McAfee Professional Services

McAfee Services

Unisys ClearPath® OS 2200 Software Series Security Assessment

Prepared for Unisys

October 28, 2019

McAfee™

Table of Contents

Overview

Unisys engaged McAfee Advanced Cyber Threat Services (ACTS), to deliver a multiphase independent product penetration test and security assessment against the Unisys ClearPath® OS 2200 Software Series (OS 2200) operating system. The scope of this project included virtualized instances of the OS 2200 Operations Server (Operations Sentinel, SMC), Apex Server and QProcessor Server. The test bed provided consisted of virtualized instances, on an ESXi host.

The engagement consisted of, an initial threat modelling exercise based on detailed documentation review and interviews with the Unisys architects team and Development team. In addition, an operating system security control evaluation was conducted and testing of the network interfaces exposed across the Public, Private and Operations networks.

The McAfee consultant conducted a security review, and exploitative penetration testing, from the perspective of differing threat actors, during phases 1 and 2 of the assessment. Phase 1 and 2 were conducted in March 2019. The McAfee consultant provided continual engagement feedback to the Unisys teams during testing. The testing was conducted using a white box approach resulting in greater detailed testing coverage. This allowed the tester to work with development and architecture teams to refine test execution during testing phases and provide instant findings through a process of daily meetings with the Unisys key stakeholders and technical teams.

This document provides a security overview of OS 2200 Software Series by Unisys, based on the white box security testing conducted by McAfee. The OS 2200 Software Series operating system was designed for an enterprise class client base, requiring a high level of information security and assurance, and an operating system designed to exceed information security best practices for authorization, resource management, and reliability.

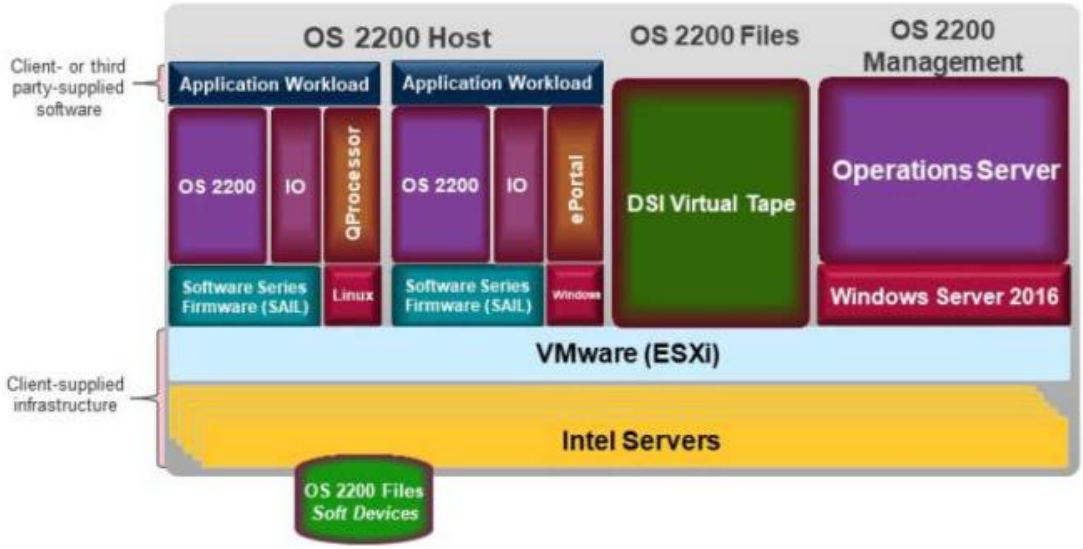
ClearPath OS 2200 Software Series Summary

The Unisys ClearPath OS 2200 operating system is designed to provide a robust and secure platform for a wide variety of customer requirements.

