GammaSecure

G-Cloud 15: Microsoft Consultancy

Secure, Simplify, Modernise

Gamma

Introduction

Modern organisations face increasing complexity across identity, devices, data, cloud workloads, and compliance.

Our cybersecurity services provide a clear, evidence based understanding of your current security posture and a practical plan to modernise, consolidate, and strengthen your environment using Microsoft 365 E5, Microsoft Entra, Microsoft Purview, Azure Security, and Defender XDR.

Each service delivers leadership ready insights, detailed technical findings, and a prioritised roadmap to help you reduce risk, avoid unnecessary spend, and achieve a secure by default operating model.

Microsoft 365 E5 Security Health Check & Roadmap

GammaSecure

Overview

The Security Health Check & Roadmap to E5 service gives organisations a clear, evidence driven view of their current Microsoft 365 security posture and a practical plan for adopting the advanced protection capabilities available in Microsoft 365 E5. It highlights not only gaps and risks, but also areas where organisations are unintentionally duplicating security tools and spending more than they need to.

What This Service Delivers

1. Comprehensive Security Assessment

- Current-state configuration review across identity, devices,data, threat protection, and compliance
- Best practice alignment analysis to identify misconfigurations and improvement opportunities
- Overlap and duplication detection to uncover where third party tools replicate capabilities already available in Microsoft 365 E5

2. Risk, Exposure & Cost Efficiency Analysis

- Threat aligned risk mapping to show how vulnerabilities relate to real attack paths
- High risk configuration identification to prioritise what matters most
- Redundant control assessment to highlight where multiple tools are solving the same problem (e.g., MFA, DLP, MDM, email security), enabling cost optimisation without compromising protection

Microsoft 365 E5 Security Health Check & Roadmap

GammaSecure

3. E5 Capability Readiness

- Feature-by-feature readiness evaluation for Defender XDR, Purview, Entra ID Premium, and advanced compliance
- Governance and policy evaluation including Azure Policy, Blueprints, and management groups
- Adoption prerequisites including licensing, configuration, and operational considerations

4. Prioritised Roadmap to E5 Review

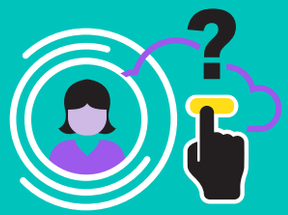
- Quick wins that immediately strengthen security posture
- Consolidation opportunities where E5 can replace or streamline existing third party solutions
- Adoption prerequisites including licensing, configuration, and operational considerations

Executive Summary & Technical Deep Dive

- Leadership ready insights that clearly articulate risk, cost, and business impact
- Technical recommendations with actionable steps for IT and security teams

Ideal for

Organisations preparing to transition to Microsoft 365 E5, seeking to rationalise their security stack, or wanting independent validation of their current security posture and spend



Why Customers Choose This Service

- **Strengthens security posture with targeted, actionable insights**
- **Reduces risk exposure by addressing critical vulnerabilities**
- **Eliminates duplicated tools and identifies opportunities to consolidate overlapping security products**
- **Accelerates E5 adoption with a clear, structured plan**
- **Supports strategic planning with evidence based recommendations**

Azure Core Security Review

GammaSecure

Overview

The Azure Core Security Review provides organisations with a clear, evidence based understanding of their current Azure security posture across identity, networking, compute, storage, and governance. It highlights configuration gaps, misaligned practices, and areas where organisations are unintentionally duplicating security controls—helping reduce risk, eliminate unnecessary spend, and strengthen alignment with Azure's native security capabilities.

