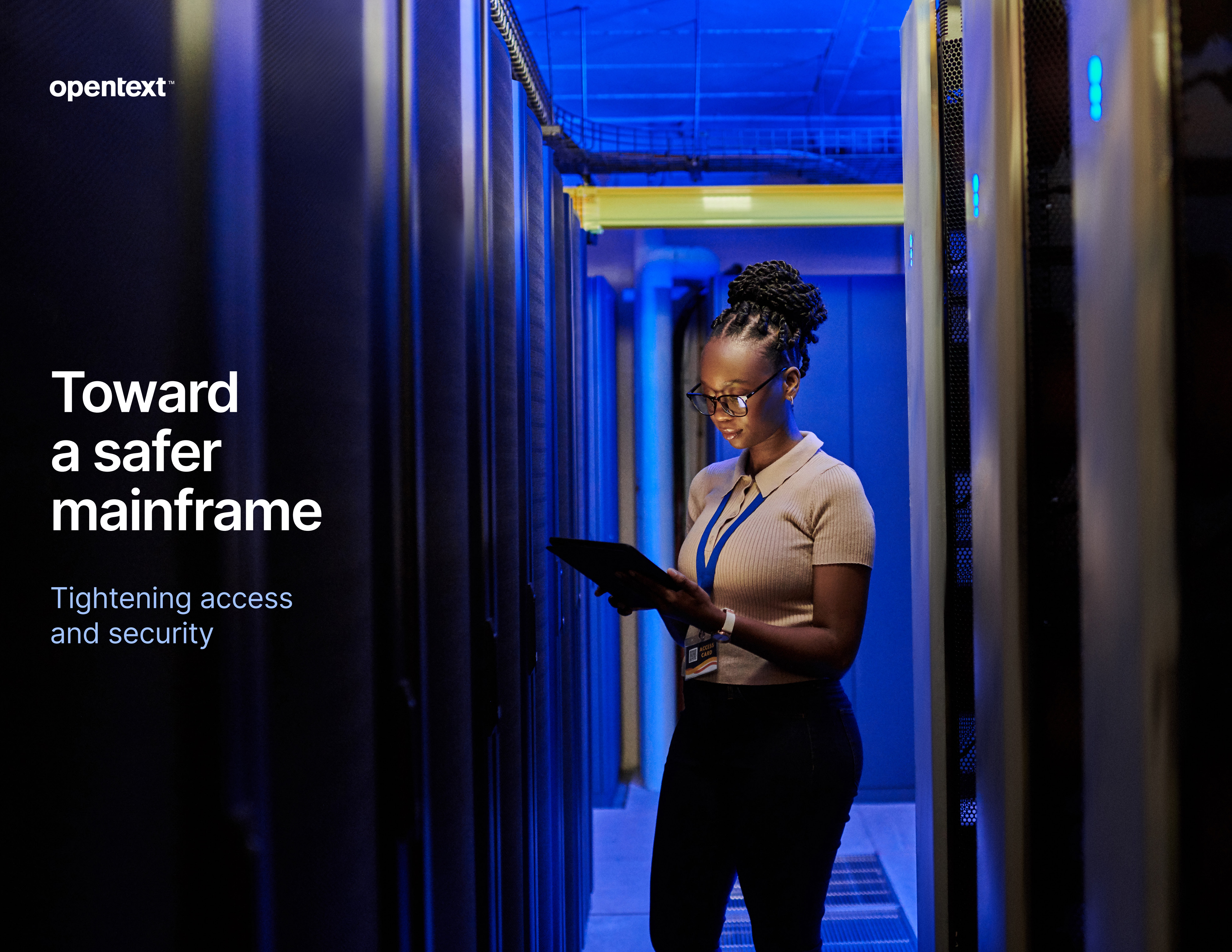
opentext™

Toward a safer mainframe

Tightening access and security



The mainframe is evolving to be an integral part of a rapidly evolving connected, digital and hybrid IT world.

Which means the platform must be as agile, fit for purpose, open to innovation and, crucially, as secure as other systems. While the mainframe may have security built in, there are challenges with more mature installations and the external end points accessing them.