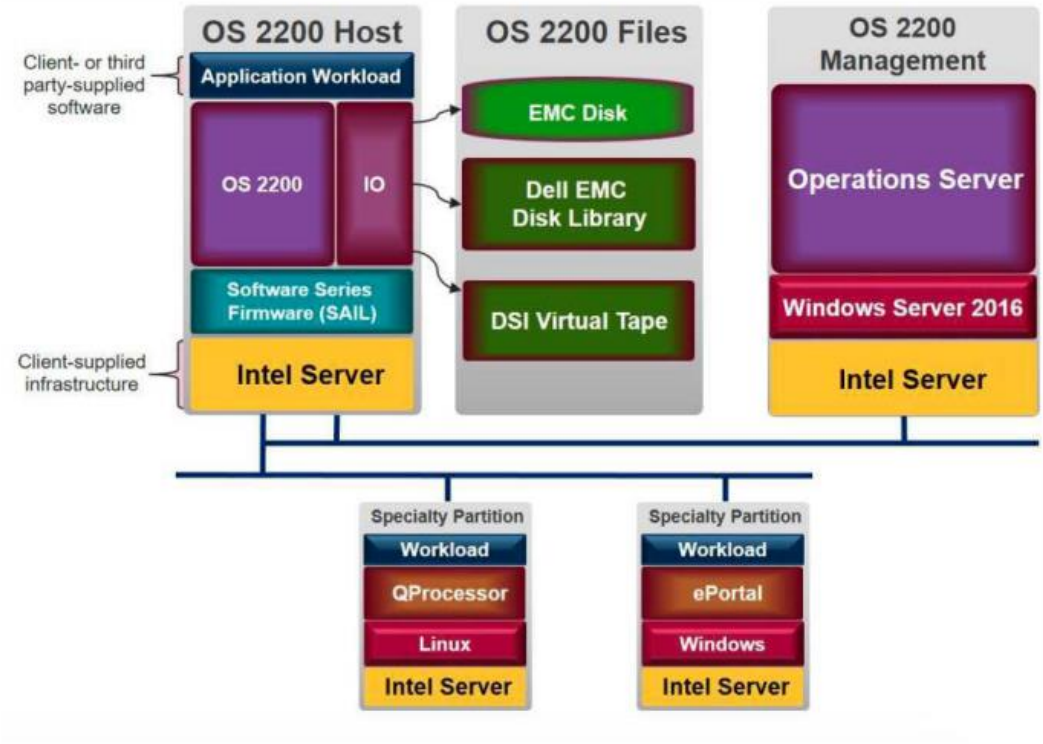
ClearPath OS 2200 Software Series uses the same ClearPath OS 2200 release software as the ClearPath Forward® Dorado systems. ClearPath OS 2200 Software Series combines the SAIL (System Architecture Interface Layer) infrastructure along with the I/O processing into a single operating environment. This allows for deployment in a VMware environment or on a single bare metal platform for the OS 2200 host.

The below Unisys images show the relationship between the ClearPath OS 2200 Software Series and its basic components on VMware and bare metal platforms. Similar to the ClearPath Forward Dorado environment, the administration and operation of the ClearPath OS 2200 Software Series environment is provided by OS 2200 Server Management Control (SMC), Operations Sentinel, and the SAIL Control Center. SAIL is the firmware that provides the infrastructure that allows OS 2200 software to execute in an Intel processor environment. SAIL is a locked down Linux environment that includes only a minimal number of required packages.

VMWare Deployment



Bare Metal Deployment



Unisys has developed the concept of Security Levels. These are a set of OS 2200 security configuration templates, designed to support a broad range of customer information security objectives. Fundamental security and Security Levels 1 through 3 each provide sets of capabilities that a client can enable. For sites with more stringent information security requirements, a higher Security Level provides a more rigidly protected OS 2200 environment.

The operating system kernel of OS 2200 provides a fine-grained security mechanism based on the principle of least privilege. This principle demands that only the minimum privilege be granted necessary to perform the task required. Therefore, the OS 2200 operating system has no concept of a super user role, unlike most other operating systems, which can be assumed by any user. Rather, OS 2200 uses a large set of specific privileges which may be granted separately to each user, with each privilege being associated with a specific authority. The OS 2200 Exec contains all the code in the system allowed to run at the highest privilege levels. There are no mechanisms for other code to be promoted to those privilege levels. The OS 2200 Exec is responsible for managing the system hardware, scheduling and managing work, and communicating with operators and administrators. The OS 2200 Exec supports thousands of concurrent users and insulates them from affecting each other's execution while providing the highest degree of access security available in the industry. In addition, the OS 2200 implements a fully virtual file system, allowing files to be allocated anywhere, across any of the mass storage devices.