What This Service Delivers

1. Comprehensive Azure Security Assessment

- Identity, access, and privilege review covering Entra ID, RBAC, managed identities, and privileged access workflows
- Network security evaluation including NSGs, firewalls, segmentation, and exposure points
- Compute and container hardening analysis across VMs, AKS, and PaaS workloads
- Storage and data protection review focusing on encryption, access paths, and data governance
- Duplication and overlap detection to identify where third party tools replicate Azure-native controls such as firewalls, DDoS protection, SIEM, or vulnerability scanning

2. Risk, Exposure & Cost Efficiency Analysis

- Threat aligned risk mapping to show how misconfigurations relate to real attack vectors
- High risk asset identification including publicly exposed services, weak identity paths, and insecure defaults
- Redundant control assessment to highlight where multiple tools are solving the same problem (e.g., third party firewalls vs Azure Firewall, external SIEM vs Sentinel, external scanners vs Defender or Cloud)

Azure Core Security Review

GammaSecure

3. Azure Security Baseline Alignment & Best Practice Alignment

- Benchmark comparison against Microsoft Cloud Security Benchmark (MCSB) and CIS
- Governance and policy evaluation including Azure Policy, Blueprints, and management groups
- Secure-by-default configuration review to ensure workloads follow Azure-native patterns

4. Prioritised Remediation Plan

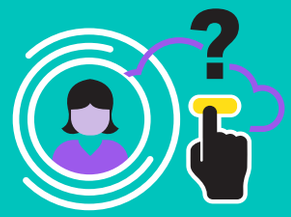
- Quick wins that immediately reduce exposure
- Strategic initiatives to modernise, consolidate, and optimise the security stack
- Medium term improvements aligned to Zero Trust and Azure Well Architected principles
- Effort/impact scoring to support planning, sequencing, and budget decisions

Executive Summary & Technical Deep Dive

- Leadership ready insights that clearly articulate risk, cost, and business impact
- Technical recommendations with actionable steps for cloud, security, and platform teams

Ideal for

Organisations operating workloads in Azure that want to validate their security posture, reduce tool sprawl, or ensure alignment with Azure best practices and Zero Trust principles.



Why Customers Choose This Service

- **Strengthens Azure security posture with targeted, actionable insights**
- **Reduces risk exposure by addressing critical misconfigurations**
- **Eliminates duplicated tools and identifies opportunities to consolidate overlapping security products**
- **Improves operational efficiency by aligning with Azure-native capabilities**
- **Supports strategic planning with clear, evidence based recommendations**

Endpoint Management & Protection Review

GammaSecure

Overview

The Endpoint Management & Protection Review provides organisations with a clear, evidence based understanding of how well their devices are managed, secured, and protected across Windows, macOS, mobile, and virtual endpoints. The service identifies configuration gaps, operational inefficiencies, and areas where organisations are unintentionally duplicating endpoint security tools—helping reduce risk, simplify operations, and optimise licensing spend.

What This Service Delivers

1. Comprehensive Endpoint Management Assessment

- Unified endpoint management review across Intune, Configuration Manager, and co management setups
- Application and update management evaluation to ensure patching, deployment, and lifecycle processes are robust
- Device compliance and configuration analysis to assess alignment with security baselines and Zero Trust principles
- Overlap and duplication detection to uncover where third party tools replicate native Microsoft endpoint capabilities (e.g., AV, MDM, VPN, DLP, encryption)

2. Endpoint Protection & Threat Surface Analysis

- Defender for Endpoint configuration review including onboarding, sensor health, and advanced features
- Threat exposure mapping to identify vulnerable devices, misconfigurations, and weak security controls
- Redundant control assessment to highlight where multiple tools are solving the same problem (e.g., third party AV vs Defender AV, third party MDM vs Intune, external VPN vs Entra ID based access)

Endpoint Management & Protection Review

GammaSecure

3. Policy, Compliance & Governance Review

- Security baseline alignment against Microsoft recommendations and industry frameworks
- Data protection and endpoint DLP review to validate encryption, access controls, and data handling policies
- Conditional Access and device trust evaluation to ensure secure access to corporate resources

