

Increase Visibility and Simplify your Security

WE'VE GOT YOUR BACK.

LAB³ Security Fusion

Workplace, Cloud and Hybrid Security working together on one homogenous platform.

Builds on standard Microsoft products to aggregate your tools onto a single platform to both consolidate the views and provide a live view of your security posture. Rules are defined to extend between security toolsets to ensure complete coverage, visibility, and enforcement.

Suitable to meet the compliance requirements of highly regulated industries, while retaining flexibility so security is not a roadblock but integrated into all organisation solutions.

Member of
Microsoft Intelligent Security Association

Homogenous Security
Integration of Security tools to work as a single platform reducing exposure and gaps. Optimising active and passive defence configurations.

Swift Integration
Leverage automation and pre-defined architectures to accelerate your adoption and coverage. Aligned to the ISM for highly regulated customers.

Cost Optimisation with E5
Utilise all entitled security services under your Microsoft E5 license for greater cost and operational efficiencies.



"I am pleased to have LAB³ join us as a partner in the Microsoft Intelligent Security Association (MISA). By including our strategy Managed Security Services Providers (MSSPs) in MISA, we help enable further collaboration between cybersecurity industry leaders in protecting and supporting our joint customers."

- Mandana Javaheri, Director of Business Strategy, Microsoft Security Partner Development

What does LAB³ do differently?

Data Locality
Australia owned and managed.
Data remains in your organisation's tenancy. You remain in control.

Automation First
Scalable deployments Powered by Code.
Operational response efficiencies with automated policies.

Enterprise Grade
Template architectures for Federal/State Governments, and Highly Regulated Industries.
Accelerate deployments with tried and tested policies.

Single Platform
Extended integration between all Microsoft Security services.
Reducing gaps and aligning policies across the platform.

ISM Compliant
Extend compliance requirements above the Microsoft standard aligning to Information Security Manual by Australian Signals Directorate.

Did you know on average we identify critical security incidents within 12 hours?

Speak with our team to find out how we can provide a free Organisational OSINT Report today.

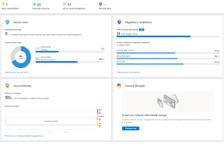
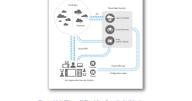
LAB³ Security Fusion

Cloud, Workplace, Hybrid



MODERN THREAT PROTECTION
COMBINING AI AND INDUSTRY EXPERTISE

LAB³ Security Fusion (Adv. Active/Passive Defence)

