DXC Technology

Micro Segmentation for Zero Trust

G-Cloud 15

Service Definition Document

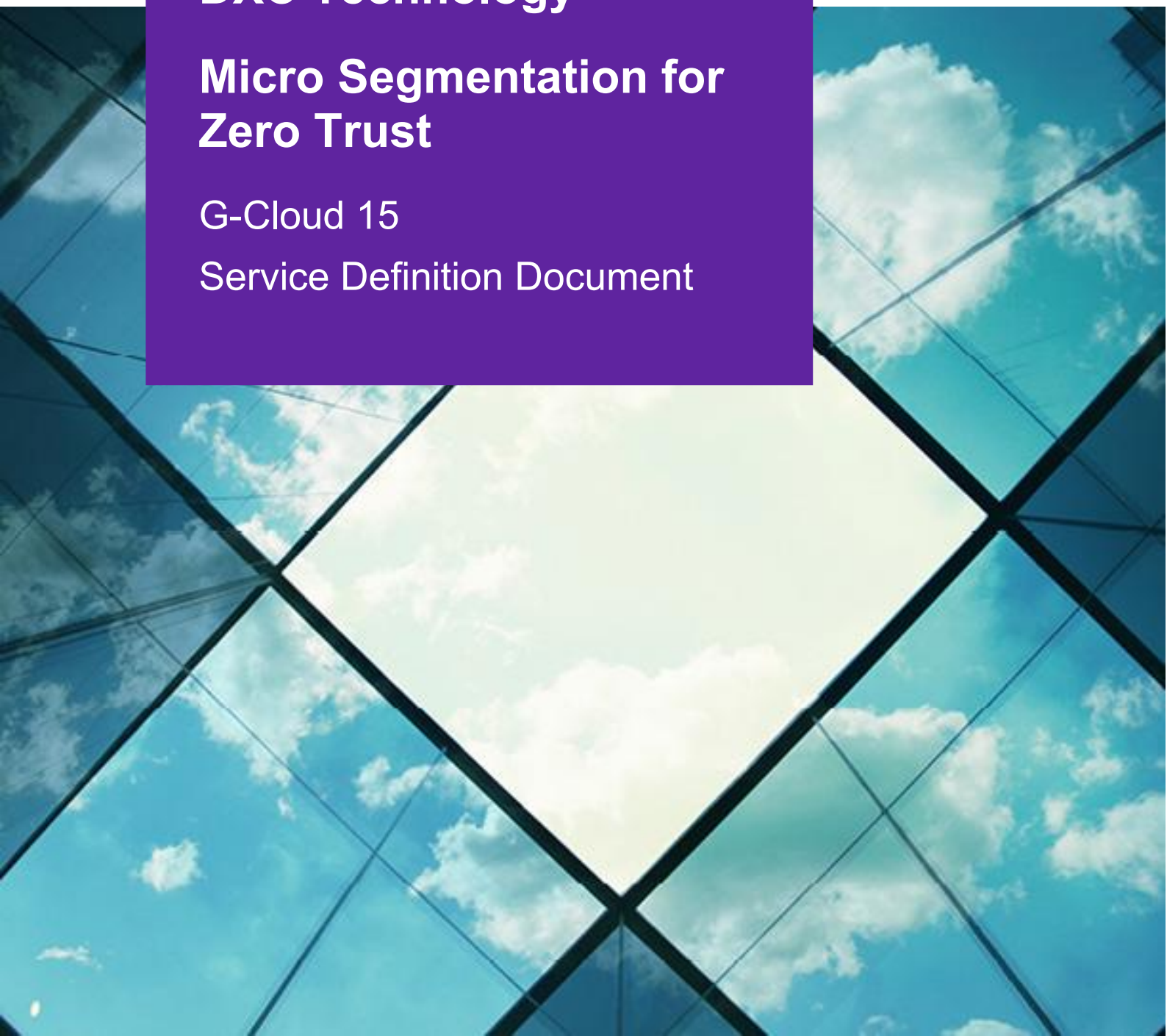

Table of Contents

DXC Micro Segmentation for Zero Trust

1. Service Overview

Micro segmentation for Zero Trust Security

Micro segmentation is an advanced security approach that extends traditional network segmentation by applying **granular, workload-level policies** across hybrid environments. Unlike perimeter-based defences, micro segmentation focuses on **containment-first strategies** to prevent lateral movement of threats, ensuring that even if a breach occurs, its impact is minimized.