Testing Rational & Methodology

Threat Modeling

The threat-modeling process began with a high-level architecture review of the OS 2200 Software Series operating system's design to build on the consultant's existing experience and understanding of the OS 2200 security considerations and deployment scenarios. McAfee worked with the Unisys architects and development teams to understand the implementation and structure of the testbed that had been built and the relevant security controls.

Through meetings and a thorough review of the detailed documentation provided by Unisys, McAfee derived a list of credible threats to the various components which make up the solution. This process resulted in a number of test scenarios relating to the OS 2200 Software Series test bed, its attack surface and a profile for the potential threat actors within these scenarios. The result was an informed testing approach used during the following phases of the engagement.

OS 2200 Software Series Penetration Testing and Security Configuration Review

The Internal Penetration Testing against the OS 2200 Software Series testbed sought to attack the operating systems of both the OS 2200 instance but also the supporting systems within a typical client deployment. This testing was undertaken across the testbed from the perspective of an authenticated and unauthenticated network-based user. Concentrating on the services advertised and the vulnerabilities in these services that could be leveraged by an attacker, to compromise the integrity of the systems and the data stored, processed, and transmitted by them.

In addition, a Security Configuration Review was performed to assess the effectiveness of the security controls applied by an OS 2200 Software Series instance. The systems reviewed during this engagement were configured in accordance with publicly available documentation provided by Unisys. The tests conducted sought to enumerate, analyze, test and evidence the presence and effectiveness of the OS 2200 Software Series security controls and those controls interaction with supported applications on the OS 2200 testbed.

These controls are core to the maintenance of the confidentiality, integrity and availability of assets stored, processed and transmitted by the operating system.

The System Security Review, was performed using both interview-based questioning of the development team, application specialists, security consultant and operational team, and an interactive review of the settings on the test systems provided. This approach provided an effective means of rapidly determining the nature of the configured host-based security controls.

Network Protocol Analysis and Attack

Within the ClearPath OS 2200 Software Series test environment, consisting of the Public, Private and Operations network in the virtualized environment, several proprietary network protocols and protocol implementations were tested. Security testing was performed against application and operations management protocols as both an unauthenticated user with network level access to the exposed interface and as an authenticated network user, to ensure maximum code base coverage.

In scope application protocols selected as attack targets based on the threat modelling exercise included; cpFTP, CIFS, TIP and JDBC connectivity to an RDMS database. Operations network protocols selected included; Demand, Operations Sentinel, Systems Management Console (SMC), QProcessor and Apex Agent.

Areas of Analysis & Recommendation

Analysis Topic	Best Practice	Evaluation	Recommendation
Network Protocol Testing (Operations)	Where OS 2200 operations management protocols are exposed on the segmented Operations network. These protocols should effectively protect the confidentiality, integrity and availability of the data and interface. In addition, the daemon should effectively restrict access and handle malformed traffic throughout the client server communications.	Two phases of fuzzing were conducted against the elements of the OS 2200 Software Series test bed's attack surface. In the first phase scripts and utilities were developed to duplicate the client server conversation and replicate these protocols, including initial dialog setup and the authentication exchanges under test. The second phase, performed protocol fuzzing utilizing the native client for the network protocol. Under this scenario the McAfee consultant, was able to more comprehensively test the wider code base of the target daemon. This second phase was performed using a TCP and UDP redirector to allow the McAfee consultant to manipulate precise segments of the protocol exchange.	The Operations Sentinel, SMC, Apex Agent and Demand management protocols were tested extensively during the second phase.
Network Protocol Testing (Application)	Where OS 2200 application protocols are exposed on the segmented Public or Private networks. These protocols should effectively protect the confidentiality, integrity and availability of the data and interface. In addition, the daemon should effectively restrict access and handle malformed traffic throughout the client server communications.	Two phases of fuzzing were conducted against the elements of the OS 2200 Software Series test bed's attack surface. In the first phase scripts and utilities were developed to duplicate the client server conversation and replicate these protocols, including initial dialog setup and the authentication exchanges under test. The second approach performed protocol fuzzing utilizing the native client for the network protocol. Under this scenario the McAfee consult was able to more comprehensively test the wider code base of the target daemon. This second phase was performed using a TCP and UDP redirector to allow the McAfee consultant to manipulate precise segments of the protocol exchange.	The cpFTP, CIFS, TIP and JDBC-RDMS protocols were tested extensively during the engagement. Vulnerabilities were found in application services which resulted in a Denial of Service condition for the daemon when malicious and malformed data was sent to the network daemon. In collaboration with the Unisys development teams, code fixes were developed, tested and applied to the test bed for retesting and continued testing.

