

SUNSM MANAGED OPERATIONS

**Security White Paper
April 2006**

Table of Contents

Executive Summary	3
Sun Managed Operations	3
Deployment Architecture	4
Sun Managed Operations Delivery	6
Data Privacy	7
Summary	7

Executive Summary

Selective outsourcing is increasingly becoming an important tool in an IT manager's arsenal of options for helping to assure appropriate management of an organization's IT infrastructure. The operations model for IT management has shifted from delivery inside the customer's four walls to remote delivery or hybrid delivery models, where on-site staff are augmented by a remote support team. Moving management controls outside the "firewall" poses some significant challenges for customers, including connectivity, security and privacy concerns.

It's important to note that helping ensure security is not simply a matter of deploying technology, but is an equal mix of people, process and technology. To help ensure harmony between these three areas, SunSM Managed Operations adopted the IT Infrastructure Library (ITIL). These proven processes have been embedded into the core of Sun Managed Operations for more than five years.

This white paper details the best practice approach applied by Sun Management Operations to help ensure protection of customer assets when delivering services remotely.

Sun Managed Operations

Sun Managed Operations has adopted a classic security model based on confidentiality, integrity and availability. These principles create a foundation for the delivery of remote managed services.

- **Confidentiality** helps ensure a customer's data remains private and is not disclosed to unauthorized individuals. This is perhaps one of the most important aspects in delivering remote services, but correspondingly, is also attacked most frequently. Cryptography and encryption are examples of methods that help ensure that the confidentiality of data transferred from one system to another remains confidential.
- **Integrity** helps ensure that data is an accurate and unchanged representation of the original secure information.
- **Availability** helps ensure that data is readily accessible to the authorized viewer at all times. Some types of security attacks attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or for some secondary effect. For example, a denial of service attack against a service provider obscures direct attacks against customers of the service provider.

Included within each of these security principles are technology-based solutions Sun Managed Operations has developed or integrated from best-of-breed tools. Micromuse Netcool forms the foundation of the management framework, integrated tightly with BMC Remedy ARS to help ensure smooth and automated transition between alarms and ITIL incidents. Sun Managed Operations developed a middleware stack based on the JavaTM Message Service called ControlTower. ControlTower adds many additional security controls, data segregation and encryption to help ensure appropriate controls are in place to protect a customer's IT assets. Collectively, these applications provide functions such as user authentication, audit record creation and management and data privacy.

The ControlTower architecture consists of the following applications:

