White Paper

Integrating Host Systems with Modern Security Frameworks

The world has changed around your host systems. Today, these enterprise workhorses—rich with decades of data—don't fit into your modern security framework. In fact, your modern security framework protects everything but your critical hosts. And yet regulatory requirements demand equal data protection for all.

This white paper reveals a practical way to bring your host systems into the modern security fold—finally closing the technology gap—without jeopardizing business operations.

opentext™

Table of Contents

page

The Host Stands Alone 1
Modern Security Frameworks 2
Building the Host-IAM Alliance 3
Equal Protection for All 8

The Host Stands Alone

Once upon a time, host systems lived in a secure world. Host data traveled a protected path to and from a trusted terminal. The host knew who the user was, where the data came from, and where the data was going.

Times have changed. Today we have open networks, service-oriented architectures, and hackers who hack faster than IT can patch. Host security hasn't kept up. Traditional host-access security leaves data dangerously exposed in a number of ways:

Weak, Decentralized Authentication

Simple eight-character passwords may be all that stand between a malicious hacker and your critical host data. Host-based authentication, by itself, cannot leverage the full power of the identity management system used by the rest of the enterprise.

Weak, Decentralized Authorization

Once logged onto the corporate network, a user has easy access to your host applications. That means an attacker need only steal a user's eight-character host credentials to trespass into personal data fields.

Decentralized Auditing

Host-access auditing is performed by each host, based on each user's host ID. When multiple hosts are involved, security administrators have to examine the logs on each one—comparing the user ID for each host to the user ID for the enterprise—to build a complete audit trail.

Problematic Encryption

Until the arrival of SSL/TLS encryption in the 1990s, data and passwords traveled between the client and the host in clear text. There was no safe haven from prying eyes. SSL/TLS solved the encryption problem, but not without a catch: Encrypted traffic cannot be monitored in the DMZ—which means IT security is forced to allow traffic through without knowing anything about the content.

Lack of Centralized Control

Because authentication, authorization, and auditing can be applied only at individual hosts, the central security team cannot effectively monitor and enforce the use of enterprise security policies.

Given the value of your critical host data, these are significant security holes. The question is, how can you protect your data without changing host applications that have taken decades to develop? How can you move your hosts into the new world of security?

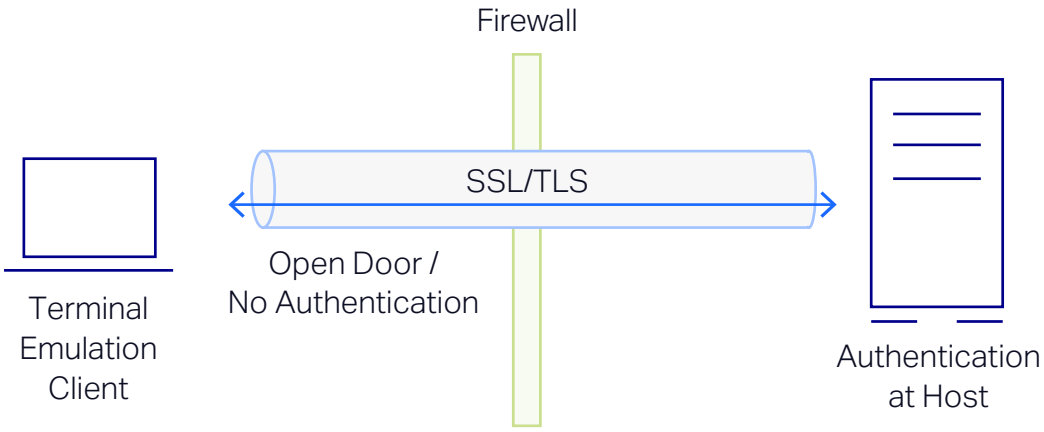

Figure 1. First-generation host security provides SSL/TLS direct-to-host encryption, but authentication doesn't happen until the connection has reached the host.

