

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 / New Zealand owned and operated.

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.

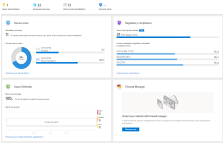
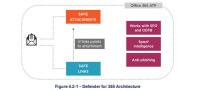

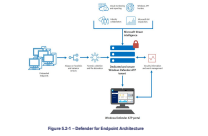
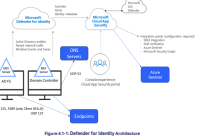

LAB³ Security Fusion

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 4.1 - 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 attachments from external sources. Policies can be configured for each protection feature that determine the detection and prevention search and detection rules.</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 in a specific environment, and then sends machine learning and analysis feedback to Microsoft Defender for Office 365 to determine safety. It checks the message forwarded to the mailbox. To learn more, see Safe Attachments. Safe Links: Provides link-level protection for Office 365. It examines links in emails, messages, and OneDrive files. It checks the link for malicious content and provides real-time updates on link safety. To learn more, see Safe Links. Safe Search: Provides search-level protection for Office 365. It checks search results for malicious content and provides real-time updates on search results. To learn more, see Safe Search. Anti-phishing protection: Detects attempts to impersonate your users and obtain or control accounts. To learn more, see Configure anti-phishing protection in Microsoft Defender for Office 365.  <p>Figure 4.3 - 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 detecting and classifying unencrypted documents and emails. This is done using an intelligent natural classification learning model on all data and metadata.</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 2 - AIP Information Protection Framework</p> <p>Mapping these Microsoft products to existing Australian Information Protection framework is reflected on 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 client is provisioned for each customer and is installed from every device. Each client has the best behavioral capabilities of cloud telemetry, including telemetry, behavioral data, and the ability to securely connect to the cloud. It sends data to the cloud. Defender for Endpoint Security: This tool uses the Defender Security Center to scan the DfE client for malware and suspicious activity, and investigate suspicious activity. It also scans for malware and suspicious activity on the cloud. Defender for Endpoint Protection: This tool uses the Defender Security Center to scan the DfE client for malware and suspicious activity, and investigate suspicious activity. It also scans for malware and suspicious activity on the cloud.  <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-premise Active Directory 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 to detect suspicious activity, such as anomalous logon attempts, password resets, and other suspicious activity. It also provides real-time alerts and investigation capabilities.</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"> Security: A Microsoft service that runs on either a domain controller or AD FS server. It will send AD traffic, network traffic, and other events and data back to the DfE cloud service. Defender for Identity: The cloud service that runs on the Microsoft Defender for Identity cloud service. It receives data from the on-premise agents and processes it to detect suspicious activity. Defender for Identity Protection: This tool uses the Defender Security Center to scan the DfE client for malware and suspicious activity, and investigate suspicious activity. It also scans for malware and suspicious activity on the cloud.  <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 a central hub to help control cloud risk, assess risk, enforce policies, manage alerts, and stop abuse. MCAS is the primary tool to monitor and control your cloud environment and help you understand your cloud environment. To learn more, see Microsoft Cloud App Security.</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 is a cloud-based security solution that provides visibility into cloud application activities. It provides a central hub to help control cloud risk, assess risk, enforce policies, manage alerts, and stop abuse. MCAS is the primary tool to monitor and control your cloud environment and help you understand your cloud environment. To learn more, see Microsoft Cloud App Security. Cloud Security Posture Management (CSPM): CSPM is a cloud-based security solution that provides visibility into cloud application activities. It provides a central hub to help control cloud risk, assess risk, enforce policies, manage alerts, and stop abuse. MCAS is the primary tool to monitor and control your cloud environment and help you understand your cloud environment. To learn more, see Microsoft Cloud App Security.  <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



<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

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

*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