To remain relevant, and a cornerstone of the enterprise, the mainframe must meet new demands for device connectivity and security. But what does that look like? This e-book explains how organizations can protect their mainframe systems by using every facet of enterprise-level security, including access control, data privacy, and endpoint hardening.

Why mainframe security matters

The mainframe remains business critical. According to IBM, 71 percent of Fortune 500 companies now use mainframes.[1] A surprising 90 percent of credit card transactions are processed through a mainframe, while the mainframe[2] manages 68 percent of IT workloads worldwide, but only accounts for 6 percent of IT costs.[3]

Despite all this, many organizations struggle to extend enterprise security to the mainframe. According to Forrester, 85 percent of companies say mainframe security is a top priority, yet 67 percent admit they only “sometimes” or “rarely” factor security into mainframe environment decisions.

Regulatory requirements demand additional security for the mainframe, as it is a crucial component of the enterprise. These regulations include Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA). These regulations protect individuals and their data, and demand unprecedented levels of security.

PCI DSS: Mandates multifactor authentication (MFA) in certain scenarios regarding cardholder data, encryption, and data masking, as well as specifics around applying security patches.

GDPR: Requires data security in transit and at rest, and at its core, requires that personally identifiable information is only accessible by those with a legitimate reason to do so.

CCPA: Shares much of the same foundation as GDPR.

85%

of companies say mainframe security is a top priority.[4]

67%

admit they only “sometimes” or “rarely” factor security into mainframe environment decisions.[4]

71% of Fortune 500 companies use mainframes.[1]

90% of credit card transactions are processed through a mainframe.[2]

[1] Precisely, 10 Mainframe Statistics That May Surprise You. (2022)

[2] Ibid

[3] Ibid

[4] Forrester and Key Resources, Inc., Don’t Let Mainframe Security Complacency Leave Your Critical Customer Data at Risk.

Sensitive data needs strong security

In addition to regulatory mandates, the uptick of breaches also proves the need to secure those systems holding sensitive data. The most common breach is through compromised account credentials. Making access harder is the key to breach prevention.

Multi-factor authentication (MFA) is one of the best ways to prevent unauthorized access, because the password alone will not be enough to gain access. Data privacy through encryption, used in conjunction with data masking, ensures sensitive data stays secure because even if systems are compromised, encrypted and masked information will not be visible.

More than ever before, organizations must extend enterprise-level security controls to the mainframe. At a minimum, these controls include:

- Access control through authentication and authorization
- Data privacy through access control and masking/encryption
- Endpoint hardening through securing mainframe access points
- Zero footprint access through secure cloud entry

Let us look at these controls in more detail.

Access control

Access control combines authentication and authorization.

Authentication proves who you are by querying what a user knows (for example, a user ID and password), what they have (perhaps a smartcard or chip), and what they are (biometric indicators such as a fingerprint or retina scan). The more factors, the stronger the authentication.

Authorization gives users access to only applications and data they have legitimate reason to access, based on their role in the organization (the principle of least privilege).

