



## Data Center Management and Information Security

### **Remotely manage your data center out-of-band without sacrificing information security**

This is a document on information security related to data center management. It was designed to help you evaluate remote management products for a secure environment. Examples of those products are Console Servers, KVM gateways, and Intelligent Power Distribution Units.



Data center management is evolving to encompass a growing number managed nodes in heterogeneous environments dispersed over multiple locations. At the same time, limitations in IT budgets demand consolidation and more efficient use of support resources. The ability to remotely manage equipment is a top priority and information security became a major concern. Security-related features are one of the main factors in product selection.

This paper explains that security in a product is more than support for a feature, and requires robust implementation of protocols, sound design and, most important, a good security policy governing its use.

Each section starts with a short summary paragraph, so that you can quickly skim through them and adjust to your interest or knowledge level.

If you are specifically interested on how the Cyclades AlterPath products can support the security policies in your data center better than any other out-of-band management product line, please skip to "Why Cyclades AlterPath?" at the end of this document.



## Contents:

Data Center Management and Information Security .....	1
Contents: .....	2
Information Security - What Is It? .....	3
Security Policy - Why Do I Need It? .....	4
Mechanics of Protection - Layered Security .....	5
Vulnerability Exploits - What Is "Buffer Overflow" .....	7
Open Source Software and Security .....	8
Management and Security - SSH is not enough .....	9
Out-Of-Band - Security Features and Protocols .....	10
Why Cyclades AlterPath?.....	11
Customer Perspective .....	11
Feature set .....	11
Embedded Linux.....	12
Cyclades firmware testing and release .....	13
Knowledge in Security .....	13
Resources, References, Feedback And Contact Information.....	14
Resources .....	14
References .....	14
Contact Information .....	14



## Information Security - What Is It?

**Information Security has the objective of preserving confidentiality, integrity and availability of information in an organization and is achieved by combining good components, good architectural design, and good practices in the data center.**

Security cannot be purchased in a box.

That is similar to maintaining security of a home against burglary: strong and reliable door locks (components) are not effective unless everyone in the house remembers to lock them properly (process). Checking all doors and windows before leaving on vacation (process) will not prevent a burglar from breaking in if one of the windows has flimsy locking mechanisms (a single weak component can break the security of the system).

Information security processes deal with three attributes of information.

**Confidentiality** is the assurance that information is shared only among authorized persons or organizations.

**Integrity** is the assurance that the information is authentic and complete and can be relied upon to be sufficiently accurate for its purpose.

**Availability** is the assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Loss of any of the above information attributes threatens the continued existence of the corporate entities.

In order to maximize security, we need to define, document and follow the guidelines, procedures and rules that govern the data center (i.e. Implement a security policy), create a sound architectural design, and select robust products and systems implementing the security-related features necessary to support those policies and architecture.

## Security Policy - Why Do I Need It?

**In practical terms, a security policy is a published set of documents laying out the organization's philosophy, strategy, policies and practices with regard to confidentiality, integrity and availability of information and information systems.**



Defining a security policy may be a legal requirement in some industries and shows the commitment of an organization with its information security, fostering reputation and trust by business partners.

But the main reason to define a policy is that they play an important role in protecting your information assets and that is strategic to the survival of the organization.

The **Philosophy** is the approach towards information security, the guiding principles of the information security strategy. The security philosophy is a big umbrella under which all other security mechanisms should fall.

The **Strategy** is a measurable plan detailing how the organization intends to achieve the objectives that are laid out, either implicitly or explicitly, within the framework of the philosophy.

**Policies** are simply rules. They're the do's and the don'ts of information security, again, within the framework of the philosophy. Practices define the how of the organization's policy. They are a practical guide regarding what to do and how to do it.

