Managed Secure Infrastructure Service

A constantly evolving security threat landscape, increased pressure around compliance and the potentially devastating impact of a security breach means that businesses don’t just rely on IT, they demand secure IT. Information security breaches can severely impact business and damage brand reputation if made public – in some countries, non-IT executives may even be held personally liable. Moreover, the drive towards a more mobile workforce has rendered management of the traditional corporate perimeter, an increasingly complex endeavour.

A robust security infrastructure is essential to protect any business. As new security threats continue to arise and evolve, an active strategy is a necessity for any business that wants to remain secure. To be truly effective, your organisation’s security posture must be constantly monitored and well maintained. This requires significant time, effort and access to specialised expertise that you may not have in-house. What’s more, focusing your internal team’s energies on security means they will have less time to execute on strategic business requirements which in turn can lead to loss of revenue and competitive advantage.

Dimension Data’s Managed Secure Infrastructure Service

If your business is seeking a better way to strengthen security, reduce complexity, manage compliance and navigate regulatory challenges, Dimension Data’s Managed Secure Infrastructure Service may be what you’re looking for.

The service provides:

- A platform for the operational management of IT and security assets
- World-class security operations technology, processes and services to continuously monitor your security assets and to provide in-depth analysis of security events
- Consistent application of industry best practices and standards such as IT Infrastructure Library (ITIL), National Institute of Standards and Technology (NIST), ISO27001 and documented manufacturer guidelines
- Access to a range of services that highlight infrastructure deficiencies, suggest remedial actions and report on a wide range of infrastructure and security activities
- Skilled resources to augment your existing in-house security capability or provide a complete, outsourced operations management capability

Delivery of this service is based upon core elements of Dimension Data’s Operational Support and Management infrastructure, including:

- A setup and on-boarding process to stabilise, assess and manage your security assets
- An online service portal and service desk which are used to communicate with the management service team
- Service management and reporting functions that can provide continuous review and assessment of the effectiveness of your security posture

The service offering consists of the following four modules, each designed to address specific security infrastructure management needs:

- **Operations Management** which delivers day-to-day operations management tasks on security configuration items, based on industry best practices
- **Performance and Availability Monitoring** which provides notifications and statistics on configuration item health to assist in capacity and architecture planning activities
- **Compliance Management** which delivers continuous service improvement functions, such as configuration optimisation against industry best practices like ISO27001
• **Security Information and Event Management** which delivers a range of options to help you deal with security log data management and security incident management. These service elements also monitor access activity and collect and store logs for compliance purposes.

**The benefit to you**

By opting for our service you can look forward to:

• **Better risk management**: The ability to measure risk, report on risk posture, respond to audit requirements and substantiate a best effort approach to security

• **Enhanced cost control**: You can eliminate the cost of hiring, training, managing and retaining high quality security engineering personnel

• **Improved agility**: Your team is free to focus on core business outcomes and requirements while information security requirements are being taken care of under a service level agreement driven service

• **Increased compliance**: You can measure your risk profile against best practice standards, on an on-going basis. It helps ensure compliance and improves responsiveness to audit requirements

**Service Structure**

**Service Calendars**

The Managed Secure Infrastructure Service is modular, scalable and flexible to suit your individual requirements. It is available in the following service calendar options:

<table>
<thead>
<tr>
<th>Service Element</th>
<th>8x5</th>
<th>24x7</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations Management</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Performance, Availability Monitoring</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Compliance Management</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Security Information and Event Management Level 1</strong></td>
<td>NA</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Security Information and Event Management Level 2</strong></td>
<td>NA</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Service Elements and Service Level Agreement Options**

**Service Readiness Review**

**Operations Management**

- Asset and Configuration Management
  - Configuration and Rule-base Backup
  - Operating Platform Backup
  - Proactive Patch Release Notification
  - Asset Inventory Management
  - Intrusion Prevention System (IPS) Policy Tuning

- Release Management
  - Configuration and Rule-base Restore
  - Operating Platform Restore
  - Patch Installations
  - Signature Update Maintenance

**Incident Assessment**

- Remote Incident Diagnosis and Troubleshooting
- Workaround / Permanent Resolution Identification

