



Solution Brief



2012

## D-Man Distributed monitoring for Federated e-business environments

SecurIT D-Man is a light-weight, open-standards based monitoring system that is focussed on highly-distributed environments. It has been designed from the bottom up to integrate smoothly in e-Business applications that span across internet boundaries.

This Product Description describes why SecurIT D-Man is probably the best product on the market to monitor large, complex e-Business environments. While it is not absolutely required to be familiar with SecurIT D-Man to fully grasp the value of the product in this context, it might help to first read the generic SecurIT D-Man Product Description. The following paragraph will however set the scene.

## About SecurIT D-Man Distributed Monitoring

Traditional monitoring systems don't fit very well e-Business environments. Because they were initially designed to monitor internal processes and applications mainly from a technical point of view, they don't pay too much attention to infrastructural security and the user's perspective.

The first aspect is reflected by the heavy frameworks on which many of these systems rely. These frameworks tend to use protocols that are not supported within a Demilitarized Zone (DMZ) or across firewalls.

The latter aspect might result in e-Business environments of which the isolated tiers are in perfect health, but where the service as a whole does not behave as expected.

SecurIT has designed and built a monitoring solution for Distributed e-Business Environments, from the ground up, with exactly these aspects in mind. It addresses both, helping IT-Administrators isolating and solving IT problems appropriately as well as end-to-end Monitoring of business applications to identify service outage before it effects end-users.

This solution was released by SecurIT under the name SecurIT D-Man in 2004. The D-Man monitoring framework consists of two main components:

- D-Man Application Manager (DAM)
- D-Man Data Manager (DDM)

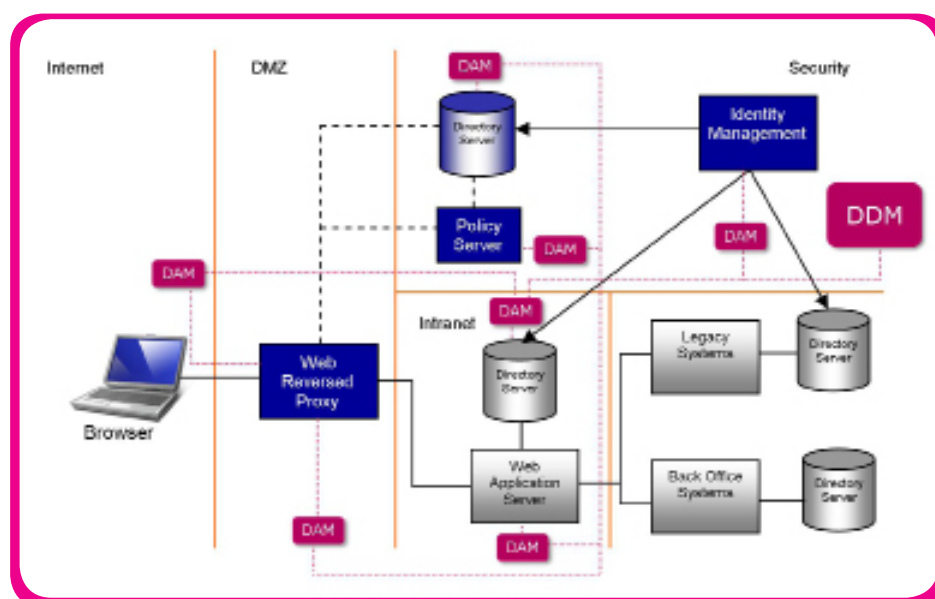
The **D-Man Application Manager (DAM)** represents a traditional monitoring agent. It is used to gather information from any component in the infrastructure that needs to be monitored. Typically there will be one DAM residing on every single server in the e-Business environment. A DAM is responsible for monitoring any activity that is relevant to the server on which it resides. This could be local as well as remote activity.

The following example illustrates some aspects of an e-Business environment that can be monitored by a DAM residing on a server within the DMZ:

- Availability of the process running a Secure Reverse Proxy
- Response time of a remote Directory Server (e.g. LDAP) when validating a username/password authentication by the Secure Reverse Proxy
- Resource consumption of a Web Application Server

The **D-Man Data Manager (DDM)** sits at the core of the D-Man monitoring framework. On one site it is used for the administration of the D-Man environment while on the other site it is responsible for collecting and analyzing the data that is gathered by all DAMs in the infrastructure.