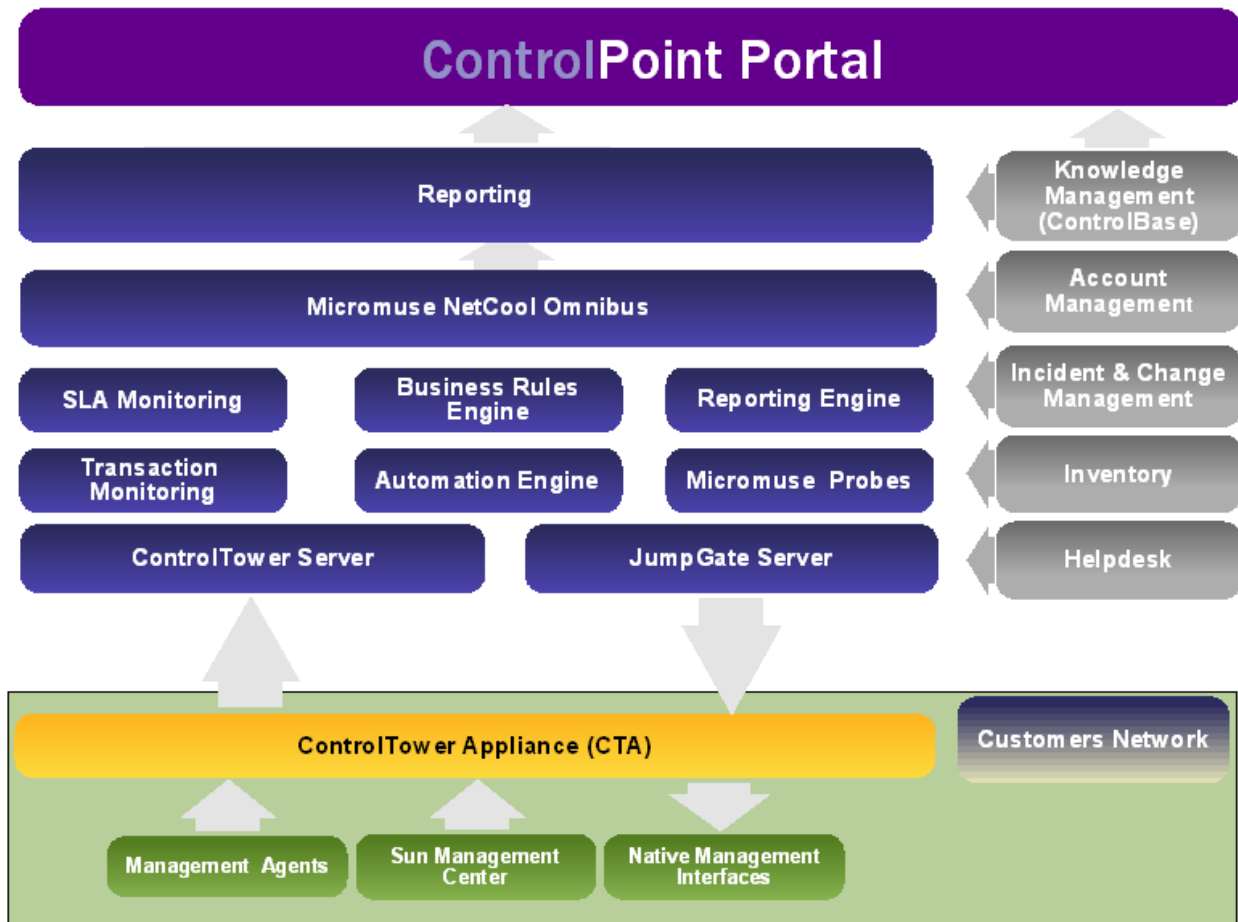


Figure 1. ControlTower architecture

Deployment Architecture

Within the customer's environment, ControlTower consists of a management agent deployed on the servers or native agents devices such as routers and firewalls. These agents deliver messages to the ControlTower appliance (CTA), that lives inside the customer's network. All communications between the agent and the CTA use open standards protocols that allow customers to collaborate on security controls with Sun to help ensure the management solution conforms to the customer's security policies.

The CTA also provides a capability known as JumpGate. JumpGate is the management interface to interactively control managed servers and devices. This is accomplished using native management interfaces of these servers/devices, such as Microsoft RDP, SSH, Telnet etc. All access to Jumpgate requires token based authentication and must originate from the JumpGate server hosted within the Sun Managed Operations core network. 2048bit RSA public keys are used to help facilitate trust. All access to JumpGate is logged to help ensure accountability of actions.

The CTA supports multiple deployment configurations including DMZ, trusted network, management network and in some cases outside the customer's firewall. The appropriate placement of the appliance is defined in collaboration with the customer during the implementation phase of an engagement.

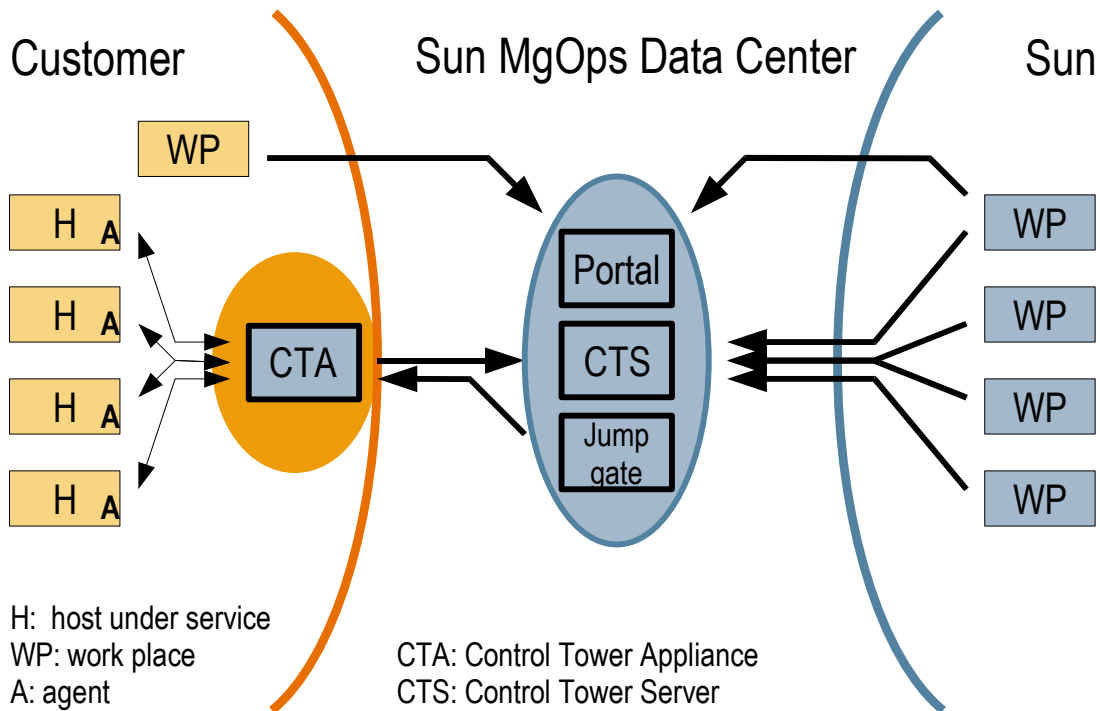


Figure 2. Typical CTA deployment

Summary of CTA capabilities:

- hardware and software critical event monitoring
- hardware and software performance monitoring
- acquisition of performance metrics for reporting and trending
- XML event encapsulation
- event filtering and suppression
- guaranteed delivery of events
- JumpGate management gateway
- patch management
- deep security scanning
- execution of diagnostic scripts
- collection and monitoring of device configuration
- compression of event and management traffic
- support for the Solaris™ Operating System (OS), Microsoft Windows, Linux, AIX, HP-UX, etc
- support for a wide range of network devices from vendors such as Cisco, Juniper, extreme networks, etc.

