Microsoft 365
Business Premium

ZERO TRUST DEPLOYMENT FOR YOUR BUSINESSES

DIRACDELTA
SYSTEMS

P : +27 64 655 1853 **E :** info@diracdelta.co.za **W :** diracdelta.co.za

Reduce risk by rapidly modernizing security capabilities and practices

WHAT IS ZERO TRUST?

PRINCIPLE	DESCRIPTION
Verify explicity	**Always authenticate and authorize** based on all available data points.
Use least privilege access	**Limit user access with Just-In-Time and Just-Enough-Access (JIT/ JEA),** risk-based adaptive policies, and data protection.
Assume breach	**Minimize blast radius and segment access.** Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defences.

This is the Core of Zero Trust: https://learn.microsoft.com/en-gb/security/zero-trust/zero-trust-overview

WHO
WE ARE

Dirac Delta Systems (DDS)
Your Trusted IT Partner

Founded in 2011, DDS empowers businesses with cutting-edge technology solutions. Since our inception, we have established ourselves as a trusted Managed Services Provider (MSP), delivering industry best practice support and infrastructure management to clients across various industries.

In addition to our MSP arm, DDS also offers comprehensive consulting services that help organizations navigate the complexities of modern IT landscapes. Our team of experienced professionals excels at identifying opportunities for innovation and transformation, assisting clients in leveraging cloud technologies to enhance their business operations. Whether it's optimizing existing infrastructure or developing tailored strategies for digital growth, we guide our clients through every step of their technology journey.

Technology Solutions.
Delivered with Excellence.

OUR
PARTNERS

Microsoft
Cloud Solution Provider

N-ABLE

CORO

> Reduce risk by rapidly modernizing security capabilities and practices

HOW WE HELP
YOUR BUSINESS GROW

Business and Technical Drivers

- What is top of mind for business stakeholders?
- What risks are important to the business?
- Business/technology initiatives driving change?
- What metrics are important to your program?

Architecture, Policy, and Collaboration

Describe how teams work together on end-to-end security + guiding documents/artifacts

- Enterprise-wide security architecture approach and documentation
- Policy update, monitoring, and related governance processes
- Posture and vulnerability management processes
- Technical collaboration processes (e.g. sharing learnings, joint technical planning, etc. with security operations, architects, engineers, posture management, governance, others)
  Differences between on premises vs. cloud processes

Geography and Cloud Usage

- Where does your organization operate?
- Which workloads are in the cloud?
- Which major cloud providers?
  (SaaS, PaaS, IaaS)

Compliance

Large & notable regulatory requirements

Threats

What types of attacks and adversaries are top of mind?

KEEPING YOUR ASSETS AWAY FROM ATTACKERS

IT Security is Complex

Many Devices, Users, & Connections

Trusted network security strategy

- Initial attacks were network based
- Seemingly simple and economical
- Accepted lower security within the network