Please refer to the "[SecurIT D-Man. Distributed monitoring for e-Business environments](#)" Product Description for additional information on the Core D-Man Infrastructure.



## Solution Brief

## SecurIT D-Man Scalability

In isolated or small environments, it is usually sufficient to have a single DDM to control the SecurIT D-Man system. In case there would be a requirement for high-availability of the monitoring solution as well, a second DDM could be configured for redundancy.

In federated environments, it is however recommended to split the environment in more manageable domains. This can be handled by creating a hierarchy of DDMs. This model, and its advantages, is described in more detail further on in this document.

### How it works

The model for deploying SecurIT D-Man in large distributed environments is best illustrated by an example. Consider an international or multi-national organisation with three locations: headquarters (HQ) in Brussels, affiliates in New York and Tokyo. The organisation operates an international e-Business service which is hosted in all its affiliates. While each affiliate is responsible for managing its own IT infrastructure, HQ in Brussels wishes to be informed about the overall availability and serviceability of the system.

Each location (Brussels, New York and Tokyo) hosts its own SecurIT D-Man system. This system operates in stand-alone mode and fully monitors the local e-Business environment. The system contains its own administration and configuration module and can be controlled from a local browser. At each location SecurIT D-Man is able to integrate with local reporting systems, like TEC or HP Openview. This can be achieved using SNMP or any other published interface.

The only thing that is different from a normal SecurIT D-Man configuration is that at each location, there is also a link to a SecurIT D-Man system that is located

in Brussels. This latter system, called DCM, is not a standard configuration, but operates at a Meta level. This SecurIT D-Man Meta system uses exactly the same technology and components as the DDM. In other words, only its configuration is different.

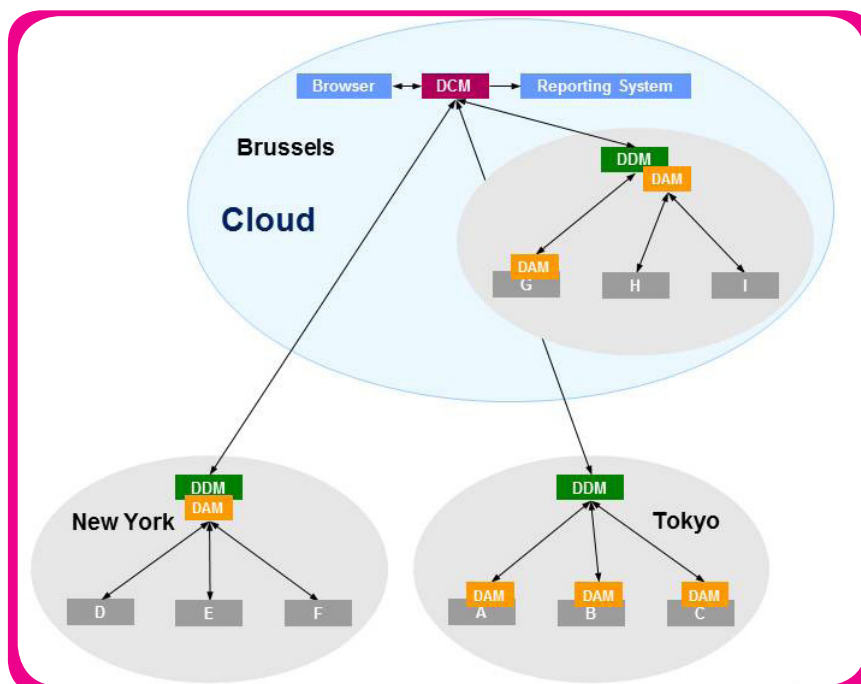
The SecurIT D-Man Meta system is able to extract on a regular basis event information from the SecurIT D-Man systems at the different affiliates. The mechanism used to extract this information is exactly the same as the one used to extract event information from the DAMs. The connection is established from the DCM, it runs over HTTPS and uses mutual authentication to validate the identity of the peers. Because each DDM has a local event database, occasional failures of the connections (which might run over the public internet) between the DDMs, will not harm the system.

Being a standard SecurIT D-Man system, the DCM provides its own administration and configuration module and can be controlled from a local browser. Furthermore it is able to consolidate and correlate the events it gets from the remote systems and send them to a local reporting system, exactly the same as a normal DDM will do.

