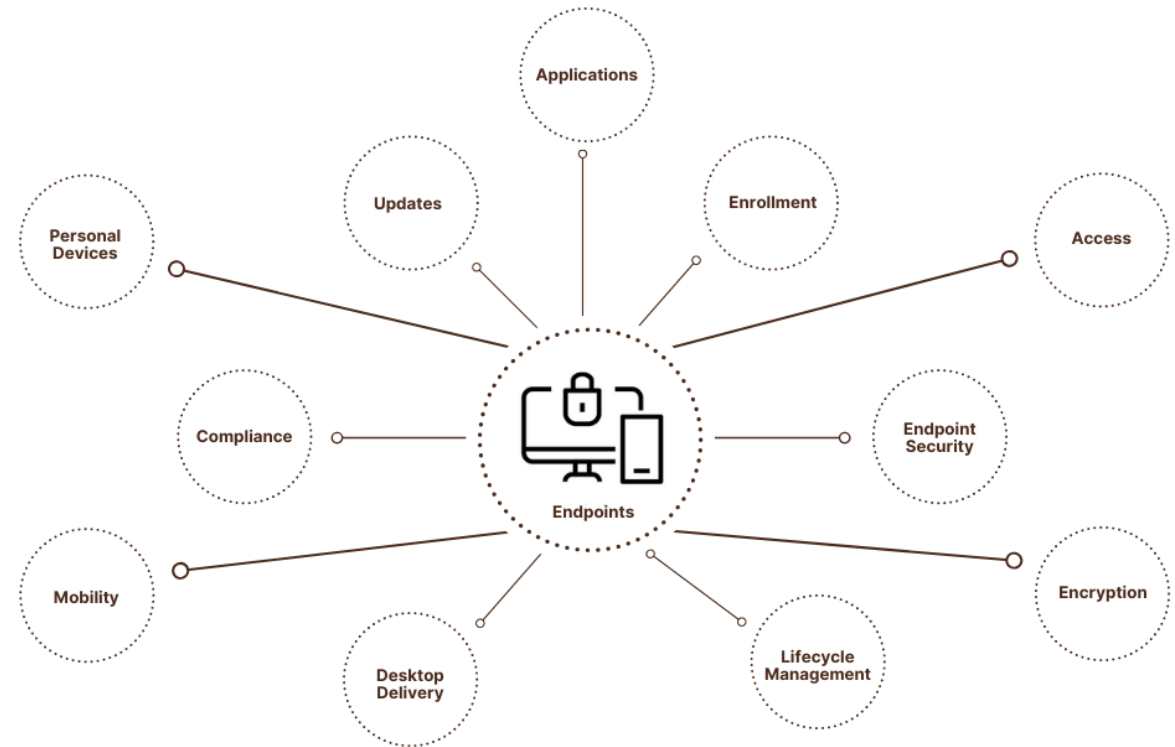
# Create Roadmap



# Endpoint Management

Based on 4 major cornerstones:

- Enrolling and managing Endpoints
- Protecting and securing all Endpoints and applications
- Maintaining and updating endpoints to achieve compliancy
- Delivering applications in a secure manner

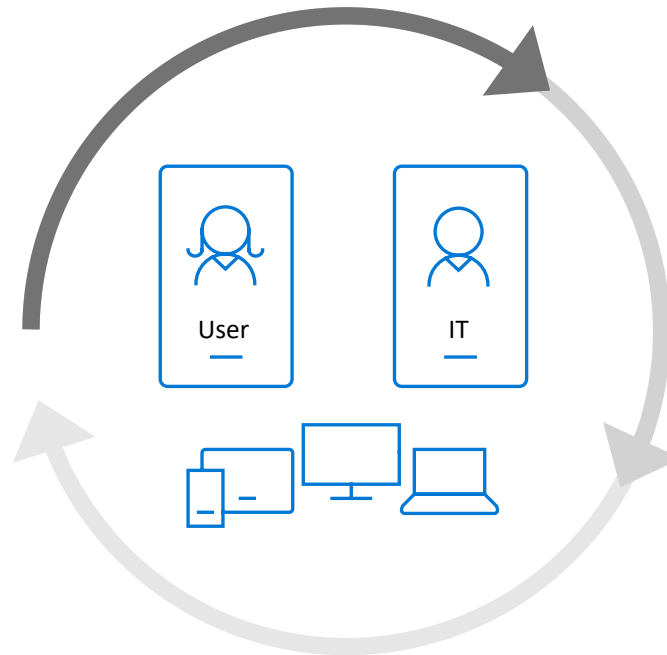


## Enroll

- ✓ Provide specific enrollment methods for iOS/iPadOS, Android, Windows, and macOS
- ✓ Provide a self-service Company Portal for users to enroll BYOD devices
- ✓ Deliver custom terms and conditions at enrollment
- ✓ Zero-touch provisioning with automated enrollment options for corporate devices

## Support & Retire

- ✓ Revoke access to corporate resources
- ✓ Perform selective wipe
- ✓ Audit lost and stolen devices
- ✓ Retire device
- ✓ Provide Remote Assistance



## Configure

- ✓ Deploy certificates, email, VPN, and Wi-Fi profiles
- ✓ Deploy device security policy settings
- ✓ Install mandatory apps
- ✓ Deploy device restriction policies
- ✓ Deploy device feature settings

## Protect

- ✓ Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- ✓ Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- ✓ Report on device and app compliance



# Technical Support Services



## Essentials

Service Desk Access

Incident handling  
(All incidents included)

Patch management



## Standard

Technical monitoring

Backup Management

Compliance monitoring



## Premium

Incident Priority Upgrade

Functional / Technical Advisory

Xylos Technical  
Account Management

Essentials: Business hours, Standard and Premium: 24/7

### Service Delivery Management

Service reporting

Service Management

Governance

### Support Package

Standard changes

Non-standard changes

Functional support

Information request



# Xylos

Inspired by technology,  
atypical by nature.