Rocket® software

Rocket® Secure Host Access

Security-first green screen access you don't have to think about

Contents

Rocket® Secure Host Access

If you have a terminal emulator providing users access to critical applications, you likely don't think about how secure it is.

However, security incidents involving stolen or compromised credentials are on the rise. At the same time, major regulations — such as NY DFS Cybersecurity Regulations, the California Consumer Privacy Act (CCPA), and the Digital Operations Resilience Act (DORA) — are being implemented. Now is the time to secure your green screen access.

Whether an insider threat or growing cybersecurity regulations top your list of concerns, you need to be prepared. Extending your enterprise authentication and authorization to your terminal emulation process is a good place to start.

Rocket® Secure Host Access is a security-first terminal emulator that enables you to integrate green screen access with your existing identity and access management (IAM) solutions to achieve true defense in depth. Partner with Rocket Software — the only organization committed to securing access to host applications.

Benefits

- Keep your organization secure and compliant with solutions that enable host access while protecting against evolving security threats and meeting compliance regulations, such as HIPAA, DORA, PCI-DSS, GDPR, and more.

- Get the support you need to simplify your host access through centralized management, whether you require desktop or web emulation or a hybrid of both.

- Ensure that access to your data and applications remains secure with modern security encryption methods, such as TLS 1.3, SSH, elliptic curve cryptography (ECC), and more.

- Support multifactor authentication (MFA) and single sign-on (SSO) to the host without user interaction to eliminate a potential fault point in the process.

- Continue to derive value from your existing IAM systems by integrating them with the Rocket solution to secure all high-value targets, including your mainframe and other host systems.

Users keep your business running, but they can also be your weakest link

Cybersecurity concerns are everywhere these days. High-profile cyberattacks regularly make headlines, so even those with no sense of the technical world recognize adversaries hunting for valuable data. However, many people assume that mainframe-based organizations and those that rely on this host technology are secure.

We have firewalls, and we use strong passwords and multifactor authentication (MFA) for the applications we touch daily, but what about the green screen terminal emulators we use to access applications on those hosts?

It's time to think about securing green screen access with the same rigor we apply to applications and systems we have on the front end. If services like Active Directory (AD) handle authentication and authorization, and tools like Okta® ensure MFA and single sign-on (SSO), why not employ the same scrutiny on the back end? Eight-character, case-insensitive passwords for the green screen access are no longer good enough.
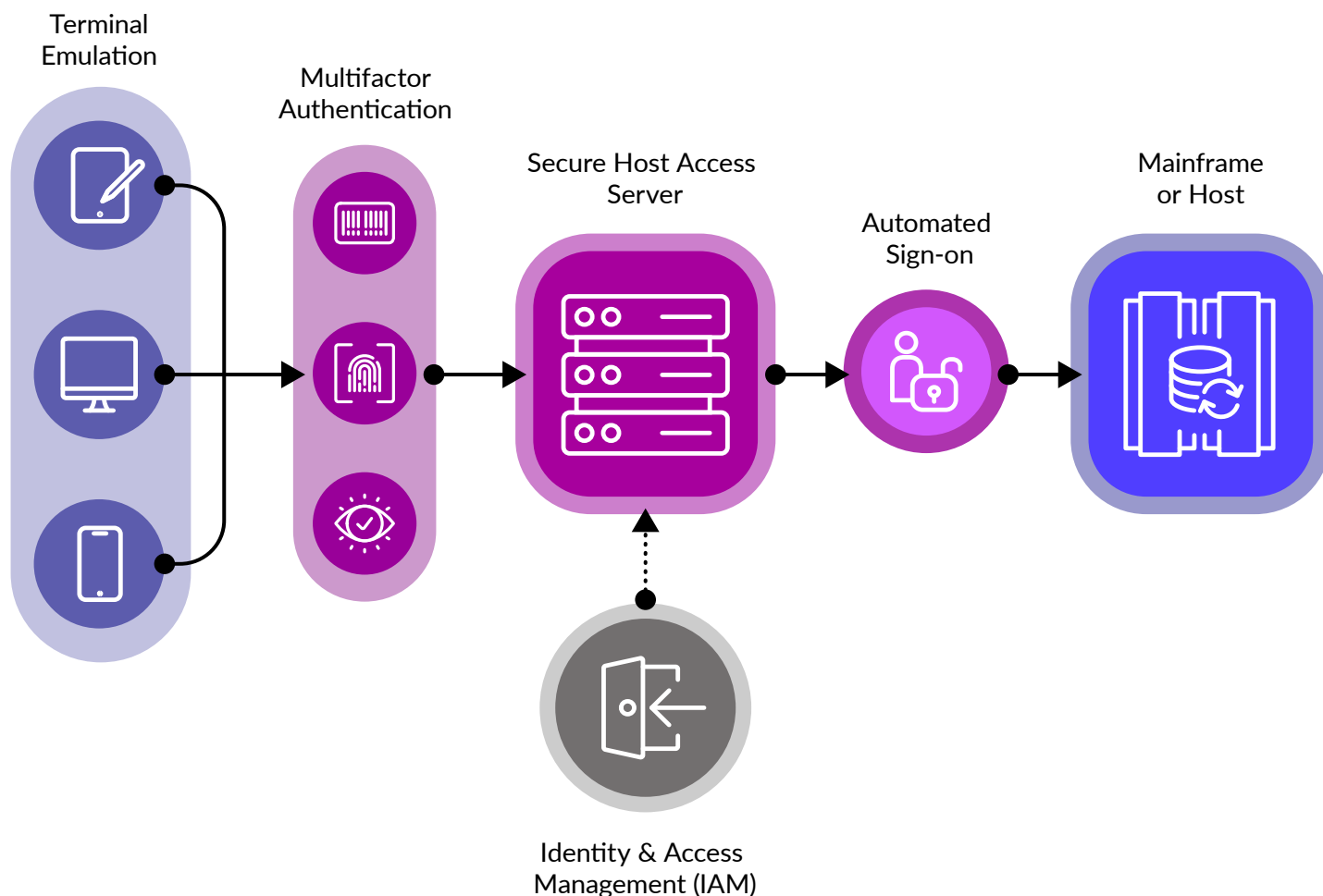
The average cost associated
to a cyber event is