In very large environments, it is possible to make the SecurIT D-Man hierarchy even deeper. In such a configuration there can be several Meta levels. Another reason for creating more levels could also be to perform more interim correlations or to spread the correlation load over different systems. Meta DDMs can also be used for redundancy reasons and as backup systems.

## Cloud Monitoring

D-Man monitoring in and from the Cloud uses a D-Man Cloud Manager (DCM). The DCM provides a



## Solution Brief

centralized way of monitoring multiple local D-Man environments. These could be entities within a large corporation or Cloud, but can also be used to monitor multiple customer environments from the Cloud.

A monitoring solution must provide a number of important features in order to fulfill the specific requirements in a cloud-based environment. D-Man addresses these needs.

The features are:

- Scalability
- Multi-domain support (Multi-tenant and Multi-channel environments)
- Security (internal/external)
- Deployment (installation/configuration)

More information about Secure monitoring in and from the cloud can be found in the 'Solution Brief Secure monitoring in and from the cloud', which can be downloaded on our website: [www.securit.biz](http://www.securit.biz)

## Summary

This Product Description clearly shows that through its unique and secure foundation SecurIT D-Man is a powerful monitoring solution that can easily be deployed in large, distributed e-Business environment where there is a need to have a centralised view on the status and health of the overall system.

## Key Features

### Multi-platform

Highly distributed environments normally consist of a heterogeneous set of platforms. SecurIT D-Man, being entirely based on Java, is available on all platforms that support a basic JVM. Among the supported platforms are AIX, HP-UX, Linux, Solaris and Windows.

### Straightforward installation

While standard packages are available for all supported platforms, D-Man is also available as a basic compressed file that can easily be distributed and expanded to any remote target system. This allows it to be integrated within any software distribution solution.

### One-step deployment

Once extracted, D-Man is immediately operational. No interventions on the target systems are required and the system can be completely configured and controlled from a central location.

### Firewall-friendly

To be able to cross the numerous firewalls that might

be in between the monitored system and the central reporting system, all internal SecurIT D-Man communication is entirely based on the HTTP and/or HTTPS protocols.

### Compliant to DMZ rules

E-Business systems contain components that reside within the DMZ zone. Because security rules dictate that connections from less secure zones to secure should be avoided as much as possible, D-Man will never create such connections.

### Light-weight

SecurIT D-Man has no external dependencies. It requires no application server and relies completely on the embedded light-weight Jetty runtime. The SecurIT D-Man agents require less than 500K of disk space and hardly consume more than a few mega of memory.

### Secure foundation

The bigger the environment, the higher the risks are for security breaches. A system monitoring such an environment should as such not impose an extra thread. For this reason, SecurIT has translated its years of experience in securing e-Business environments into a highly secure D-Man foundation based on SSL communication with mutually authenticated components.

### Embedded intrusion protection

To prevent malicious users from interfering with the monitoring system, the SecurIT D-Man agents never write any critical data (configuration data, events or monitor scripts) to disk. As such, the expected behaviour of the system can only be modified through the central administration console, which is protected by strong authentication.

### Redundancy

In distributed systems, the chances on unavailability increase by the size of the environment. SecurIT D-Man has been designed in such a way that the failure of any single component of the infrastructure will never cause the monitoring system to a stop or to lose any critical event data. At the monitored end-points, all SecurIT Agents are able to cache event data until it is collected

### Ready for Cloud

SecurIT D-Man is a powerful monitoring solution that can easily be deployed in the Cloud for a large, distributed environment, where there is a need to have a centralised view on the status and health of the overall system and its individual parts.

\* \* \*

For more information [www.securit.biz](http://www.securit.biz)

Copyright © 2012 SecurIT bvba. All Rights Reserved

No part of this document may be copied, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of SecurIT bvba. SecurIT has made every effort to ensure that the information in this document is accurate and complete; however, SecurIT assumes no responsibility for any errors or omissions. Information in this document is subject to change without notice.

Tivoli® is a registered trademark of Tivoli Systems Inc. in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavnssommer-Tivoli A/S.

IBM is a registered trademark of International Business Machines Corporation in the United States, other countries or both.

WebSphere is a registered trademark of International Business Machines Corporation in the United States or other countries or both.

Other product names mentioned in this paper may be trademarks or registered trademarks of their representative companies and are hereby acknowledged.