Security Configuration Assessment	Apply stringent resource restrictions based on user access requirements. Vendors should encourage secure installations of products. Optional security settings and cryptographic controls should be configured in a default secure state.	OS 2200 Software Series supports a range of four security configuration levels. These allow administrators to configure OS 2200 Software Series to select a comprehensive set of security control configurations to meet a specific organization's security objective. Each Security Level from Fundamental to Security Level 3, creates a more stringent environment than the previous profile. In addition to the templated Security Levels to govern the OS 2200 system security settings, Unisys have published a security support library allowing customers to customize the operating system's security controls to meet their specific requirements. The evaluation of the secure configuration of the OS 2200 Software Series virtualized systems performed by McAfee, was conducted through interactive systems testing, including assessments against the implementation of cryptographic controls to protect the confidentiality and integrity of data. This included interview led questioning with the Unisys development and architecture teams and penetration testing.	Clients should follow the comprehensive documentation guides and recommendations provided by Unisys when configuring and building their OS 2200 Software Series environment. These guides provide a well-structured recommended configuration and options for tailoring customers' OS 2200, for specific operational security goals. During testing the controls implemented and configured within the OS 2200 Software Series testbed proved resilient to attack and circumvention. During the phases of this engagement McAfee was unable to circumvent or undermine the effectiveness of the operating systems controls configured.
Access Control and Authorization Security Testing	Access Control and Authorization Control should be configured to consistently apply the Principle of Least Privilege and minimize the attack surface of the systems at all times.	All access points into the OS 2200 Software Series systems presented on the testbed were designed to require authentication. Further minimizing the potential attack surface of the OS 2200 Software Series systems tested, segregation of traffic types is configured using separation of Public, Private and Operations communications. During testing no restrictions were placed on the networks that McAfee could test from, therefore giving maximum coverage across all interfaces during the project test phases.	By following the Unisys implementation guides, clients can gain assurance that access control and authorization in their OS 2200 Software Series deployment has been consistently and effectively applied.

Logging and Auditing Assessment	The operating system should be capable of presenting administrators with a log of all system activities.	Following the phases of testing against the OS 2200 Software Series testbed several of the tests generated both audit events and debug output which were required to assess the effectiveness of the network-based attacks conducted by McAfee. The configuration of logging and debugging throughout the testbed provided a granular and detailed view into the attack activity conducted. Use and review of these logs allowed McAfee to determine the nature and suitability of events captured during attacks.	No recommendations are necessary for this topic. The OS 2200 Software Series test-bed reviewed both meets or exceeds industry best practice, in relation to their ability to effectively record, manage and maintain detailed system event logs.
QProcessr Administration Console Web Application Assessment	The QProcessor Administration Console web application and supporting infrastructure, should protect the confidentiality, integrity and availability of the systems and data resources at all times.	A web application assessment was undertaken of the QProcessor Administration Console. This included assessment of the PHP web application, with particular attention focused on the authentication and authorization controls.	No flaws were discovered in the authentication and authorization controls in place developed to protect access to resources and administrative functions relating to QProcessor. It should be noted that the authentication and authorization controls in place, were controlled by the granular controls of the OS 2200 Software Series.