**Change Requests**

- Configuration and Rule-base Administration
- Change Request Process

**Role-based Access Control**

**Operations Management Service Reporting**

- Change and Release Reports
- Asset Inventory Reports
- Operations Management Ad Hoc Reports

**Performance and Availability Monitoring**

**Event Management**

- Performance and Availability Monitoring and Notification

**Performance and Availability Monitoring Service Reporting**

- Performance and Availability Reports

**Compliance Management**

**Security Compliance Management**

- Change Compliance Assessment
- Standards and Control Management
- Rule-base Optimisation Analysis
- Non-Compliance Alerting and Notification

**Compliance and Assurance Management Service Reporting**

- Standards Compliance Reports
- Complex Log Analysis Reports

**Security Information and Event Management (SIEM) module**

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2 (Option)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Management</td>
<td>✓</td>
</tr>
<tr>
<td>Log Collection and Storage</td>
<td>✓</td>
</tr>
<tr>
<td>Security Incident Handling</td>
<td>✓</td>
</tr>
<tr>
<td>Security Alert Notification</td>
<td>✓</td>
</tr>
<tr>
<td>Remote Security Incident Analysis and Response</td>
<td>✓</td>
</tr>
<tr>
<td>SIEM Service Reporting</td>
<td>✓</td>
</tr>
<tr>
<td>Log management reports</td>
<td>✓</td>
</tr>
<tr>
<td>Security analysis report</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Core Service Elements**

- Request Fulfilment
- Incident Management
- MACD Service Units
- Escalation Management
- Service Management

- Client services manager
- Service review meetings
- Service management reporting

- Service Portal
- Service Desk
- Service Activation and Establishment
Managed Secure Infrastructure Service

**Supported Configuration Items:**
- Check Point Firewall-1 / VPN-1 Appliance
- Cisco PIX / FWSM / ASA
- Fortinet Fortigate
- Cisco IOS Router & Switch ACLs*
- McAfee IPS (Intrushield)
- Blue Coat SG Web Proxy*
- Ironport WSA (Web Security Appliances)*

**Service Elements**

**Service Readiness Review**
Prior to implementing this service, a Dimension Data engineer will perform a Service Readiness Review. The readiness review will include an analysis of your configuration items and infrastructure architecture to ensure the managed configuration items can be supported by the service.

**Operations Management**
Operations Management focuses on delivering day-to-day support and maintenance tasks required to operate your security infrastructure. This is performed within the guidelines set by security best practice to ensure that your security infrastructure continues to operate efficiently and effectively.

Key features include:
- Asset and Configuration Management – assists you with creating, populating, updating, managing and maintaining the configuration of configuration items and rule-bases.
  Service elements include:
  - Configuration and Rule-base Backup
  - Operating Platform Backup
  - Proactive Patch Release Notification
  - Asset Inventory Management
  - Intrusion Prevention System Policy Tuning
- Release Management – provides the ability to identify, review, plan and implement patches, configurations and rule-base changes on supported configuration items.
  Service elements include:
  - Configuration and Rule-base Restore
  - Operating Platform Restore
  - Patch Installations
  - Signature Update Maintenance
- Incident Assessment – assists you to manage unexpected operational incidents with the primary objective of returning service as quickly as possible.
  Service elements include:
  - Remote Incident Diagnosis and Troubleshooting
  - Workaround / Permanent Resolution Identification
- Change Requests – process assists you to ensure changes to your IT environment are managed properly, appropriate parties are notified of the pending changes, applicable approvals are given to proceed with the changes and the proper parties test the change.
  Service elements include:
  - Configuration and Rule-base Administration
  - Change Request Process
- Role-based Access Control – Dimension Data applies security access controls to:
  - Authorised end user accounts on the Service Portal.
  - Authorised access accounts on configuration items.
  Service elements include:
  - Operations Management Service Reporting – provides the analysis and reporting of technical infrastructure management process and exposes weaknesses that allow management to take corrective action or to improve process where required.
  Service elements include:
  - Change and Release Reports
  - Asset Inventory Reports
  - Operations Management
  - Ad Hoc Reports

**Performance and Availability Monitoring**
Performance and Availability Monitoring focuses on assessment and reporting of security infrastructure health, capacity and performance. These functions are necessary to ensure optimal operation of the infrastructure that supports the implementation of security controls in an organisation.