Sun provides three connectivity options to interface the CTA to the Sun Managed Operations data center:

- **SSL/SSH VPN:** This is the preferred and default connectivity mechanism. In this mode, the customer permits an outbound SSL connection from the CTA to the Sun Managed Operations data center and an inbound SSH connection between the center and the CTA. This provides equivalent encryption standards as a traditional IPSEC VPN, but reduces the complexity of deploying a VPN termination device into the customer's network and also provides the customer with a less intrusive configuration. The outbound connection utilizes RSA cipher suite featuring 128bit RC4 private key encryption. Inbound connection is SSH2 featuring 2048bit RSA public key encryption. Customers are provided two firewall rules for connectivity restricting traffic to specific IP addresses in Sun Managed Operations Delivery.
- **IPSEC VPN:** Sun Managed Operations provides support for IPSEC VPN deployments where the SSL/SSH VPN traffic is encapsulated inside a traditional IPSEC VPN. IPSEC VPN is provided in exception basis.
- **Private Circuit:** Private connections are also supported via frame-relay networks. Private circuits are provided in exception basis

Sun Managed Operations Delivery

Sun Managed Operations uses class A data center facilities to host the management infrastructure used to support customer deployments. Data centers are located in Washington DC with disaster recovery in London, England. Physical access to these data centers is restricted to named individuals and requires biometric authorization.

All changes to Sun Managed Operations infrastructure is tightly controlled via ITIL change management processes, with active change detection controls deployed. Every 24 hours, a deep security scan occurs where any detected changes or new vulnerabilities released by software vendors are evaluated for impact to the platform. This process and the ongoing support of Sun Managed Operations Delivery is provided by a dedicated team providing 24/7 coverage. Access to all key systems requires strong token based authentication which is logged and reviewed regularly.

Within the infrastructure Sun Managed Operations Delivery uses Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Sun purchased IDS/IPS software from diverse vendors to improve signature coverage and diversity of attack mitigation of these tools.

Every device, server and environment metric is collected from the systems and delivered into the same monitoring frameworks used to support our customers. This provides continuous monitoring of performance, availability and security of the core infrastructure.

Data Privacy

Sun only collects information key to the delivery of services, such as performance, event alarms and machine configurations and avoids situations where privacy classified information might be collected. This dramatically reduces the value of the message should it be intercepted enroute. Since only machine performance/health data is extracted, Sun Managed Operations does not maintain any privacy related data types inside core systems.

```
<event>
  <eventType>SNMP</eventType>
  <ctaId>54103</ctaId>
  <sourceAddress>10.0.4.86</sourceAddress>
  <timestamp>1134062488388</timestamp>

  <snmpVersion>v1</snmpVersion>

  <varbinding1 name=".1.3.6.1.4.1.546.6.1.1.2.607" type="4">#3-High Interrupt Rate</varbinding1>
  <varbinding2 name=".1.3.6.1.4.1.546.6.1.1.5.607"
type="6">.1.3.6.1.4.1.546.1.1.7.8.17.0</varbinding2>
  <varbinding3 name=".1.3.6.1.4.1.546.6.1.1.6.607" type="2">173816</varbinding3>
  <varbinding4 name=".1.3.6.1.4.1.546.6.1.1.8.607" type="2">150000</varbinding4>
  <varbinding5 name=".1.3.6.1.4.1.546.6.1.1.12.607" type="2">1</varbinding5>
  <varbinding6 name=".1.3.6.1.4.1.546.6.1.1.7.607" type="2">2</varbinding6>
  <varbinding7 name=".1.3.6.1.4.1.546.6.1.1.1.607" type="2">607</varbinding7>
  <varbinding8 name=".1.3.6.1.4.1.546.6.1.1.16.607" type="2">3146496</varbinding8>
  <enterpriseOID>.1.3.6.1.4.1.546.1.1</enterpriseOID>
  <genericType>6</genericType>
  <specificType>1</specificType>
  <upTime>169611602</upTime>
</event>
```

Figure 3. Sample XML message

This data is delivered to the management center as an encryption XML message. Within the XML message, it is not possible to associate the message with a specific customer without access to the Sun Managed Operations correlation system.

Helping ensure the privacy of customer data is of paramount importance to Sun. In fact, Sun is an active member of many privacy forums and is on the forefront of defining controls for the next generation of privacy legislation.

Summary

Using the appropriate blend of people, process and technology, Sun Managed Operations is able to safeguard the security and privacy of customers' environments and has been doing so for five years. The technology and processes deployed are under continuous review to help ensure appropriate responses to new threats.

For more information regarding this approach, or for a discussion of how Sun Managed Operations can help deliver operations management in your environment, please contact your Sun account manager.