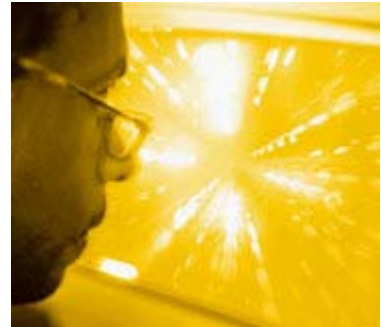
Implementing a security policy requires creating a supportive environment and promoting user education. The creation of a policy is normally driven by the power structures of the organization, motivated by a clear vision of the strategic importance of information security for the success of the enterprise. If that is not initially the case, changes to the structures and culture may be necessary since an effective security policy has to be implemented throughout the organization.

Explaining how to define a security policy is beyond the scope of this text, but a good introductory article on that is "Introduction to Security Policies" [1].

For business arguments to justify investing in security policies, refer to "Making a Compelling Case to Invest in Information Security" [3], available at the CERT site.

## Mechanics of Protection - Layered Security

**User authentication, data encryption, network traffic control, physical access control are some of the mechanisms available to preserve information security. Because no mechanism or device alone can maintain information integrity, it is important to deploy the security apparatus in a layered manner.**



A good general security principle is "defense in depth." Do not rely on a single protection mechanism and deploy them in layers designed so that an attacker has to defeat multiple defense mechanisms to perform a successful attack.

For example, packet filtering that blocks access from network addresses outside the organization may prevent the access of an attacker that has stolen authentication passwords. Data encryption can protect information confidentiality even when someone taps the physical network wires by breaking physical access security.

**User authentication** mechanisms are designed to uniquely identify users, assign their corresponding access rights to information, and track their activities. Let your workers know that you take the security of your organization's systems seriously, that they should as well and that user IDs and strong passwords are the primary means of safeguarding organizational assets. Authentication is usually performed by challenging the user to provide access keys (passwords, biometric information, tokens, ID cards, etc) and checking their access privileges against a RADIUS, LDAP or SLDAP database.

**Data Encryption** is the process of encoding data (through a series of mathematical functions) to prevent unauthorized parties from viewing or modifying it. It has the objective to protect the confidentiality and integrity of the information, even when the encrypted data is in transit over insecure media (such as the Internet). Data encryption works so that only the recipient can decode the data using the decoding algorithm (which is not necessarily secret) and an encryption key (which is secret). As an example, a remote terminal session using secure shell SSH usually encrypts data using 3DES or better algorithms.

**Network Packet Filtering** is performed at network level and can be performed at routers and gateways by analyzing headers of IP packets and allowing or denying forwarding based on source or destination address, protocol type, TCP port number, packet length, etc. This is useful to prevent access even before there is an attempt to authenticate or look at system data. Firewalls are devices that perform packet filtering but look beyond the IP headers and also analyze the packet payload for patterns to deny/allow.

**Physical Access Control** is the most basic level of security, but it is frequently forgotten. The most trivial way of stealing data or disrupting IT operations is to physically



take or destroy pieces of equipment. Before spending thousands of dollars securing your data against threats coming from the network, make sure to control physical access to critical servers and network infrastructure. A padlock may be your most effective information security investment.

**Data Logging, Health Monitoring and Event Notification** are facilities that do not have as main objective to obstruct intrusions, but to promote early detection of security breaches, identification of the source of the attack, and enabling faster recovery of lost data. They can prevent an attack from succeeding and minimize the damage would a security breach occur.



## Vulnerability Exploits - What Is "Buffer Overflow"

**While usually not a major concern for appliances and network infrastructure, patch and software vulnerability management are important in the context of the data center, because the existence of security vulnerabilities are frequently exploited in standard server and networking platforms.**

Software systems may have design flaws that can be exploited to work around established security mechanisms. Any system that is widely replicated over a standardized platform (such as server operating systems, for example) are particularly subject to attacks. Keeping up with patch and vulnerability management to fix known exploits of software bugs as soon as they are uncovered takes much of the attention of data center managers.

Let's look at some examples of common security exploits.

**Buffer Overflow** attacks take advantage of a specific and relatively common software design flaw. Many network-related programs fail to test the size of the messages they receive and, upon the receipt of messages that are longer than expected, they overflow the buffers and write data in memory that was originally reserved for something else (stack or executable code, for example). A well crafted malformed message can place arbitrary malicious code in memory and, with some luck, get the CPU to execute it. Exploiting buffer overflows requires detailed knowledge of the platform architecture and application memory map.