Warding off new security threats perpetuated by increasingly sophisticated fraudsters has become a way of life.

Modern Security Frameworks

Warding off new security threats perpetuated by increasingly sophisticated fraudsters has become a way of life. Unfortunately, there is no fail-safe way to get the job done. The best defense is applying layers of security, including advanced authentication and authorization technologies, to minimize risk.

For example, U.S. government IT organizations have established Public Key Infrastructures (PKIs) and adopted the use of smart cards to support personal identification standards such as PIV (FIPS 201). These types of controls are gradually being adopted by commercial entities as they seek compliance with new standards like PCI DSS, SOX, and HIPAA.

Modern IAM systems were never designed to work with heritage host systems, and vice versa. But what if there were a way to integrate the two systems—extending strong, centrally managed security to your host applications—without jeopardizing business operations? Fortunately, there is a way. It's called OpenText™ Host Access Management and Security Server (MSS).

Adding layers of security is a best-practice approach that you can carry out in phases. But the reality is that you can't have strong security without strong management. That's why organizations implement Identity and Access Management (IAM) systems. IAM systems, such as Active Directory, are a key component of modern security frameworks. They enable IT to grant access, revoke access, and audit access to enterprise data, resources, and applications from one central location.

The problem is that IAM systems do not work with your long-standing, data-rich IBM, HP, UNIX, and Unisys hosts. And there's no simple way to integrate the two systems. It's difficult, risky, and expensive to rewrite the host logic that run your company—even if you somehow find a qualified mainframe programmer who hasn't retired. It's also completely unacceptable to weaken your strong IAM credentials to match weak host logon credentials. The costs involved are just too high.

Basically, that leaves you with two separate security infrastructures. On the one hand, you have your hosts, probably managed by RACF or Top Secret. On the other, you have everything else, managed by IAM. Looming large over both infrastructures are increasingly stringent regulatory mandates for you to contend with.

Building the Host-IAM Alliance

Modern IAM systems were never designed to work with heritage host systems, and vice versa. But what if there were a way to integrate the two systems—extending strong, centrally managed security to your host applications—without jeopardizing business operations?

Fortunately, there is a way. It's called OpenText™ Host Access Management and Security Server (MSS). MSS and its add-on components work with your IAM system to centrally manage and secure host access through your OpenText™ Reflection, OpenText™ Extra!, OpenText™ InfoConnect, and OpenText™ Rumba+ terminal emulators. It's a nonintrusive solution that requires no changes to your host applications or your IAM system.

For each of the following security categories, we'll outline how modern security frameworks operate and then explain how you can integrate them with your host systems using MSS:

Centralized Authentication

How modern security frameworks operate: An IAM system enforces strong authentication and rigid security policies across the enterprise.

What MSS does: MSS includes an administrative server that leverages your IAM system to validate a user's credentials before granting host access. In other words, users can't get near the host logon screen until they've been authenticated and authorized with strong IAM credentials—proving they are who they say they are. Now you can require the same strong authentication for host access that you require for access to other systems.

MSS facilitates the integration process by supporting all common IAM systems, including Active Directory, NetIQ eDirectory by OpenText™, IBM Tivoli Directory Server, OpenLDAP, and Oracle Directory Server Enterprise Edition. It also supports a variety of authentication technologies, including Kerberos, NTLM, CRL, OCSP, PKI, and X.509 certificates used with smart cards such as CAC and PIV.

Centralized Authorization

How modern security frameworks operate: An IAM system ensures that users have access only to the resources and information necessary to do their jobs, and nothing more.

What MSS does: MSS makes it possible to extend IAM authorization schemes to host access without requiring any changes to the host or user workflow. For example, you can grant or deny access based on group or role—enabling a user to access your 3270 mainframe, but not your Unisys host. You can take authorization up a notch with the MSS security proxy. The security proxy provides a patented time-limited, digitally signed token that uses public key cryptography to prevent unauthorized users from connecting to the host.