Assets increasingly leave the network

- BYOD, WFH, Mobile, and SaaS

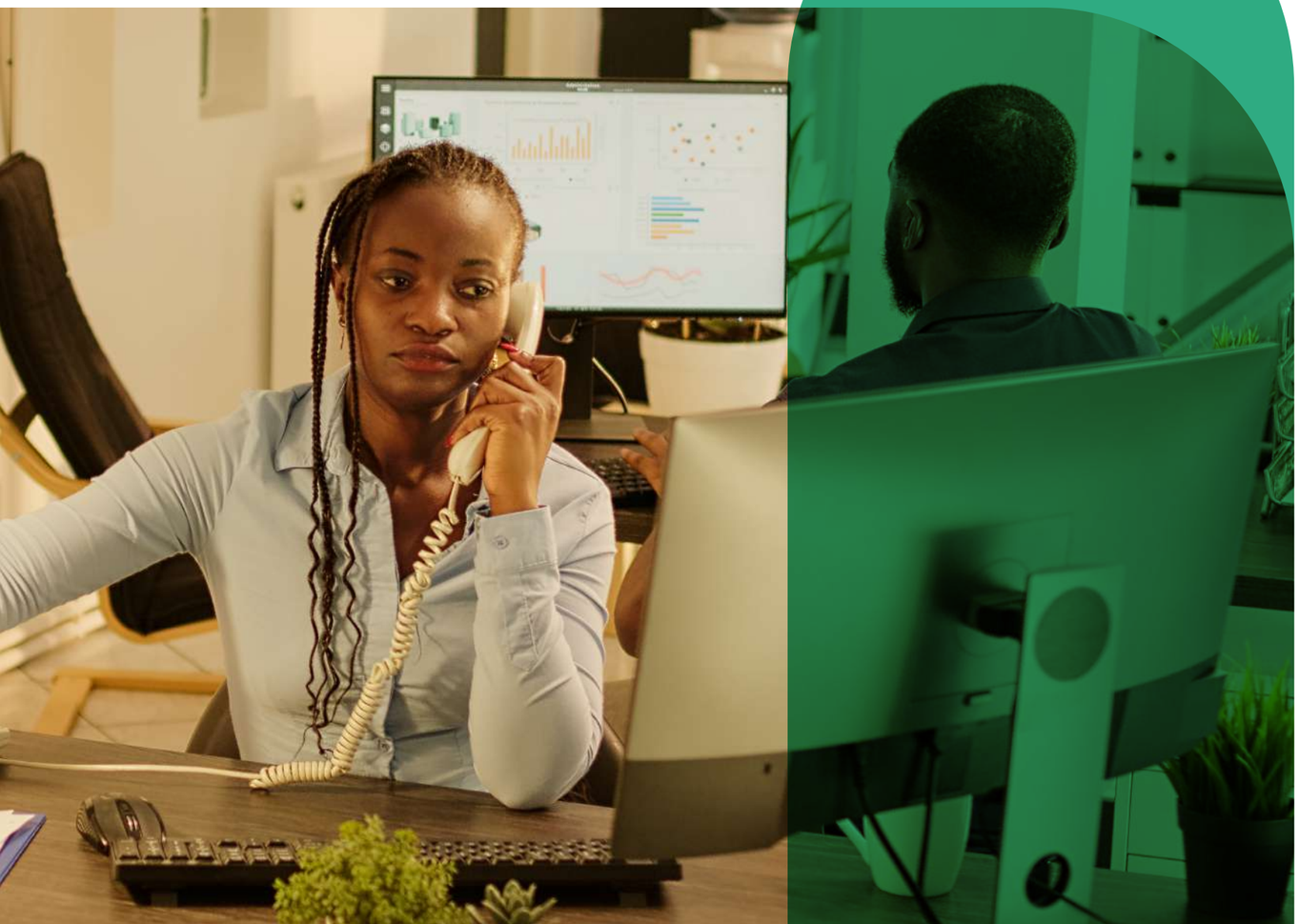
IT Security is Complex

- Phishing and credential theft
- Security teams often overwhelmed

ZERO TRUST FOR YOUR BUSINESS

Introduction to Microsoft Zero Trust

- **What is Zero Trust?**
  Zero Trust *is a* ***security*** *framework that assumes no user or device is* ***trustworthy*** *by default, requiring* ***continuous verification*** *and* ***strict access*** *controls to protect data and systems.*
- Microsoft Zero Trust Security Principles
- Microsoft Zero Trust Architecture
- Microsoft Cybersecurity Reference Architecture (MCRA)

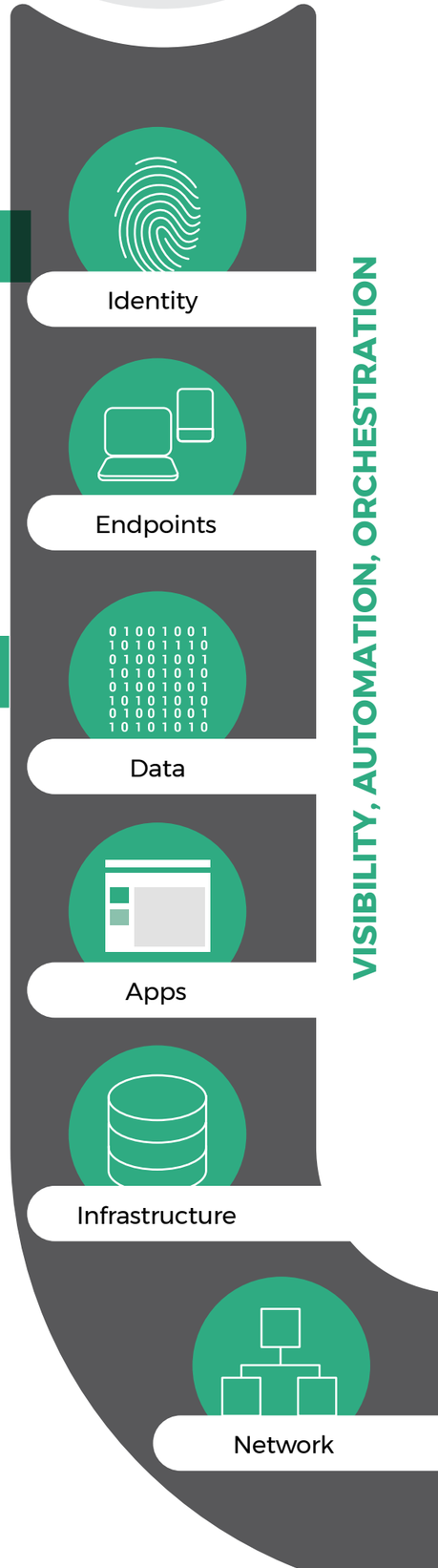


Five Steps to apply Zero Trust for SMB

- **Step 1.** Configure Zero Trust identity and device access protection
- **Step 2.** Manage endpoints with Intune
- **Step 3.** Add Zero Trust identity and device access protection
- **Step 4.** Evaluate, pilot, and deploy Microsoft Defender XDR
- **Step 5.** Protect and govern sensitive data