4. Prioritised Remediation & Optimisation Plan

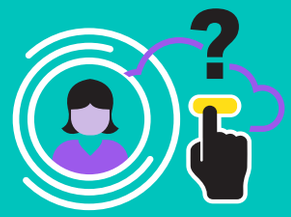
- Quick wins that immediately strengthen endpoint security and reduce operational friction
- Strategic initiatives to consolidate overlapping products and maximise Microsoft 365 value
- Medium term improvements to modernise device management and streamline tooling
- Effort/impact scoring to support planning, sequencing, and budget decisions

Executive Summary & Technical Deep Dive

- Leadership ready insights that clearly articulate risk, cost, and business impact
- Technical recommendations with actionable steps for IT, security, and endpoint operations teams

Ideal for

Organisations operating hybrid or diverse device estates (Windows, macOS, iOS/Android, virtual desktops) that need a consolidated, evidence based view of how well endpoints are managed, secured, and protected and Organisations seeking to optimise Microsoft 365 licensing, reduce spend on redundant endpoint software, or leverage Defender for Endpoint to its full potential



Why Customers Choose This Service

- **Strengthens endpoint security posture with targeted, actionable insights**
- **Reduces risk by addressing critical vulnerabilities and misconfigurations**
- **Eliminates duplicated endpoint tools and identifies opportunities for consolidation**
- **Improves operational efficiency through modern, cloud based management**
- **Supports strategic planning with clear, evidence based recommendations**

Identity Management Review

GammaSecure

Overview

The Identity Management Review provides organisations with a clear, evidence based understanding of how identities, access, and authentication are managed across Microsoft Entra ID and connected systems. The service highlights misconfigurations, operational gaps, and areas where organisations are unintentionally duplicating identity and access controls—helping reduce risk, simplify architecture, and optimise licensing and tooling costs.

What This Service Delivers

1. Identity & Access Assessment

- Identity architecture evaluation across Entra ID, hybrid identity, synchronisation, and federation
- Role and privilege analysis covering RBAC, PIM, service principals, and managed identities
- Authentication and MFA review to validate secure access patterns and identify unnecessary third party MFA or SSO tools
- Duplication and overlap detection to uncover where external IAM tools replicate Entra ID capabilities (e.g., MFA, SSO, conditional access, identity governance)

2. Access Governance & Lifecycle Review

- Joiner Mover Leaver process assessment to ensure identities are created, updated, and removed securely
- Identity governance evaluation including access reviews, entitlement management, and automated workflows
- Group and entitlement management review to identify excessive access, stale permissions, and manual processes

Identity Management Review

GammaSecure

3. Threat, Exposure & Cost Efficiency Analysis

- Identity attack surface mapping to highlight weak authentication paths, legacy protocols, and high risk accounts
- Redundant control assessment to identify where multiple tools provide the same function (e.g., third party SSO vs Entra ID, external identity governance vs Entra ID Governance)
- Conditional Access effectiveness review to ensure policies enforce Zero Trust principles

4. Policy, Compliance & Best Practice Alignment

- Benchmark comparison against Microsoft identity security baselines and Zero Trust identity standards
- Secure-by-default configuration review to ensure modern authentication and least privilege access
- Compliance alignment with regulatory and organisational requirements

5. Prioritised Remediation & Optimisation Plan

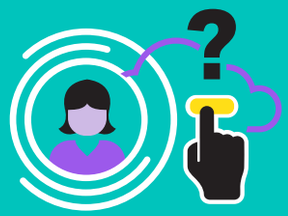
- Quick wins that immediately strengthen identity security
- Strategic initiatives to consolidate overlapping IAM tools and maximise Microsoft Entra value
- Medium term improvements to modernise identity governance and streamline access processes
- Effort/impact scoring to support planning, sequencing, and budget decisions

Executive Summary & Technical Deep Dive

- Leadership ready insights that clearly articulate risk, cost, and business impact
- Technical recommendations with actionable steps for identity, security, and platform teams

Ideal for

Organisations looking to modernise or simplify their identity and access architecture, especially those juggling Entra ID, legacy Active Directory, and third party IAM or MFA tools.