Key features include:
- Event Management – ensures that events on supported configuration items are detected, analysed, communicated and swiftly channelled to the Incident Management process if required.
  Service elements include
  - Performance and Availability Monitoring and Notification
- Performance and Availability Monitoring Service Reporting – provides you with the ability to understand current and future business and IT needs relating to configuration item availability and performance.
  Service elements include:
  - Performance and Availability Reports

**Compliance Management**
Compliance Management focuses on delivering quality security best practice through analysis, measurement, comparison, reporting and remedial recommendations on security infrastructure. Continuous service improvement is an iterative process and requires accurate measurement and reporting throughout the infrastructure management process.

Key features include:
- Security Compliance Management – ensures that the required discipline is applied to technical infrastructure management for continued alignment to IT policy.

As new security threats continue to arise and evolve, an **active strategy** is a necessity for any business that wants to remain secure. To be **truly effective**, your organisation’s security posture must be **constantly monitored** and well maintained.

*Firewall rule-base analysis and optimisation is not available on these devices*
Service elements include:
- Change Compliance Assessment
- Standards and Control Management
- Rule-base Optimisation Analysis
- Non-Compliance Alerting and Notification

- Compliance Management Service Reporting – assists in providing timely response to requests by audit departments through continuous measurement and reporting against known industry best practice.

Service elements include:
- Standards Compliance Reports
- Optimisation Analysis Reports

### Security Information and Event Management

Security Information and Event Management can support you with managing the volume of security event information and in addition, assist with meeting operational requirements and compliance mandates to respond effectively to security incidents.

This module is available at two levels:

- **Level 1** – Provided by default when the module is selected, this level provides logging and logging functions.
- **Level 2** – Available as an option for an additional charge, this level extends the logging and reporting functions and provides analysis and response to security incidents.

**Key features include:**
- Log Management – is the collection and aggregation of raw log data into a centralised storage repository. The solution provides manageable security event information that you can use for historic forensic analysis or incident investigation. Log Management is the starting point to controlling the increasing volume of security events and provides you with a platform, a collection strategy and a support structure to successfully collect and store security log data.

Service elements include:
- Log Collection and Storage

### Security Alert Notification (Level 1 & Level 2)

<table>
<thead>
<tr>
<th>Event Priority Level</th>
<th>Initial Client Notification**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30 Minutes</td>
</tr>
<tr>
<td>2</td>
<td>60 minutes</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Time for the initial notification parameter is measured from when the relevant event is detected by the Dimension Data management system.

### Remote Security Incident Analysis and Response (Level 2)

<table>
<thead>
<tr>
<th>Incident Priority Level</th>
<th>Diagnosis Notification To The Client**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>60 Minutes</td>
</tr>
<tr>
<td>2</td>
<td>180 minutes</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Time for the diagnosis notification parameter is measured from when the relevant event is detected by the Dimension Data management system.

### Log Collection and Storage

Retention Period: 3 months online log data, 3-12 months offline log data

### Security Incident Handling – is the function of aggregating and correlating the large amount of logged data with the purpose of identifying potential risk. Potential risks are highlighted by generating alerts that can then initiate incident investigations.

Service elements include:
- Security Alert Notification
- Remote Security Incident Analysis and Response (Level 2)

### Security Information and Event Management Service Reporting – can provide you with historical analyses of security event data and security threat statistics. These reports will provide awareness of the risks presented by security threats and assist you to plan proactive security controls to support your business requirements.

Service elements include:
- Log Management Reports
- Security Analysis Reports (Level 2)

### Request Fulfilment

The Request Fulfilment service enables you to request and receive services for which a pre-defined approval and qualification process exists.

**Key features include:**
- Request Fulfilment Process – for dealing with common or recurring configuration item related requests including queries and everyday tasks such as Service Portal password resets.

### Incident Management

Incident Management ensures the service is operating effectively and that identified incidents are resolved in a timely manner.