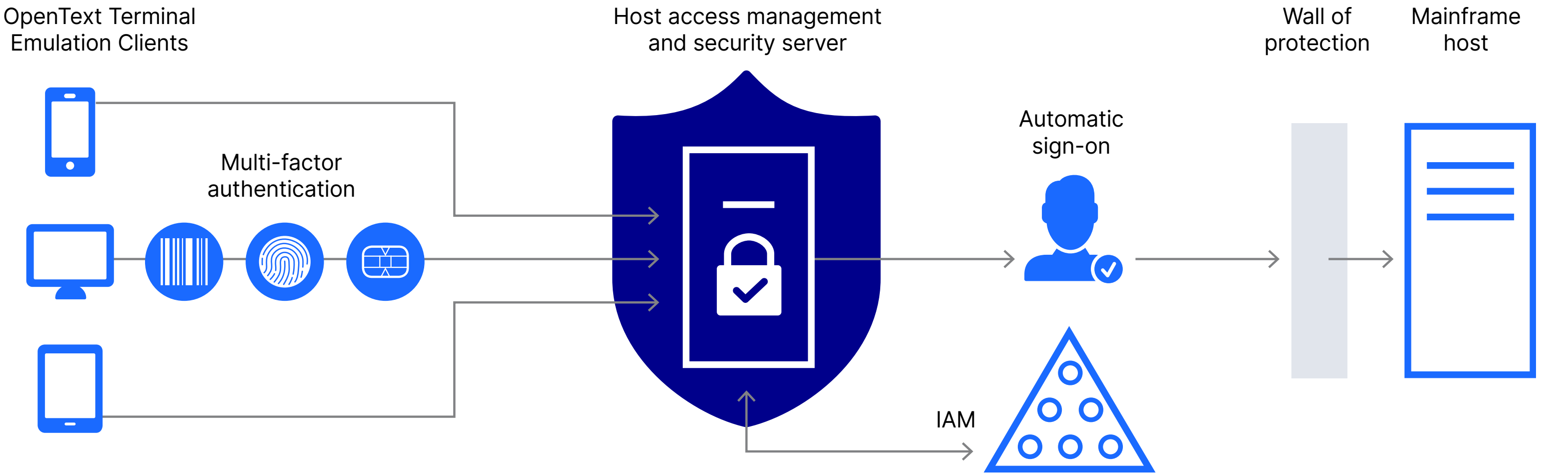
In mainframe organizations, difficulty and cost often prevent access control from integration with corporate security frameworks, typically the stronger security requirements of identity and access management (IAM) systems. Instead, it is a separate activity often implemented through RACF®, ACF2, and Top Secret. Many organizations still use eight-character passwords for mainframe access.

While many enterprises are implementing MFA, the strongest form of authentication, mainframes are either not included in the MFA plan or mainframe MFA is separate from the enterprise.

Organizations should consider an MFA platform that delivers MFA across the enterprise, including the mainframe.

Another way to secure the mainframe is by leveraging IAM in the enterprise to enable or deny access, so the organization can use existing enterprise access security controls with the mainframe. This makes IAM the primary control of who gets in and what they get access to.

Integrating IAM with the mainframe


OpenText Terminal Emulation Clients
Multi-factor authentication
Host access management and security server
Automatic sign-on
IAM
Wall of protection
Mainframe host

Data privacy

Data privacy dovetails neatly with access control and is essential to securing mainframe data. Organizations should be looking at their data privacy options to ensure mainframe data integrity. There are a few options to protect your sensitive information.

First, only allow as much access as a user's role requires and protect your data either using encryption, which secures data in transit and at rest, and masking, which hides viewable data.

However, as mainframe applications often pre-date modern security mandates, such as PCI DSS and the Health Insurance Portability and Accountability Act (HIPAA), and these applications can be difficult and costly to update, sensitive data is probably viewable by every mainframe user.

Encryption

Encryption encodes data in transit so that only authorized parties can decode it in order to access it. Typical encryption technologies for mainframe data include TLS and SSH, and encryption protocols often need upgrading to counter security vulnerabilities.

Redaction

Masking or obscuring any fixed or variable data field on the mainframe can hide data at the presentation level. Redaction should be role based, according to least privilege. Doing this requires a complete and universal understanding of what data is sensitive.

Examples include the primary account number for credit card data, and any information that identifies the individual to whom it applies. Redaction replaces some of that data with random characters or dummy information, breaking the link to a specific identity.

Used in conjunction with encryption, redaction is another option for ensuring mainframe data security.

Endpoint hardening

Endpoint hardening describes the process of helping prevent attacks by strengthening the endpoints (devices) from which the user has mainframe access. It reduces the “surface of vulnerability” by installing the latest security patches and configuring operating systems and applications according to least privilege principles, policies, and standards.

In mainframe organizations, the key application requiring endpoint hardening is the terminal emulator, or similar host access software. Owners must lock down terminal emulation, as not all users need to create new sessions, edit macros or connect to unauthorized systems.

In the new era of cyber security, terminal emulators need to be controlled. Centralized management of host access software simplifies locking down the emulator and applying the necessary security configuration changes on demand.