Why Customers Choose This Service

- **Strengthens identity security posture with targeted, actionable insights**
- **Reduces risk by addressing weak authentication paths and excessive privileges**
- **Eliminates duplicated IAM tools and identifies opportunities for consolidation**
- **Improves operational efficiency through modern, automated identity governance**
- **Supports strategic planning with clear, evidence based recommendations**

Data Loss Prevention (DLP) Review

GammaSecure

Overview

The Data Loss Prevention (DLP) Review provides organisations with a clear, evidence based understanding of how sensitive data is identified, protected, and governed across Microsoft 365, endpoints, cloud services, and third party platforms. The service highlights policy gaps, operational blind spots, and areas where organisations are unintentionally duplicating DLP or data protection tools—helping reduce risk, simplify architecture, and optimise licensing and operational spend.

What This Service Delivers

1. DLP Policy & Architecture Assessment

- Current state DLP policy review across Microsoft Purview, Exchange, SharePoint, OneDrive, Teams, and endpoints
- Data classification and labelling evaluation to assess how effectively sensitive information is identified and tagged
- Policy coverage and enforcement analysis to determine whether controls align with regulatory, compliance, and business requirements
- Overlap and duplication detection to uncover where third party DLP, CASB, or endpoint tools replicate capabilities already available in Microsoft Purview

2. Data Flow, Risk & Exposure Analysis

- Data movement mapping to understand how information flows across devices, cloud apps, and external channels
- High risk behaviours and leakage points such as personal email forwarding, unmanaged devices, or unmonitored cloud apps
- Redundant control assessment to highlight where multiple tools are solving the same problem (e.g., third party endpoint DLP vs Purview Endpoint DLP, external CASB vs Defender for Cloud Apps)

Data Loss Prevention (DLP) Review

GammaSecure

3. Governance, Compliance & Best Practice Alignment

- Benchmark comparison against Microsoft recommendations and regulatory frameworks
- Secure by default configuration evaluation to ensure consistent enforcement across workloads and devices
- Policy lifecycle and governance review to assess ownership, change control, and operational processes

4. Prioritised Remediation & Optimisation Plan

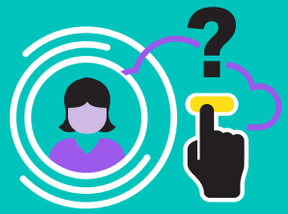
- Quick wins that immediately strengthen data protection posture
- Strategic initiatives to consolidate overlapping DLP and CASB tools and maximise Microsoft Purview value
- Medium term improvements to modernise classification, labelling, and policy enforcement
- Effort/impact scoring to support planning, sequencing, and budget decisions

Executive Summary & Technical Deep Dive

- Leadership ready insights that clearly articulate risk, cost, and business impact
- Technical recommendations with actionable steps for security, compliance, and information governance teams

Ideal for

Organisations preparing to modernise or rationalise their data protection stack, especially those with a mix of Microsoft Purview, legacy DLP, third party CASB, and endpoint tools



Why Customers Choose This Service

- **Strengthens data protection posture with targeted, actionable insights**
- **Reduces risk by addressing high impact data leakage scenarios**
- **Eliminates duplicated DLP and CASB tools and identifies opportunities for consolidation**
- **Improves operational efficiency through unified, modern data protection controls**
- **Supports strategic planning with clear, evidence based recommendations**

Contact

Get in touch with Gamma today to enquire about your G-Cloud 15 service.

Gamma

#GoodTogether

gammagroup.co

CERTIFIED CARBON NEUTRAL® paper

CarbonNeutral.com

We're a certified Carbon Neutral* Company. This means you can demonstrate green credentials yourself. By working with us you have a solution that not only helps the environment but also enables you to become greener and conform to new Government environmental policies.