As organizations transition to **Zero Trust architectures**, micro segmentation becomes a critical enabler. It provides:

- **Real-time visibility** into application traffic and dependencies.
- **Dynamic policy enforcement** based on workload identity rather than IP addresses.
- **Consistent security controls** across on-premises data centres, cloud workloads, and containerized environments.

Our solution leverages **Illumio's Adaptive Security Platform (ASP)** to deliver:

- **Application Dependency Mapping** for complete traffic visibility.
- **Label-based policy management** for simplified segmentation.
- **Host-based enforcement** using native OS firewalls, eliminating the need for network re-architecture.
- **Integration with SIEM/SOAR platforms** for enhanced monitoring and incident response.

This service is designed to be **non-disruptive, scalable, and future proof**, aligning with your existing infrastructure and compliance requirements while supporting long-term Zero Trust strategies.

DXC & Illumio

Identify risks

Set policies

Stop adversaries

2. Service Description

2.1Service Features (Base)

Our Micro segmentation solution, powered by **Illumio Adaptive Security Platform (ASP),** delivers a comprehensive set of capabilities designed to secure workloads across hybrid environments without requiring network re-architecture. Key features include:

1. Application Dependency Mapping

- Visualize all traffic flows between workloads, applications, and environments.
- Identify critical communication paths to support segmentation decisions.

2. Label-Based Security Policies

- Simplify policy creation using labels such as Role, Application, Environment, and Location.
- Enable consistent enforcement across diverse infrastructure.

3. Real-Time Policy Simulation

- Test segmentation policies before enforcement to avoid disruptions.
- Validate impact on live traffic without affecting production workloads.

4. Zero Trust Segmentation

- Enforce least-privilege access dynamically.
- Prevent lateral movement of threats across on-premises, cloud, and containerized environments.

5. Host-Based Enforcement

- Apply policies at the workload level using native OS firewalls.
- No dependency on network changes or complex firewall architectures.

6. Ransomware Containment

- Isolate compromised workloads instantly to stop malware propagation.
- Enable proactive breach containment strategies.

7. Integration & Automation

- Seamless integration with SIEM/SOAR platforms (e.g., Microsoft Sentinel) for monitoring and incident response.
- API-driven automation for policy creation and updates.
- Support for configuration management tools like Ansible, Puppet, and Terraform.

8. Reporting & Compliance

- Generate detailed reports on application dependencies, segmentation status, and policy enforcement.
- Achieve audit-ready compliance for frameworks like PCI DSS.

2.2 Service Benefits

DXC's Microsegmentation service delivers strategic security and operational advantages that help organizations transition to a Zero Trust architecture while maintaining business continuity. Below are the key benefits:

1. Enhanced Security Posture

- Stop Lateral Movement: DXC implements Illumio's host-based segmentation to prevent attackers from moving across workloads.
- Zero Trust Enforcement: Policies are aligned with least-privilege principles, reducing exposure to internal and external threats.
- Context-Aware Segmentation: DXC ensures policies are based on application behavior, user context, and workload criticality.

2. Rapid Breach Containment

- Immediate Isolation: DXC enables proactive isolation of high-value assets or reactive isolation of compromised systems during an active attack.
- Ransomware Mitigation: By segmenting workloads, DXC helps limit ransomware spread and minimize business impact.

3. Simplified Compliance

- Audit-Ready Policies: DXC delivers structured labeling and policy frameworks that meet compliance standards like PCI DSS, GDPR, and ISO 27001.
- Data-in-Motion Encryption: SecureConnect ensures encrypted workload-to-workload communication, supporting regulatory requirements.

4. Operational Efficiency

- Non-Disruptive Deployment: DXC uses host-based enforcement, avoiding complex network redesigns.
- Automation at Scale: DXC integrates Illumio with automation tools (Ansible, Puppet, Terraform) for large-scale deployments.
- Integration with Existing Ecosystem: DXC connects Illumio with SIEM/SOAR platforms (e.g., Microsoft Sentinel) for unified monitoring and incident response.

5. Scalability & Future-Readiness

- Hybrid Environment Support: DXC ensures consistent policy enforcement across on-premises, cloud, and containerized workloads.
- Adaptable Architecture: The solution scales with business growth and integrates seamlessly with existing security stacks.

6. Cost Optimization

- Reduced Hardware Dependency: DXC minimizes reliance on expensive perimeter firewalls and legacy segmentation methods.
- Lower Operational Overhead: Automated policy management and simplified workflows reduce administrative burden.

