Rocket® software

Integrating Host Systems with Modern Security Frameworks

Contents

← Back to contents

Introduction

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

The host stands alone

There was a time when host systems lived in a secure world — host data traveled a protected path to and from the 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 bad actors with constantly evolving tactics. 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 an attacker 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?

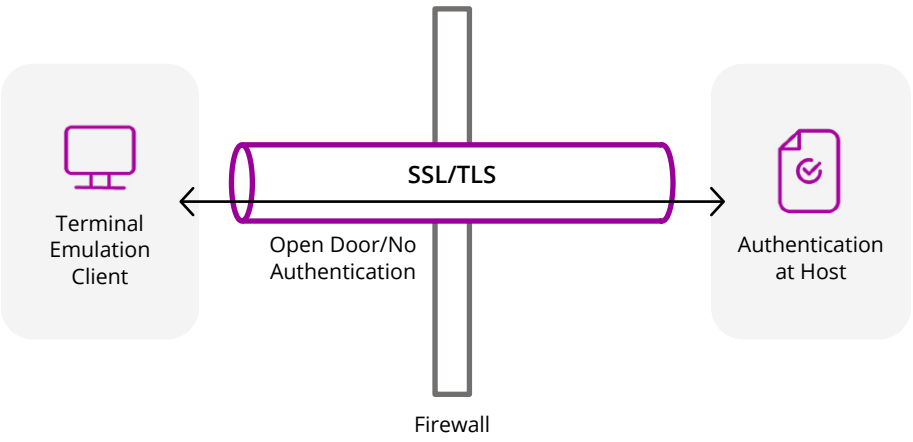

Figure 1. First-generation host security provides SSL/TLS direct-to-host encryption, but authentication doesn't happen until the connection has reached the host.

Modern security frameworks

Warding off new security threats perpetuated by increasingly sophisticated attacks 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, US 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.

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

← Back to contents

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 Microsoft Active Directory, are a key component of modern security frameworks. They enable IT to grant, revoke, and audit access, to enterprise data, resources, and applications from one central location.

The issue is that IAM software does not work with your core host systems (IBM, HP, Linux/UNIX, Unisys, and airlines). What if you could leverage your existing IAM software to ensure only authenticated and authorized users can access the host?

Building the host-IAM alliance

Fortunately, there is a way. It's called Rocket® Secure Host Access and it works with your IAM system to centrally manage and secure critical host connectivity through your Rocket terminal emulator. It's a non-intrusive solution that requires no changes to your host applications or your IAM system.

Modern IAM systems were never designed to work with heritage host systems, and vice versa. But what if there were a way to make these systems work together — extending strong, centrally managed security to your host applications — without jeopardizing business operations? Fortunately, there is a way. It's called Rocket® Secure Host Access.

← Back to contents

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 Rocket Secure Host Access:

Centralized authentication

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

What Secure Host Access does: Rocket Secure Host Access 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 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.

Rocket Secure Host Access facilitates the integration process by supporting all common IAM systems including Active Directory, OpenLDAP, Kerberos, SAML OIDC, 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 Secure Host Access does: Rocket Secure Host Access 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 Secure Host Access 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 Secure Host Access, 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, or even TLS 1.3.

From the Rocket Secure Host Access 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.

Rocket Secure Host Access facilitates the integration process by supporting all common IAM systems including Active Directory, OpenLDAP, Kerberos, SAML OIDC, PKI, and X.509 certificates used with smart cards such as CAC and PIV.

← Back to contents

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 Secure Host Access does: Rocket Secure Host Access 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 Secure Host Access does: Rocket Secure Host Access works with the 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 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 Secure Host Access, attackers who attempt to make an SSL/TLS connection to the host — without first being authenticated and authorized via the Secure Host Access administrative server — will be denied access at the security proxy. The security proxy uses a Rocket patented secure token (formerly a micro focus product) to ensure that only authorized users get to host resources.

Rocket Secure Host Access 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.

Rocket Secure Host Access uses your existing IAM system to authenticate users and authorize host access, logging all activity in a central location.

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 Secure Host Access does: Rocket Secure Host Access 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 Secure Host Access does: Rocket Secure Host Access enables you to manage host-access operations from your central 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 manage host access for all your desktops from a single point with ease. And you can do it on your schedule, not someone else's.

A key advantage of Secure Host Access 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.