**Denial of Service** attacks have as the primary goal to affect information availability and deny the victim(s) access to a particular resource. Examples include attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between machines, thereby preventing access to a service. Illegitimate use of resources may also result in denial of service. Denial of Service attacks can rely on design flaws or be operated by brute force.

**Viruses, Worms and Trojan Horses** are different modalities of self-replicating pieces of malicious code. Users are misled to execute or install the code for the first time and then the code replicates itself into other systems through the network. Those usually exploit both software bugs and slack in the implementation of security policies in an environment.



## Open Source Software and Security

**Because Cyclades pioneered the use of Open Source technology in embedded management appliances, we are frequently questioned on the security implications of that choice. Open Source software is not inherently more or less secure than proprietary code. Security of a software system is result of the quality of its design, not to the availability of source code.**

There has been much media and public debate on the security merits (or weaknesses) of open source software.

Open Source advocates have argued that Open Source software is inherently more secure because fixes for uncovered design flaws are quickly distributed and made available. They further argue that early and intense code review promotes development of better quality code.

The counter argument is that, while it may be true that bugs are fixed quicker in Open Source, that is not a replacement for a sound security design.

Proprietary software advocates have argued that Open Source software is inherently less secure because hackers have access to the software supposed to protect system data and can easily find and exploit existing design flaws.

While keeping secrets usually does not hurt security, secrecy of the source code or encryption methods are weak protection and therefore not an argument in favor of proprietary software. An encryption method should protect the data even when the algorithm is well known. Security is the art of hiding in plain sight.

As any security expert will attest, the security of a system is directly related to the quality of its intrinsic design and the procedures governing its operation.

So, components of your management infrastructure should be selected based on the soundness of their design, the commitment to security demonstrated by the vendor, and by the functionality required to support your security policy.

Cyclades leverages on open source technology and believes that this choice contributes for a more secure product. But that is not the sole reason why claim to have the most secure products. The AlterPath family of product provides the best security support based on a security-focused design, proven track record in the largest security-sensitive data centers, and extensive testing in house and by independent entities (more details in the "*Why Cyclades AlterPath*" section).

For extensive additional discussion on Open Source and security, please refer to the document "*Secure Programming for Linux and Unix How to*" [2].



## Management and Security - SSH is not enough

**Console servers, KVM switches and gateways, and network-enabled intelligent power distribution units provide remote access to the management port of servers and network equipment in the data center. If security is compromised, not only data integrity may be compromised, but the integrity of the entire data center infrastructure is threatened.**

With the ability to manage large numbers of network nodes dispersed over multiple locations becoming more important to minimize data center downtime, security becomes one of the main parameters for selection of the out-of-band management components.

Capitalizing on that trend, some vendors market their products as "secure" based on the support for a few security-related feature (for example, many console servers are called "secure" just because they support SSH connections). That is in contrast to the times when most of the out-of-band management was done with Telnet through an "insecure" terminal server over a local area network.

Support for SSH or SSL connections alone does not define a secure product. The unit must support RADIUS, LDAP, and preferably SLDAP (secure LDAP, which encrypts database transactions) authentication, IP packet filtering, dual-factor authentication, IPSEC tunneling, extensive data logging and event notification, and any other feature necessary to support your security policy.

The implementation of those protocols have to be robust. For example, simply being able to connect to a box using a SSH client doesn't necessarily mean that the data is being properly and securely encrypted. You should check what the supported encryption algorithms are.

While patch management (software fixes for publicized attacks) tends to be important for servers, finding robust implementation of authentication (avoiding improper access) and encryption (protecting data in transit) protocols are the most important concerns with management appliances.

Because the out-of-band network carries management data (not application data), denial-of-service on the management infrastructure does not disrupt the application, which is the main target of attackers using that type of exploit. Also, because out-of-band management products usually utilize a proprietary hardware platform and customized OS images, crafting buffer overflow attacks would be a lot more difficult and they are not usually seen.