$4.88M

Defense-in-depth for your security and compliance needs

Even if security isn't your daily focus, it's important to consider its role in regulatory compliance. Whether you're addressing well-established mandates like HIPAA or GDPR, or preparing for newer regulations like DORA and the NY DSF Cybersecurity requirements, maintaining a secure environment — and being able to prove it — is critical. The cost of non-compliance is daunting.

Security breaches are costly — globally, the average cost of a security breach is $4.88 million US — and you can't afford the lost revenue and downtime of recovering from a cyber event. While the cost of compliance can be vast, averaging at upwards of $5 million, the total cost of non-compliance is more than $14 million, according to the Ponemon Institute. You need to mitigate the risk of auditory fines with a security-first solution that extends your existing identity and access management (IAM) solutions to the mainframe for complete, end-to-end IT security. For true defense in depth, it's important to be able to:

- Lock down your terminal emulator

- Ensure redaction

- Accurately authenticate and authorize users based on company policies

- For the NYDFS cybersecurity regulations, penalties are as follows:

  ° $2500/day of noncompliance.

  ° $15K/day of noncompliance if it's determined to be a "pattern."

  ° $75K/day of noncompliance if the violations were committed "knowingly and willfully."

  ° Enforcement actions show monetary penalties typically range from $4.5M-$5M.

Terminal
Emulation

Multifactor
Authentication

Secure Host Access
Server

Automated
Sign-on

Mainframe
or Host

Identity & Access
Management (IAM)

Phishing-resistant, password-less, security-first host access

Do more with the cybersecurity infrastructure you already have in place. With Rocket Secure Host Access, you can extend the tools you already use to authenticate and authorize users on the front end to secure green screen access to host applications.

Rocket Secure Host Access offers a security-first host access solution that starts with your terminal emulator to mitigate the risk of threats to your mainframe and other host systems as well as enhance/simplify regulatory compliance support with a layered security strategy. We offer the industry's only solution for phishing-resistant, password-less, secure access to host applications, whether on the desktop or on the web. With Rocket Secure Host Access, you can easily integrate your existing identity and access management (IAM) solutions to ensure end-to-end protection and defense in depth.

Rocket Secure Host Access is a tiered terminal emulation solution that starts as a desktop-based emulator and can scale up to add layers of security based on your requirements.

Rocket® Secure Host Access Pro

- Rocket® Secure Host Access Pro is the first tier of the solution. It offers full desktop-based host application access with the latest TLS 1.3 and SSH encryption technology.

Rocket® Secure Host Access Enterprise

- Rocket® Secure Host Access Enterprise is the second tier of the Secure Host Access solution. With this tier, you can easily integrate with your corporate IAM for centralized management and extend MFA, SSO, and terminal ID management support to your green screen.

Rocket® Secure Host Access Anywhere

- Rocket® Secure Host Access Anywhere is the top tier of the Secure Host Access solution, and it provides robust security features for both desktop- and web-based host application access.

We're with you every step of the way

With Rocket Software, you have a partner dedicated to keeping your host application access secure, no matter where you are on your modernization journey. Cyber threats are evolving, and compliance rules are getting stricter. That's why securing your mainframe is so important, just like the rest of your environment. And protecting access to your critical green screen apps doesn't have to be a solo mission. We're here to help.

Speak to an Expert

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.

Visit RocketSoftware.com >

Rocket®software

Modernization. Without Disruption.™