**Key features include:**
- Incident Management Process – A Dimension Data support engineer reviews all events detected by the Dimension Data management system and records those diagnosed as being a valid incident. Incidents received are recorded and channelled through the Incident Assessment service.
MACD Service Units
Change requests are administered through a MACD service unit system, where MACD service units are purchased up-front and then deducted in the execution of the change requests. The number of MACD service units deducted per change request is based on a predefined list of standard tasks as well as the urgency, hours-of-execution and engineering skill required for the task.
Refer to the MSIS MACD Service Unit Usage Table available upon request.

Escalation Management
Escalation Management ensures that, should a problem occur as part of an incident, change or problem, a set of procedures takes effect to ensure swift resolution of the issue.
Key features include:
• Escalation Management Process - Dimension Data considers the escalation management process critical to the effective delivery of Managed Services. Dimension Data has implemented strict escalation processes and clearly defined responsibilities for actioning escalated matters.

Service Management (Optional)
As an option, Dimension Data can provide a Client Services Manager who will run any Service Review Meetings and processes necessary to define, agree, report on and manage the service. Depending on the complexity of your environment and the number of devices under management, Dimension Data may deem that the supply of the Service Management option be compulsory.
Key features include:
• Client Services Manager – can be assigned to own the total delivery relationship between you and Dimension Data with a focus on ensuring a consistently high level of client satisfaction.
• Service Review Meetings – is a forum chaired by the Client Services Manager for you and Dimension Data to discuss various aspects of the service.
• Service Management Reporting – The Client Services Manager will provide a monthly Service Management Report for discussion at the Service Review Meeting.

Service Portal
The Service Portal provides both IT management and technical support staff access to information relating to the Managed Secure Infrastructure Service, 24 hours a day, 7 days a week.

Why Dimension Data?
There are hundreds of security services providers in the marketplace. Only a few can rival Dimension Data’s depth of skills, global presence and relationships with key security vendors. Furthermore, we differentiate through our field experience and technical competence; pre-release access to new technology releases and features; breadth of skills and solutions and neutrality within our chosen vendor set (which includes Check Point, Blue Coat, Fortinet, McAfee, RSA and Cisco.)
Managed Secure Infrastructure Service

Our Approach
Dimension Data adopts a lifecycle approach to manage security environments: from assessment through planning, architecture, technology implementation to on-going management.

- In the **Assessment** phase, we assist your organisation to identify risk within different parts of their IT environment.
- In the **Planning** phase, we work with you to develop a plan to address their areas of risks that were uncovered or explored in the Assessment phase.
- In the **Architecture** phase, we complete – if necessary – a redesign of the security infrastructure to optimally support the organisation’s security objectives.
- In the **Solutions** phase, we deploy the most suitable security technologies to meet your organisation’s current and future security needs.
- In the **Management** phase, we provide ongoing maintenance and management for the deployed technologies to assist you in determining whether to outsource the management of some, or all components of your security environment.

As a first step in gaining a better understanding of the current environment, pinpoint specific focus areas and identify urgent gaps or weaknesses in existing security infrastructure we can start with a consulting engagement, for example, a Governance, Risk and Compliance Assessment or a Vulnerability Assessment, amongst others.

For more information, please contact your nearest Dimension Data office or visit [http://www.dimensiondata.com](http://www.dimensiondata.com).


Why Dimension Data?
- Dimension Data’s security experts have been designing, deploying, integrating and supporting technology and IT risk management solutions across the world for over 20 years. By engaging with Dimension Data’s Security Solutions team, you can draw upon the skills of over 500 certified security solution experts.
- Dimension Data delivers services consistently across the world. This is achieved through the Global Services Operating Architecture – our service delivery platform for monitoring and support, information sharing and flexible reporting. The platform’s capabilities allow us to roll out new features, as requested by clients and services teams, in a short time-frame.
- Deep technical and integration expertise across a variety of IT disciplines, including – networking, security, unified communications and collaboration, data centres, virtualisation, Microsoft and contact centres.
- Strategic alliance partnerships with leading security technology vendors, including McAfee, Cisco, Blue Coat, RSA, Fortinet and Check Point.
- Over 6,000 clients across all industry sectors, including financial services, telecommunications, healthcare, manufacturing, government and education.
- Over 14,000 employees with operations in 51 countries across five continents.
- Dimension Data manages more than $12.5 billion of network infrastructure through five Global Service Centres, on a 24x7 basis, in more than 15 languages.