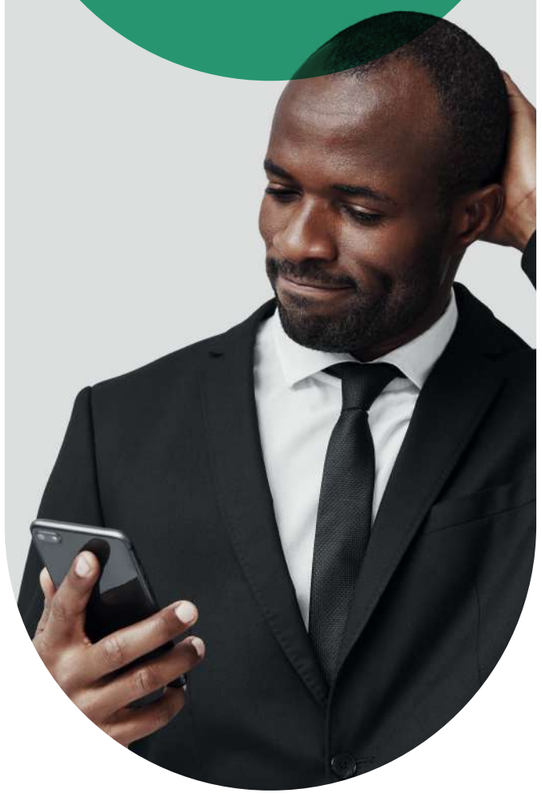
Microsoft Business Premium

- **What is M365 Business Premium?**
- ***Microsoft 365 Business Premium*** *is a*
- *comprehensive* ***subscription plan*** *that*
- *combines* ***productivity apps*** *like Word*
- *and Excel with* ***advanced security*** *features, device* ***management****, and cyber threat* ***protection.***
  Why Business Premium?
  Business Premium *is ideal for* ***small*** *and* ***medium businesses*** *needing enhanced* ***security, remote work*** *capabilities, and comprehensive* ***IT management****, all in one* ***cost-effective*** *solution.*



THE PROBLEM

False Assumptions



False Assumptions:
of implicit or explicit trust

Security is the opposite of productivity

All attacks can be prevented

Network security perimeter will keep attackers out

Passwords are strong enough

IT Admins are safe

IT Infrastructure is safe

Developers always write secure code

The software and components we use are secure

THE SOLUTION

Zero Trust Mitigation:
Systematically Build & Measure Trust

Business Enablement Align security to the organization's mission, priorities, risks, and processes

Assume Compromise Continuously reduce blast radius and attack surface through prevention and detection/ response/recovery

Shift to Asset-Centric Security Strategy Revisit how to do access control, security operations, infrastructure and development security, and more

Explicitly Validate Account Security Require MFA and analyze all user sessions with behavior analytics, threat intelligence, and more

Plan and Execute Privileged Access Strategy Establish security of accounts, workstations, and other privileged entities (aka.ms/spa)

Validate Infrastructure Integrity Explicitly validate trust of operating systems, applications, services accounts, and more

Integrate security into development process Security education, issue detection and mitigation, response, and more

Supply chain security Validate the integrity of software and hardware components from open source. vendors, and others

PHASED APPROACH

Zero Trust deployment with Microsoft 365

Define | Plan | Ready | Adopt | Govern | Manage

Step 1

Configure Zero Trust identity and device access protection:
Starting-point policies

The first step is to build your Zero Trust foundation by configuring identity and device access protection.

Step 2

Manage endpoints with Intune

Next, enroll your devices into management with Intune and begin protecting them with more sophisticated controls.

Step 3

Add Zero Trust identity and device access protection:
Enterprise policies

With devices enrolled into management, you can now implement the full set of recommended Zero Trust identity and device access policies, requiring compliant devices.

Step 4

Microsoft Defender for Endpoint (MDE)

Microsoft Defender XDR is an extended detection and response (XDR) solution that automatically collects, correlates, and analyses signal, threat, and alert data from across your Microsoft 365 environment, including endpoint, email, applications, and identity

Step 5

Microsoft Purview

Microsoft Purview Information Protection capabilities are included with Microsoft Purview and give you the tools to know your data, protect your data, and prevent data loss.

CONTACT US
LET'S TALK.

diracdelta.co.za

info@diracdelta.co.za

+27 64 655 1853

+27 64 655 1853

diracdelta.co.za

DIRACDELTA
SYSTEMS