## Out-Of-Band - Security Features and Protocols

**SSH is important, but other features that may be difficult to find in the so called "secure" console servers and almost all KVM switches are not to be ignored. Here is a look at some of the features you should look at when selecting a management product..**



**User Authentication** for a connection for out-of-band management is performed through an user-ID and access key (password, biometrics, securID token, etc). The user-ID and access key must be checked against an authentication privilege database using request based on **RADIUS**, **Kerberos** or **TACACS** (the most common protocols in networking applications) or **LDAP**, **SLDAP**, **NIS** (to query the centralized enterprise database) protocols. If the out-of-band gateway is to be accessed also over dial up lines, it should support **PAP/CHAP** dial up authentication protocols too. Support for local password authentication is not enough and creates serious management and security problems.

**Session Encryption** is also important so that authentication and management data are not transmitted in clear text form over the network. The most common connection application used in data center management is **Secure Shell (SSH) version 2**. We emphasize the protocol version because it uses more secure protocols and key exchange keys than the version 1 present in many products. If browser-based access is utilized, you should make sure the web server software is using secure **HTTPS with SSL version 3 encryption** (here again, version 3 is more robust than the most common SSL version 2).

**Packet Filtering** is a rare feature in out-of-band management products. It is true that some of the external traffic can be filtered at the corporate firewall. But, because of out-of-band management traffic is so critical, you may need to further restrict access to the console ports, limiting the protocols that can be used and the machines from which it can be accessed. You may also need to restrict traffic that is internal (corporate firewalls usually protect only against external traffic). That is why packet filtering in the out-of-band management equipment itself is required in a highly secure environment.

**Data Logging and Event Notification** are not usually seen as security features, but as we have discussed before, security strategies cover not only prevention of security intrusions, but also early detection and damage control when intrusions do occur. The out-of-band management product should be able to log events and management data create paper trail and the data should be stored either locally or at a server (using syslog or NFS protocols). Advanced products can actually parse console messages, interpret them and take automatic actions or notify the system administrator.



## Why Cyclades AlterPath?

**You should consider AlterPath products for management in a security environment because they can completely support the stringent security policies in your data center. They have a proven track record being used to manage hundreds of the largest data centers worldwide. The AlterPath products were designed with security in mind by a company with tradition in secure remote access and management.**

Cyclades revolutionized the console management market by introducing an innovative line of console servers in 1999 with a feature set specifically designed for secure remote management. The Cyclades-TS was the first console server to offer robust authentication, SSH encryption and packet filtering. Until then console management was restricted to private local LAN access using insecure reverse telnet sessions.

Introduced in 2002, the AlterPath product line of out-of-band management products builds on the original platform and adds even more resources to support secure management applications.

In addition to the rich, robust and consistent feature set in each product, the AlterPath family is integrated under a single security model preventing the information security of your out-of-band infrastructure from being compromised by a single weak component.

### *Customer Perspective*

The Cyclades AlterPath line of data center management products are being used to manage most of the largest data centers in existence, the majority of which are very security sensitive.

We have been particularly successful in the financial and Internet segments, with Yahoo, Wells Fargo Bank, HSBC, and JP Morgan/Chase figuring as some examples of deployments of Cyclades equipment. You can find a list of customers on the ["Customers" section](#) of the company website.

While customer adoption of a product is not necessarily an indication of security the confidence these and thousands of other customers have deposited in our product is certainly a good reference for you.

We invite you to search newsgroups and system management mailing lists on the Internet for independent feedback on console management products. We are confident that you will find solid good reputation for Cyclades products.

### *Feature set*



As mentioned before, security is not a software feature or a product attribute, but a good product need to offer and implement a robust feature set to support those policies. The Cyclades console servers do exactly that.

The security-related features listed below are absent or incomplete (less secure version, not all protocols or methods supported, etc) in most console servers and almost all KVM products in the market.

User authentication can be done locally or through redundant authentication servers using RADIUS, TACACS, LDAP, Secure LDAP (SLDAP, which encrypts database traffic), NIS, Kerberos and other protocols. Dial up connections can be authenticated with PAP/CHAP. Dual-factor authentication (e.g. SecurID token authentication) is supported.