The faster a security patch rolls out, the quicker a threat is nullified. However, promptly applying patches for every individual desktop device is more complicated and time-consuming than using a server-based host access solution.

Secure zero-footprint access

In addition to these controls, moving to a secure zero-footprint host access solution that can be deployed in the cloud, should be considered as part of an overall mainframe security strategy. In fact, according to BMC's 2019 Mainframe Market Survey, 45 percent of mainframe organizations see implementing cloud technologies as a priority.

Centrally managed, browser-based host access enables swift configuration, deployment, and updates. It offers terminal emulation functionality to end users from a single central location in either the private or the public cloud. Leveraging the cloud increases availability, scalability and performance, improves security, and reduce costs for most applications in the organization, including host access.

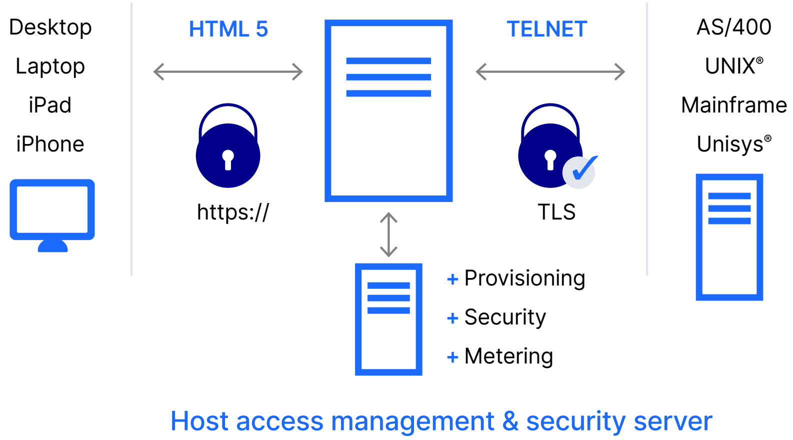
Put out your JRE fires with HTML5 emulation

Why does this matter?
As we know from experience, circumstances can compel organizations to pivot from managing an in-office to a remote workforce. Almost overnight, they may need to scale remote workers and ensure many of those users have access to host applications.

Administration of host access in a cloud environment is centralized and integrated with the corporate user directory, so provisioning, managing, and deploying secure host access is both easy and— because it is part of the overall enterprise security plan—secure.

For organizations looking at zero-footprint host access on premises, this solution can integrate with an IAM system, enabling you to leverage enterprise authentication credentials to authorize or deny mainframe access. This integration delivers on the principle of least privilege by ensuring users only have access to the mainframe systems and data they need to do their job. Enterprise-level authentication strengthens security around systems that still use eight-character passwords for mainframe access.

OpenText host access for the cloud



45% of mainframe organizations see implementing cloud technologies as a priority.

Defense in depth

To be secure in any organization, you should follow a defense in depth approach. This is the name we give to the coordinated use of multiple security controls to protect the information in the enterprise. The strategy follows the military principle that it is harder for an enemy to defeat a complex and multi-layered defense system than penetrate a single barrier.

In summary, no silver bullet will protect the enterprise from a breach. However, a multilayered defense plan, which includes the controls we have outlined in this e-book, can help secure the mainframe and the data on it.

As a reminder, at a minimum these controls include access control (authentication and authorization), data privacy (encryption and redaction), and endpoint hardening (terminal lockdown and patch rollouts). It is worth noting these security controls work better together to "defend in depth.”

What to do now

The security challenges may seem daunting. Implementing everything outlined here may feel overwhelming. However, the mainframe must be secure.

So, what should you do?
The best thing for any organization is to do something. Take any one, or more, of these controls and implement it, or them, sooner rather than later.

For the risk-averse enterprise, choosing a vendor with mainframe evolution at its heart, with many R&D millions invested in mainframe security technology, is the logical choice.

OpenText has both the experience and portfolio to meet your mainframe security needs.

Learn more now:
View more valuable content to guide you in meeting your mainframe security needs.

opentext™

The best thing for any mainframe organization is to do something.

Take any one, or more, of these controls and implement it, or them, sooner rather than later.