Conclusions

This assessment focused on the Software Series, in previous review McAfee focused on the OS 2200 ClearPath Dorado platform (the physical platform for OS 2200). During the engagement McAfee were asked to compare the maturity of the security controls tested between the OS 2200 ClearPath Dorado and OS 2200 Software Series.

The OS 2200 Software Series provides clients with a robust set of security configuration templates and secure architectural guides, from which a customer can select the level of security to be applied to their implementation and its supporting components. It is evident that the OS 2200 operating system and supporting Unisys infrastructure and applications, have had security by design as a guiding development principle. These principles include aspects such as “deny by default”, “least privilege” and “foot print minimization”. These were seen to be evident throughout earlier reviews of the OS 2200 ClearPath Dorado and similarly during the security assessment of the OS 2200 Software Series. These principles were evident by default, but also combine with deployment documentation supporting specific customization and refinements of the OS 2200 Software Series to meet and exceed a variety of information security objectives.

OS 2200 Software Series is also designed to provide a secure environment for program execution which protects against attempts to inject and execute malicious code. OS 2200 Software Series access control capabilities allow administrators a granular means to control which users and processes can access data files, execute programs, and manage all of the systems resources. OS 2200 Software Series provides a robust auditing and logging mechanism integrated into the operating system. Extensive logging includes a large number of events that are logged as being either security relevant, or security violations, enabling the rapid discovery and forensics of potential attacks. OS 2200 Software Series provides an integrated technology stack in which all system components, including resource allocation, system monitoring, and account management have all been designed, implemented, and tested to collaborate and promote system wide security.

The OS 2200 Software Series memory resource management helps mitigate buffer overflow attacks, by preventing user applications from being granted direct memory access. This concept was tested at length across the duration of the McAfee engagement for Unisys.

In addition to the security controls tested and identified within the OS 2200 Software Series operating system, the McAfee consultant noted during the review that close collaboration and effective reporting and cross working between the ClearPath OS 2200 Operations, Architecture and Development teams within Unisys are in place. During testing it was noted that this culture allows Unisys to respond rapidly and coordinate patches and remediation during the test phases.

As with any software platform, administrators and users can greatly affect the overall security. The OS 2200 Software Series environment offers a wide variety of security configuration capabilities and care should be taken to adhere appropriately to the comprehensive, security focused implementation guides provided by Unisys. During review these documentation sets seek to support clients in their specific OS 2200 Software Series deployments and help clients meet their specific information security objectives.

About McAfee

Technology has the power to enrich the life of everyone. To transform how we live and work. But as technology becomes more deeply integrated into life, security must be more deeply integrated into technology.

By combining the security expertise of McAfee with the innovation, performance, and trust of Intel, this vision is becoming a reality.

Security that's built-in by design, seamlessly integrated into every device at every layer of the compute stack. Protecting valuable intellectual property, data, devices, and identities. So in everyday and business life, people can feel secure in the digital world.

It's why we're taking a "security connected" approach. Across every architecture of every platform from chip to cloud — smartphones and tablets to PCs, servers, and beyond. We're moving security from discrete solutions to an integrated approach as pervasive as computing itself.

About McAfee Professional Services

Three practices one objective. Your security.

Our Worldwide Professional Services organization is ready to respond to the changing needs of global customers and partners seeking security consulting services — from incident response and security risk assessments to comprehensive, customized deployments and training.

Advanced Cyber Threat Services consultants are seasoned experts skilled at identifying network and application vulnerabilities, providing remediation recommendations, and helping organizations design iron-clad security programs and enforceable policies.

Solution Services consultants are highly skilled at properly planning, designing and implementing security technologies so you can feel confident that you are gaining the most from your investments in McAfee security solutions.

Education Services courseware developers and instructors design and deliver product training and security education to help fortify your security defenses. Customers gain critical skills necessary to deploy and administer their McAfee solutions through formal instructor-led training and self-paced learning opportunities, and then have the opportunity to validate these skills with industry-recognized certifications.

McAfee™

2821 Mission College Blvd.
Santa Clara, CA 95054
888 847 8766
www.mcafee.com