Console data is encrypted using SSH v2, using the same code base used in most Unix servers (OpenSSH). OpenSSH is trimmed down and all non-essential features and options are disabled, making it even more secure. Web-based traffic is encrypted with SSL.

AlterPath ACS products, can perform filtering at IP packet level and block packets based on source/destination address, protocol type, TCP port number, etc. The LAN interface supports multiple IP addresses so that you can configure exclusive management subnets.

The unit can log audit trails both in local memory and to a syslog or NFS server. All console data, events and sessions can be logged with timestamps.

Other features such as port sniffing (administrators can monitor, close or take over existing console connections) and event management allow you not only to prevent intrusions, but also to audit and detect any intrusion attempts.

### *Embedded Linux*

AlterPath products run a hardened version of embedded Linux. We take the general purpose operating system being adopted in a large number of enterprise data centers, trim it down, disable all the non essential features and options, harden and embed it in a custom-designed management appliance.

Because we run in a proprietary, purpose-specific hardware with a custom Linux image, common buffer overflow attacks affecting popular Linux distributions are unlikely to apply to AlterPath products. Brute force denial-of-service attacks could disrupt management access, but would not be effective in compromising the application or integrity of application data.

We leverage on good quality Open Source technology, but we don't rely only on that for the security of our implementation. We inspect all code, test it, remove functions that are not required for the product, and disable unused options. That way, the embedded Linux



platform becomes very stable and secure, certainly more secure than the typical enterprise Linux-based application server.

While not a common security procedure, more stringent installations such as military and governmental data centers may require source code auditing. The code in AlterPath products are available in source code form for inspection, would that be necessary.

### *Cyclades firmware testing and release*

Firmware updates for the Cyclades console servers are released approximately once a quarter. Customers can download new firmware releases from the website using ftp and save them in flash memory. New releases notifications are included in the Cyclades newsletter distributed through the user mailing list.

We are committed to maintaining the firmware bug-free and secure, so there may be intermediate releases between the quarterly releases. If there are critical vulnerabilities or bugs we may notify you about intermediate releases using the newsletter/user mailing lists.

In addition to extensive quality assurance performed in-house for functionality and security, all software releases are submitted to frequent automated security scanning during the development process. This service is provided by a third party independent company ([www.qualys.com](http://www.qualys.com)) and it consists of methodical automated scans against an up to date database of known security exploits.

We also periodically submit our code to custom inspection and testing by an independent security expert.

### *Knowledge in Security*

Differently from most vendors of out-of-band management products, Cyclades has a long history developing enterprise networking products, including routers and remote access servers. The AlterPath products benefit from that experience and incorporate the enterprise networking features that became important as out-of-band management turned from local into a remote, network-enabled application.

In addition to the general security FAQ in the company website and this white paper, Cyclades sales and support engineers are educated to discuss your security concerns.

If you are writing security policies for your data center that cover the out-of-band management infrastructure, you can request the "[Security Blueprint](#)," which is a template for best practices documentation related to the installation of console servers in a secure environment. This document can be modified to your specific needs and be incorporated into your security policy.



## Resources, References, Feedback And Contact Information

### *Resources*

CERT is a federally funded research and development center operated by Carnegie Mellon University. It is a expertise center on Internet Security and a well recognized source of information and vulnerability alerts. CERT website <http://www.cert.org>.



### *References*

[1] Introduction to Security Policies, Charl van der Walt,  
<http://www.securityfocus/infocus/1193>

[2] *Secure Programming for Linux and Unix Howto*, David Wheeler,  
<http://www.dwheeler.com/secure-programs/>

[3] Making a Compelling Case to Invest in Information Security, Julia Allen,  
[http://www.cert.org/features/green/business\\_case.html](http://www.cert.org/features/green/business_case.html)

## Contact Information

For more information and to purchase Cyclades data-centre management solutions contact KVM Partnership Ltd on **0870 2202 370**, or email **sales@kvmpartnership.co.uk**