7. Business Impact

- Risk Reduction: Significant decrease in attack surface and lateral movement risk.
- Compliance Acceleration: Faster audits and regulatory adherence.
- Operational Resilience: Improved uptime and reduced disruption during security incidents.

2.3KPI Definitions

1. Risk-Based Visibility

- **Definition:** Ability to visualize and analyze all traffic flows across environments and applications.
- **Measurement:**
  - % of workloads mapped in Application Dependency Map (ADM).
  - Number of risky flows identified (e.g., Dev-to-Prod, Telnet, FTP).
  - Time taken to generate complete visibility reports.

2. Policy Enforcement

- **Definition:** Successful implementation of segmentation policies without disrupting business operations.
- **Measurement:**
  - % of workloads transitioned from visibility-only to enforcement mode.
  - Number of policies tested and validated via simulation before enforcement.
  - Policy compliance score during audits.

3. Breach Containment

- **Definition:** Ability to isolate compromised workloads and prevent lateral movement.
- **Measurement:**
  - Average time to isolate a compromised workload (MTTI – Mean Time to Isolation).
  - % reduction in lateral movement risk post-deployment.
  - Number of ransomware containment incidents successfully mitigated.

4. Compliance Readiness

- **Definition:** Alignment with regulatory frameworks and audit requirements.
- **Measurement:**
  - % of workloads encrypted using SecureConnect.
  - Number of compliance reports generated (PCI DSS, GDPR).
  - Audit success rate for segmentation policies.

5. Operational Efficiency

- **Definition:** Non-disruptive deployment and automation at scale.
- **Measurement:**
  - % of workloads deployed using automated methods (Ansible, Terraform).
  - Average deployment time per workload.
  - Reduction in manual intervention during policy updates.

6. Scalability

- **Definition:** Ability to extend segmentation across hybrid environments.
- **Measurement:**
  - Number of workloads supported across on-prem, cloud, and containers.
  - % increase in coverage over time.
  - Integration success rate with SIEM/SOAR platforms.

7. Cost Optimization

- **Definition:** Reduction in operational and infrastructure costs.
- **Measurement:**
  - % reduction in firewall dependency.
  - Estimated cost savings from automation and simplified operations.
  - ROI achieved within defined timeline.

2.4Delivery Organizations

DXC Technology ensures successful delivery of the Micro segmentation service through a **structured governance model** and clearly defined roles across all phases of implementation. The delivery organization includes:

DXC Technology – Lead Partner

- **Role:** Owns end-to-end delivery of the Micro segmentation solution.
- **Responsibilities:**
  - Solution architecture and design.
  - Deployment strategy and execution.
  - Policy definition and operationalization.
  - Integration with existing security ecosystem (SIEM/SOAR, CMDB).
  - Governance, reporting, and compliance documentation.

DXC Security & Cloud Teams

- **Security Architects:** Define Zero Trust segmentation strategy and risk-based policies.
- **Cloud Architects:** Align segmentation with hybrid cloud environments and application dependencies.
- **Operations Team:** Manage deployment, monitoring, and automation at scale.

Customer Organization

- **IS&T Cloud & Compute Support:** Provides infrastructure access and operational alignment.
- **Application Owners:** Validate segmentation policies and ensure application continuity.
- **Security Team:** Collaborates on compliance and incident response integration.

Technology Partner – Illumio

- **Role:** Provides platform expertise and technical support.
- **Responsibilities:**
  - Enable Illumio Adaptive Security Platform (ASP) capabilities.
  - Support DXC during POC and full-scale rollout.
  - Assist with advanced troubleshooting and feature enablement.

Governance Structure

- **Steering Committee:** DXC, and Customer leadership for strategic decisions.
- **Technical Working Group:** DXC architects and customer SMEs for design and implementation.
- **Operational Support Team:** DXC and customer teams for day-to-day management post-deployment.

2.5 Service Constraints

1. Operating System Support

- **Illumio** VEN agents support a wide range of OS versions (Windows, Linux, Solaris, AIX), but **legacy or unsupported OS versions** (e.g., HP-UX, older Solaris releases) may require alternative strategies or remain outside segmentation scope.

2. Network Connectivity

- Managed servers must have **outbound connectivity on TCP port 443** to Illumio SaaS PCE endpoints for policy updates and telemetry.
- Restricted environments or air-gapped systems may require **custom deployment models** or on-prem PCE.