<p>Azure Security Center</p> <p>Azure Security Center is a cloud security service that provides visibility of Azure and on-premise workloads. Security Center is offered as two tiers:</p> <ul style="list-style-type: none"> Cloud Security Posture Management (CSPM): Security Center is available for free to all Azure users. The free experience includes CSPM features such as secure score, detection of security misconfigurations, cloud configuration, and cloud benchmarks. Cloud workload protection (CWP): Security Center integrated cloud workload protection platform (CWP) brings advanced, managed protection for Azure and hybrid resources.  <p>Figure 1-1 - Azure Security Center Dashboard</p>	<p>Defender for 365</p> <p>4.1 Overview</p> <p>Microsoft Defender for Office 365 integrates your organization against malicious threats posed by email messages, links, URLs, and collaboration tools. Policies can be configured for each protection feature that supports the features and processes search defined below.</p> <p>4.2 Architecture</p> <p>The architecture components can be described as follows:</p> <ul style="list-style-type: none"> Safe Attachments: Provides on-the-fly protection to safeguard your messaging systems by checking attachments for malicious content. It checks all messages and attachments that are sent from a communication endpoint to a safe environment, and then sends messages and attachments back to the recipient's mailbox. It is available for Exchange Online, Exchange on-premises, and Exchange Hybrid. Safe Links: Provides on-the-fly protection for all links in your organization's email messages and Office files. It checks links for malicious content and provides real-time updates on link safety. Safe Search: Provides on-the-fly protection for all search results in your organization's email messages and Office files. It checks search results for malicious content and provides real-time updates on search results. Anti-phishing protection: Detects attempts to impersonate your users and obtain or control accounts. It helps resolve security incidents and advanced threat protection (ATP) capabilities to help prevent attacks. To learn more, see Configure anti-phishing policies in Microsoft Defender for Office 365.  <p>Figure 2-1 - Defender for 365 Architecture</p>	<p>Framework</p> <p>Azure Information Protection (AIP) is a cloud-based solution that enables organizations to protect sensitive information by identifying and classifying unstructured and structured data. This is done using an intelligent natural classification technology, made up of rules and machine learning.</p> <p>Labels can be applied:</p> <ul style="list-style-type: none"> Automatically by administrators using rules and conditions Manually by users By a combination of rules and administrators before the recommendations about to users <p>These labels can both identify and automatically protect documents, enabling organizations to:</p> <ul style="list-style-type: none"> Track and control how content is used Prevent users from copying content into the business. Content may be blocked and user restricted Track document access and prevent data leakage or abuse  <p>Figure 3 - AIP Information Protection Framework</p> <p>Mapping these Microsoft products to existing Australian Information Protection framework is reflected in Figure 3 below.</p>	<p>Microsoft Defender for Endpoint</p> <p>5.1 Overview</p> <p>Microsoft Defender for Endpoint (DfE) is an enterprise endpoint security platform designed to help enterprise resources prevent, detect, investigate, and respond to advanced threats.</p> <p>5.2 Architecture</p> <p>Defender for Endpoint is composed of the following components:</p> <ul style="list-style-type: none"> Defender for Endpoint Telemetry: A DfE agent is provisioned for each customer and is installed from every user device. Each agent has the best behavioral capabilities of cloud telemetry, including telemetry, behavioral data, and the ability to securely identify sensitive data to detect suspicious activity related events in the sensor data. Defender Security Center: Security Fusion uses the Defender Security Center to access their DfE data to integrate with existing, central investigations, response, breach, or threat hunt. SIEM Solution: The central SIEM solution ingests and correlates security-related events and data from sensors to customer's SIEM. Security Fusion can trigger integrations to perform action on responses such as collecting evidence, investigate, and hunt using or sending requests from sensors.  <p>Figure 3-1 - Defender for Endpoint Architecture</p>	<p>Defender for Identity (DFI)</p> <p>Microsoft Defender for Identity is a cloud-based security solution for on-premises Active Directory (AD) environments. These agents collect network traffic, such as Kerberos tickets, and other data and compare it with AD. Microsoft Defender for Identity uses machine learning, behavioral analytics, and other techniques to detect suspicious activity, such as anomalous logon attempts, password resets, and other events.</p> <p>4.1 Architecture</p> <p>The following diagram illustrates the architecture for Defender for Identity. The primary components are:</p> <ul style="list-style-type: none"> Sensors: A Microsoft service that runs on either a domain controller or AD FS server. It will send AD traffic, network traffic, and other data to the cloud for analysis. Defender for Identity: The central service that runs in the cloud. It will receive data from the sensors and analyze it for suspicious activity. SIEM Solution: The central SIEM solution ingests and correlates security-related events and data from sensors to customer's SIEM. Security Fusion can trigger integrations to perform action on responses such as collecting evidence, investigate, and hunt using or sending requests from sensors.  <p>Figure 4-1 - Defender for Identity Architecture</p>	<p>Microsoft Cloud App Security</p> <p>Microsoft Cloud App Security (MCAS) provides comprehensive visibility into cloud application activities. It provides services to help control cloud risk, assess risk, enforce policies, manage access, and stop abuse. MCAS is the primary tool to monitor and control your cloud applications and third-party resources. It can, when you want, be linked and integrated with the data you are using to monitor your cloud applications.</p> <p>4.1 Architecture</p> <p>The primary components can be described as follows:</p> <ul style="list-style-type: none"> MCAS Agent: Provides comprehensive visibility and insight for security analysis in monitor and protect cloud apps. All configurations are done through the MCAS portal. Cloud Security Posture Management (CSPM): CSPM features can be manually updated in MCAS to discover and remediate misconfigurations. Cloud Security Scan (CSS): CSS features can be manually updated in MCAS to discover and remediate misconfigurations. Application Discovery: Application Discovery can scan your cloud environment. You can be notified as misconfigurations are discovered. Microsoft Scan uses SaaS-based and on-premise agents to collect data on applications in your cloud environment. To learn more, see Application Discovery in Microsoft Cloud App Security. Microsoft Cloud App Security (MCAS): MCAS can be integrated with Azure Sentinel for log event data for user activity, alerts, and other data. Azure Sentinel: SIEM can be directly integrated with Azure Sentinel for log event data for user activity, alerts, and other data.  <p>Figure 4-1 - Microsoft Cloud App Security Architecture</p>
<p>Infra</p>	<p>Corp. Apps</p>	<p>Data</p>	<p>Endpoints</p>	<p>Identity</p>	<p>Cloud Apps</p>



Our Security Approach

1	2	3	4
<p>AUDIT</p> <p>Discovery of Client's environment and Re-affirm attack vector weaknesses in the people, process and technology.</p>	<p>PLATFORM</p> <p>Uplift to a Defence in Depth Architecture. Deploying multiple layers of security controls providing redundancy and protection.</p>	<p>UPLIFT</p> <p>Onboarding and fine tuning of Active and Passive Defence security services</p>	<p>VISIBILITY</p> <p>Consolidation of security data providing Intelligence into security posture and providing User and Entity Behavior Analytics</p>

Service Elements

SIEM Capabilities delivered from the Azure Cloud	No additional software or hardware to deploy	Support for on-premises log sources (>30 log parsers available)	Security Monitoring of Cloud services (Azure, AWS, Google)	Access to Managed Sentinel Alert Rules Service Catalogue	Performance and availability monitoring and notification	Online access to Alert Knowledge Base
Compliance aware monitoring	Continuous alerts and playbooks tuning and optimization	24x7 Incident Detection and Response	Powered by Automation leveraging SOAR library	Cloud costs alerting & reporting	Incident Attribution with Threat intelligence service integration	Monthly service review

*Azure Sentinel SIEM runs in client's Azure subscription *Service is priced based on the number and type of log sources

Get In touch to see if this solutions is right for your business.
hello@lab3.com.au