With MSS, you can also specify what users can or cannot do. For example, you can harden terminal emulation—removing a user's ability to edit macros or locking down the connection settings for TLS 1.2.

From the MSS administrative server, it's easy to make post-install adjustments on the fly. The next time users launch a session, they'll receive the changes.

MSS facilitates the integration process by supporting all common IAM systems, including:

- Active Directory
- NetIQ eDirectory
- IBM Tivoli Directory Server
- OpenLDAP
- Oracle Directory Server Enterprise Edition

It also supports a variety of authentication technologies, including:

- Kerberos
- NTLM
- CRL
- OCSP
- PKI,
- X.509 certificates used with smart cards such as CAC and PIV

MSS Components

An administrative server and a metering server are included with your MSS license. The following add-on products provide additional, critical functionality:

MSS Security Proxy Add-On—Enforce access control at the perimeter with patented security technology.

MSS Terminal ID Management Add-On— Dynamically allocate terminal IDs based on username, DNS name, IP address, or address pool.

MSS Automated Sign-On for Mainframe Add-On— Enable users to enter their credentials just once to gain authorized access to all enterprise systems, including the mainframe.

MSS PKI Automated Sign-On Add-On— PKI-enable automated application sign on to your critical enterprise systems.

With MSS and its add-on products, you can modernize host security without changing your host applications or your IAM system.

Centralized Auditing

How modern security frameworks operate: An IAM system documents who accessed what network resources and when—arming network administrators with the data they need to fulfill audit requirements.

What MSS does: MSS uses your existing IAM system to authenticate users and authorize host access, logging all activity in a central location. This process ensures that you know who accessed what host and when. It also ensures that you have a documented paper trail when audits occur.

Encryption

How modern security frameworks operate: Data is encrypted at the start of the transmission—whether inside or outside the firewall—and decrypted upon receipt. While this process protects the data, it also prevents necessary data inspection in the DMZ.

What MSS does: MSS works with the MSS security proxy, which sits between your desktops and your hosts. The security proxy accepts SSL/TLS encrypted packets and decrypts them before they are delivered to the host. Once decrypted, packets can be monitored by intrusion detection, content inspection, and other security devices for possible attacks or data leaks.

The MSS security proxy is not like a simple SSL/TLS gateway or redirector that accepts SSL/TLS connections without first authorizing the user. Those types of solutions give intruders a free ride all the way to the host. With MSS, intruders who attempt to make an SSL/TLS connection to the host—without first being authenticated and authorized via the MSS administrative server—will be denied access at the MSS security proxy. The security proxy uses a Micro Focus (now part of OpenText) patented secure token to ensure that only authorized users get to host resources.

MSS supports encryption strengths up to 256-bit AES. It also supports cryptographic modules validated for FIPS 140-2—one of the U.S. government's top security standards. This high level of security means you can protect your host from malicious content. It also provides a framework for adding layers of security as needed.

Access to Multiple Hosts Through a Single Port

How modern security frameworks operate: Multiple backend servers can be accessed through a single listening port.

What MSS does: MSS enables you to use a single opening in the firewall (for example,port 443) to access all your hosts. You can later add other hosts without changing anything on the firewall. In addition to reducing the number of ports you need to monitor, this simplified configuration also reduces your network's attack surface.

Centralized Configuration Control

How modern security frameworks operate: IT uses an IAM system to centrally secure, manage, and deploy a wide range of application configurations across the enterprise.

What MSS does: MSS enables you to manage host-access operations from your central MSS console. You can grant or deny access based on group or role, quickly apply security updates and configuration changes to align with changing regulatory or business needs, and make post-install adjustments on the fly. In short, you can configure and lock down 100s or 1000s of desktops with ease. And you can do it on your schedule, not someone else's.

A key advantage of MSS is that it leverages your existing security investments to authorize, authenticate, and audit terminal emulation access to host systems from a central location. As a result, the practical and logistical problems associated with enforcing strong security measures at each individual backend host are significantly reduced.

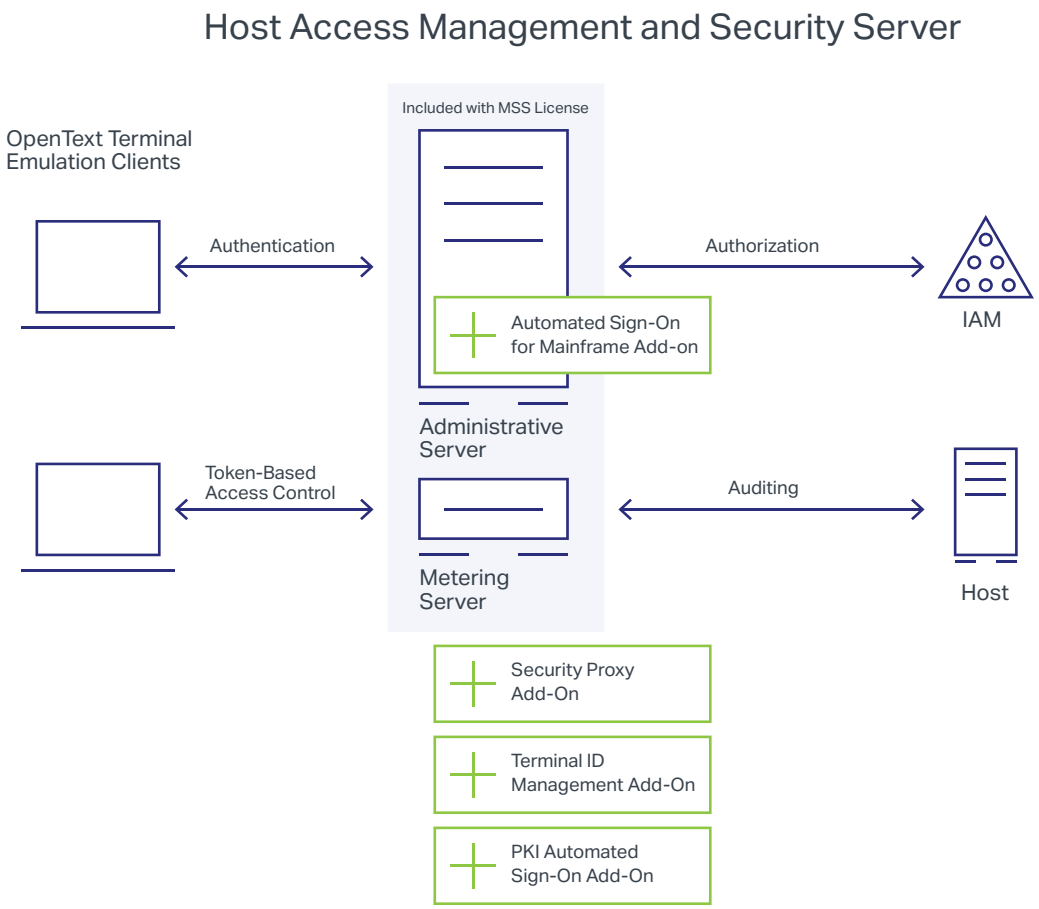

Figure 2. MSS works as an access control point in front of the host, ensuring that users are authenticated and authorized before gaining access to host resources.

Equal Protection for All

With MSS, you can finally deliver modern multilayered security to your valuable host assets without changing the host or your IAM system. By integrating these two critical enterprise systems via MSS, you can:

- Strengthen security for your critical host applications and data.
- Streamline host-access management.
- Maximize your IAM investment by extending IAM to host systems.
- Facilitate compliance with today's highest-level security mandates.
- Safely modernize host security without disrupting user workflows or business operations.

Test MSS for yourself. Download the evaluation guide at **www.attachmate.com/products/mss/mss-eval-form.html** or contact your sales representative.

Learn more at
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™