3. Agent Deployment

- VEN installation requires **root/admin privileges** and OS package dependencies.
- Automated deployment (via Ansible, Puppet, SCCM) depends on **customer's existing automation framework readiness**.

4. Integration Dependencies

- Integration with SIEM/SOAR platforms (e.g., Microsoft Sentinel) requires **API access and configuration alignment**.
- CMDB and identity system integration depends on **metadata accuracy and governance maturity**.

5. Policy Enforcement Limitations

- **Initial** enforcement must start in **Visibility Mode** to avoid application disruption.
- Full enforcement depends on **accurate application dependency mapping** and stakeholder validation.

6. Performance Considerations

- Host-based enforcement uses native OS firewalls; performance impact is minimal but must be validated for **high-throughput workloads** during POC.

7. Licensing & Cost

- Licensing is based on **workload type and quantity** (cloud VMs, container hosts, legacy OS).
- Additional costs may apply for **unsupported OS workarounds** or **custom integrations**.

8. Governance & Change Management

- Successful rollout requires **stakeholder alignment** and adherence to DXC's change process.
- Delays may occur if **application owners do not validate segmentation policies promptly**.

3 Value Proposition for UK Public Sector

DXC Technology's Microsegmentation service offers a **strategic security solution tailored for the UK Public Sector**, addressing critical challenges such as compliance, cyber resilience, and operational efficiency in complex hybrid environments.

1. Alignment with UK Government Security Frameworks

- Supports **NCSC Cyber Security Principles** and **Zero Trust Architecture** mandated by UK government guidelines.
- Enables compliance with **UK GDPR**, **PCI DSS**, and **ISO 27001**, ensuring audit-ready segmentation policies.

2. Enhanced Cyber Resilience

- Prevents **lateral movement of threats** across sensitive workloads, reducing the risk of ransomware and advanced persistent threats.
- Provides **real-time visibility** into application traffic, enabling proactive risk management and incident response.

3. Cost-Effective Security Modernization

- Reduces dependency on expensive perimeter firewalls and legacy segmentation methods.
- Offers **host-based enforcement** without network redesign, minimizing infrastructure costs and deployment complexity.

4. Operational Efficiency & Scalability

- DXC delivers **non-disruptive deployment** across on-premises, cloud, and containerized environments.
- Automated policy creation and integration with existing tools (e.g., Microsoft Sentinel, CMDB) streamline operations and reduce administrative overhead.

5. DXC Expertise & Governance

- DXC brings **proven experience in UK public sector engagements**, ensuring secure, compliant, and scalable implementations.

- Provides structured governance, stakeholder alignment, and operational readiness through DXC's **Digital Factory Services** framework.

6. Business Impact

- **Risk Reduction:** Significant decrease in attack surface and lateral movement risk.
- **Compliance Acceleration:** Faster audits and regulatory adherence.
- **Operational Resilience:** Improved uptime and reduced disruption during security incidents.

About DXC Technology

DXC Technology (NYSE: DXC) is a leading global provider of information technology services. We're a trusted operating partner to many of the world's most innovative organizations, building solutions that move industries and companies forward. Our engineering, consulting and technology experts help clients simplify, optimize and modernize their systems and processes, manage their most critical workloads, integrate AI-powered intelligence into their operations, and put security and trust at the forefront. Learn more on dxc.com.

Every day we deliver excellence for our customers and colleagues. We use the power of technology to deliver mission-critical IT services that move the world. Our customers entrust us to deliver what matters most. We are DXC.

An Employer of Choice

We inspire and take care of our people. We work to create a culture of learning, diversity and inclusion for all our people to grow and reach their full potential.

A Trusted Technology Partner

We understand technology and are committed to delivering excellence for our customers.

A Company that Cares

We are committed to improving the communities in which we live and work. We are good stewards of our company, our customers and the world.

Deliver Mission Critical

We deliver the mission-critical IT services that move the world.

Entrusted to Deliver

Every day, we earn our customers' trust by delivering transformative technologies to ensure the success, safety and well-being of businesses and people worldwide.

Delivery Excellence

Our delivery excellence gives planes flight, helps patients heal, and increases the scale and speed of commerce.

Deliver What Matters Most

We are proud of the work we do and the trust and confidence our customers place in us to deliver what matters most.

Learn more at

https://dxc.com/us/en/offerings/security/cyber-defens