Rocket Secure Host Access

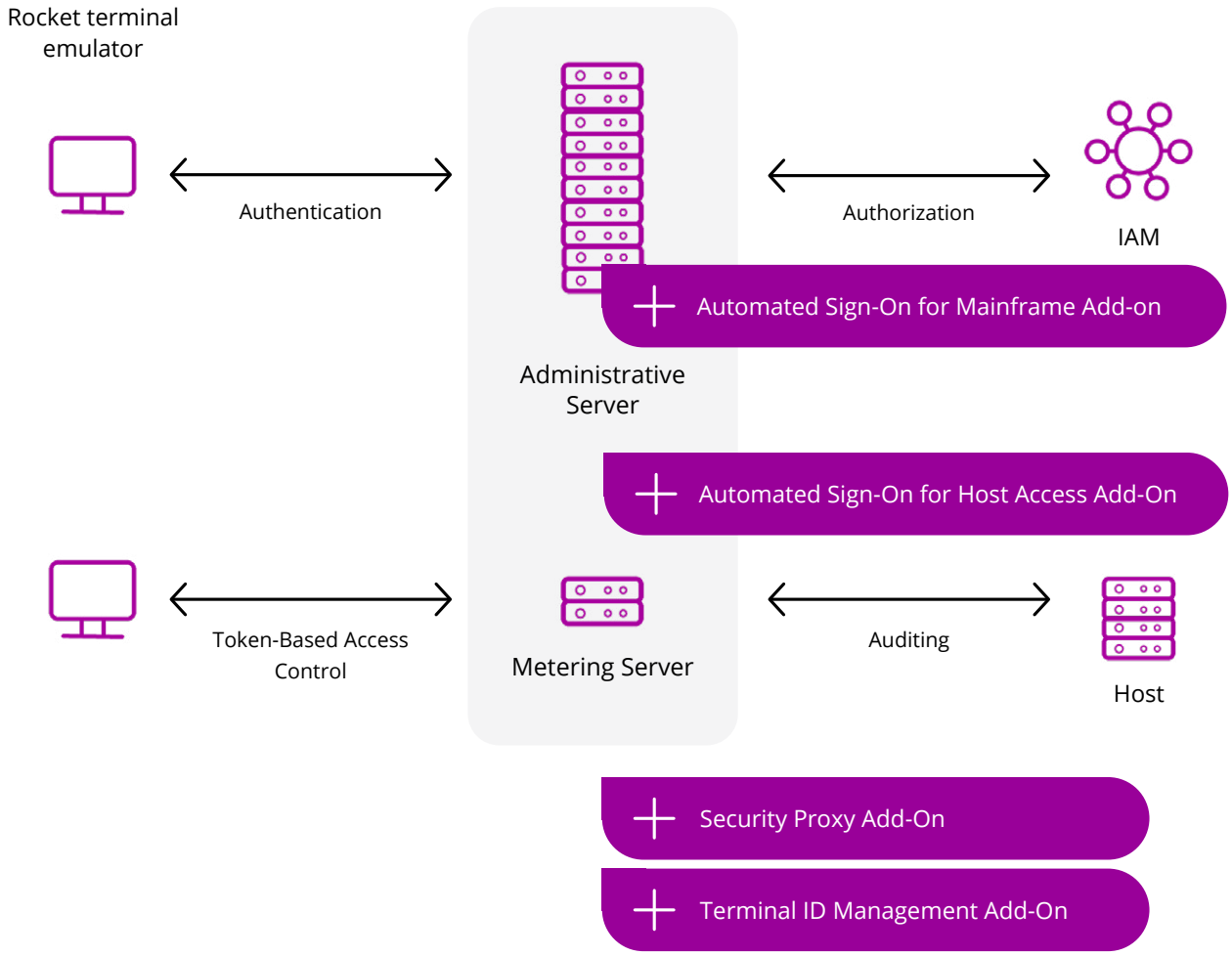

Figure 2. Rocket Secure Host Access works as an access control point in front of the host, ensuring that users are authenticated and authorized before gaining access to host resources.

← Back to contents

Equal protection for all

With Rocket Secure Host Access, 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 Secure Host Access, 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.

Get started now.

Speak to an expert

* formerly Micro Focus® products

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X.

Modernization. Without Disruption.™

Visit RocketSoftware.com ›

Learn more

Rocket software

MAR-12520_QWP_IntegratHostSysModernSecurityFrameworks_V1