



**DIRAC
DELTA**
SYSTEMS

ZERO TRUST DEPLOYMENT FOR YOUR BUSINESSES

Reduce risk by rapidly modernizing
security capabilities and practices



THE PROBLEM

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 behaviour 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.



WHAT IS ZERO TRUST?

PRINCIPLES



Verify Explicitly

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.

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





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.



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.





PHASED **APPROACH**

Zero Trust deployment with Microsoft 365



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.

Define

Plan

Ready

Adopt

Govern

Manage

CONTACT US **LET'S TALK.**



info@diracdelt.com.hk



diracdelt.com.hk

Follow us on:

