FULCRUM biometrics
— a Fujitsu company —

Using bioLOGIN™ to comply with Cyber Security Insurance MFA requirements

www.fulcrumbiometrics.com

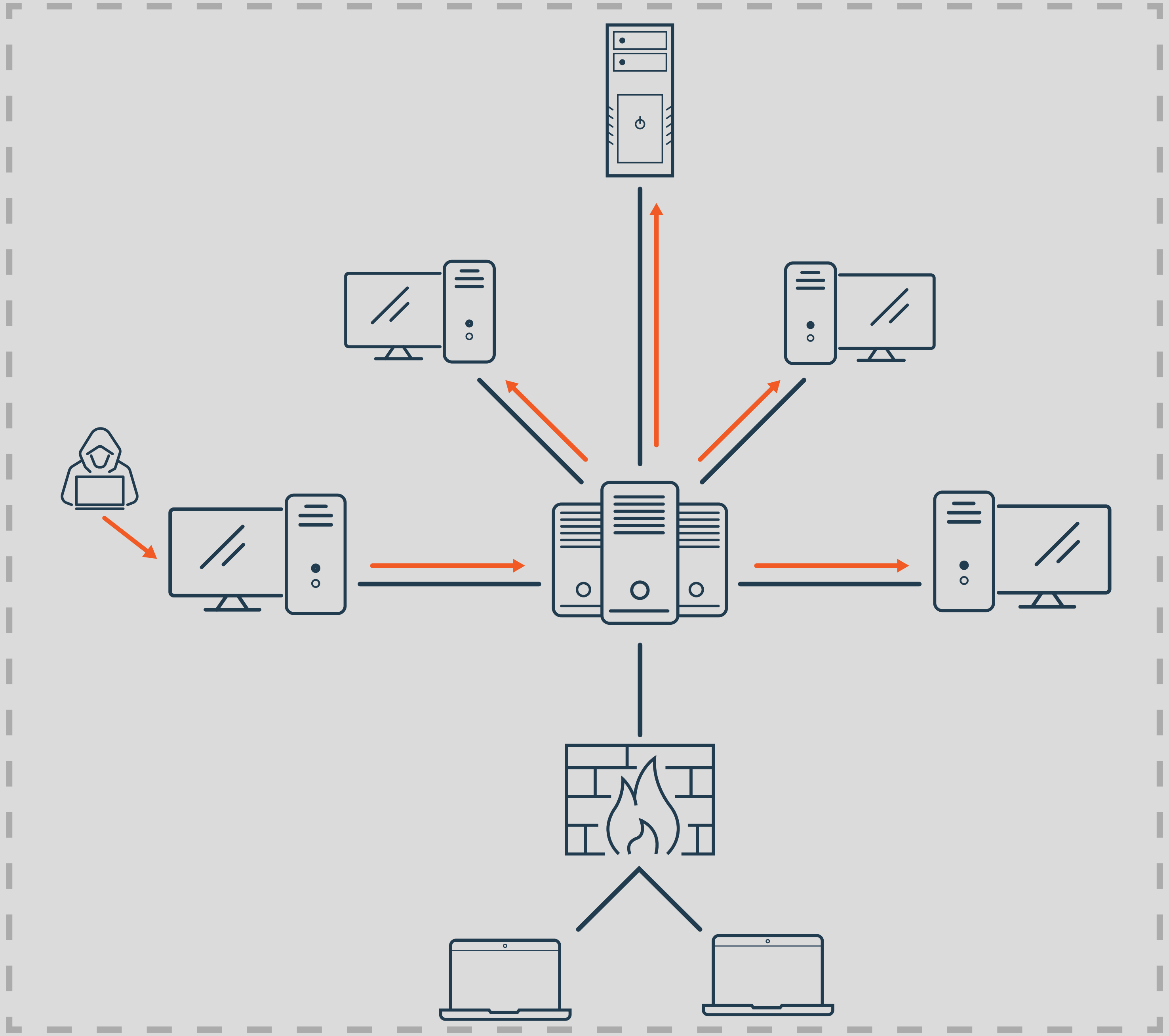
Preamble

The bioLOGIN™ server is designed using modern cloud-based technologies. The server can be deployed in a dedicated hosted environment on-premise thus ensuring that your organization's critical identity data never leaves your trusted network. As your organization grows, the bioLOGIN server capabilities can be easily scaled up just by adding additional servers in a load-balanced environment. Failover and disaster recovery protection can be deployed using additional bioLOGIN servers inside (or outside) your network. The bioLOGIN server makes it simple to deploy identity governance, provisioning, administration, and auditing features in your organization.

> "Insurers rarely provide a substantial discount based on a single security control, preferring to assess the combination of controls a company deploys against cyber threats in addition to the company's industry, size, and specific risks. Rather, enacting MFA will benefit your insurance program in two potential ways: Reducing your claims activity, which over the long term can significantly improve your insurance pricing; and, qualify your company for cyber insurance quotes from multiple carriers, ensuring competition for your business that will produce favorable terms."

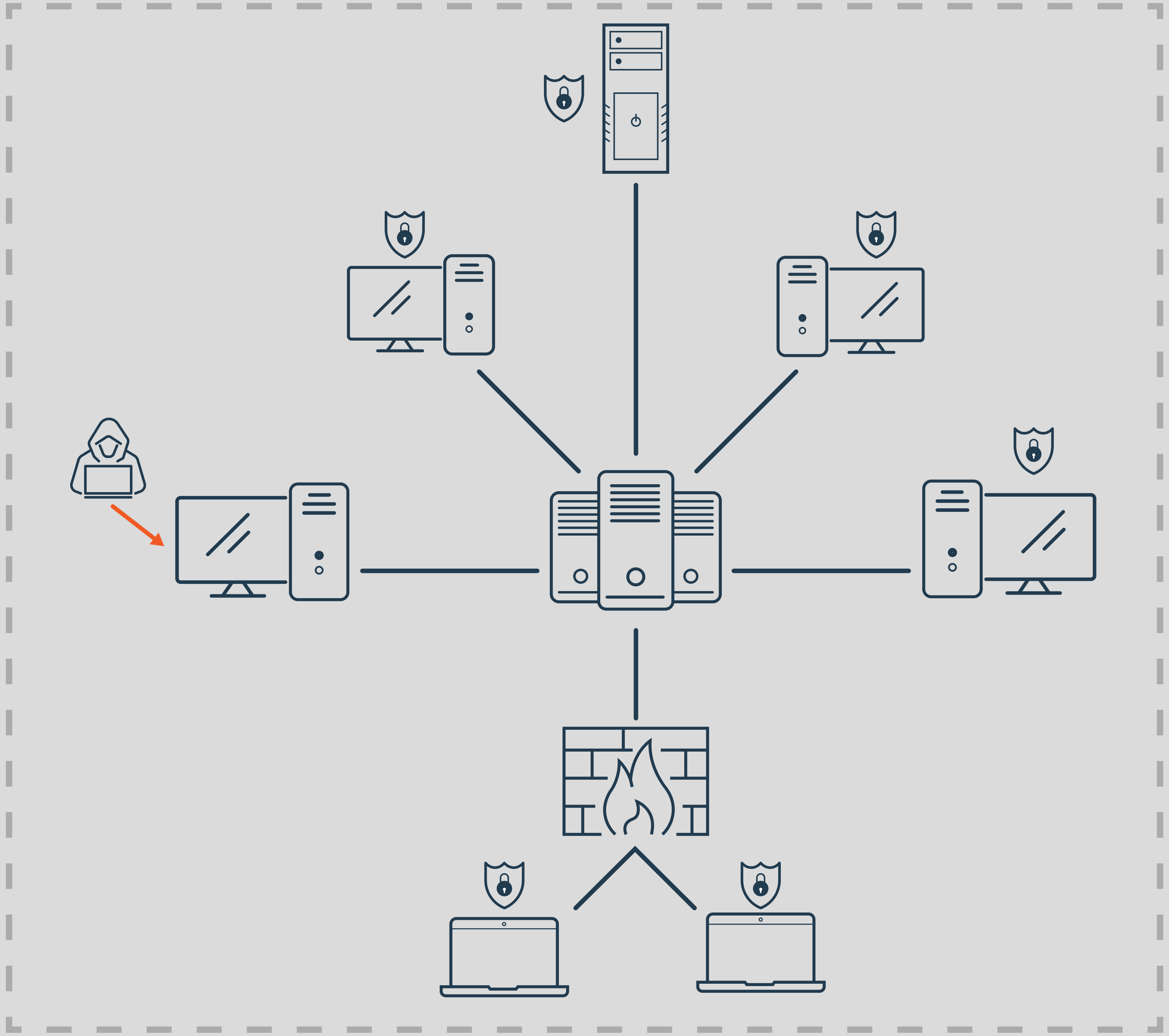
...Dan Burke, senior vice president and national cyber practice leader at Woodruff Sawyer

Unprotected passwords – the weak link to cyber threats



Criminals of cyber threats use various strategies targeted at individual employees to try to gain broader access to your corporate resources. These can include phishing, password spraying, and credential stuffing (to name a few) to get these user's passwords. It requires one compromised password to bring an entire network down.

With MFA all nodes are protected from cyber threats



MFA is a security policy that requires more than one method of authentication. It means that this layer of security combines two or more independent credentials instead of the usual username and password. Implementing MFA helps to ensure logins to information are legitimate and adds layers of protection. This makes it harder for hackers to access data.

Where Do Cyber Insurers Want to See MFA Deployed?

1. For all employees when accessing email through a website or cloud-based service to reduce the potential for access and control of corporate email accounts. With unauthorized access to a corporate email account, an attacker not only has access to sensitive data contained in email; the attacker also likely has the ability to perform self-service resets of passwords that protect other services like your corporate Active Directory and desktop logins.

2. For remote access to the network provided to employees, contractors, and third-party service providers to reduce the potential for a network security breach caused by a cracked, lost, or stolen password outside of your organization.

3. For the following, including such access provided to third-party service providers:

   a. All internal and remote administrator access to directory services (Active Directory, LDAP, etc.)

   b. All internal and remote administrator access to network backups

   c. All internal and remote administrator access to network infrastructure components (switches, routers, firewalls)

   d. All internal and remote administrator access to the organization's endpoints/servers

Multi-Factor Authentication (MFA) Implementation Best Practices

Make the MFA process easy to deploy and manage –

The way to make the practice of MFA sustainable at your organization is to make it easy for your IT team to deploy and manage. You should ideally look for solutions that will let you deploy MFA easily across all users. You should choose an MFA solution that gels well with your existing infrastructure, without the need to 'activate' it individually on every working system. Most importantly, the MFA solution must have a unified dashboard for administrators to quickly assess user queries and respond to problems if any.

Provide a Variety of Authentication Factors –

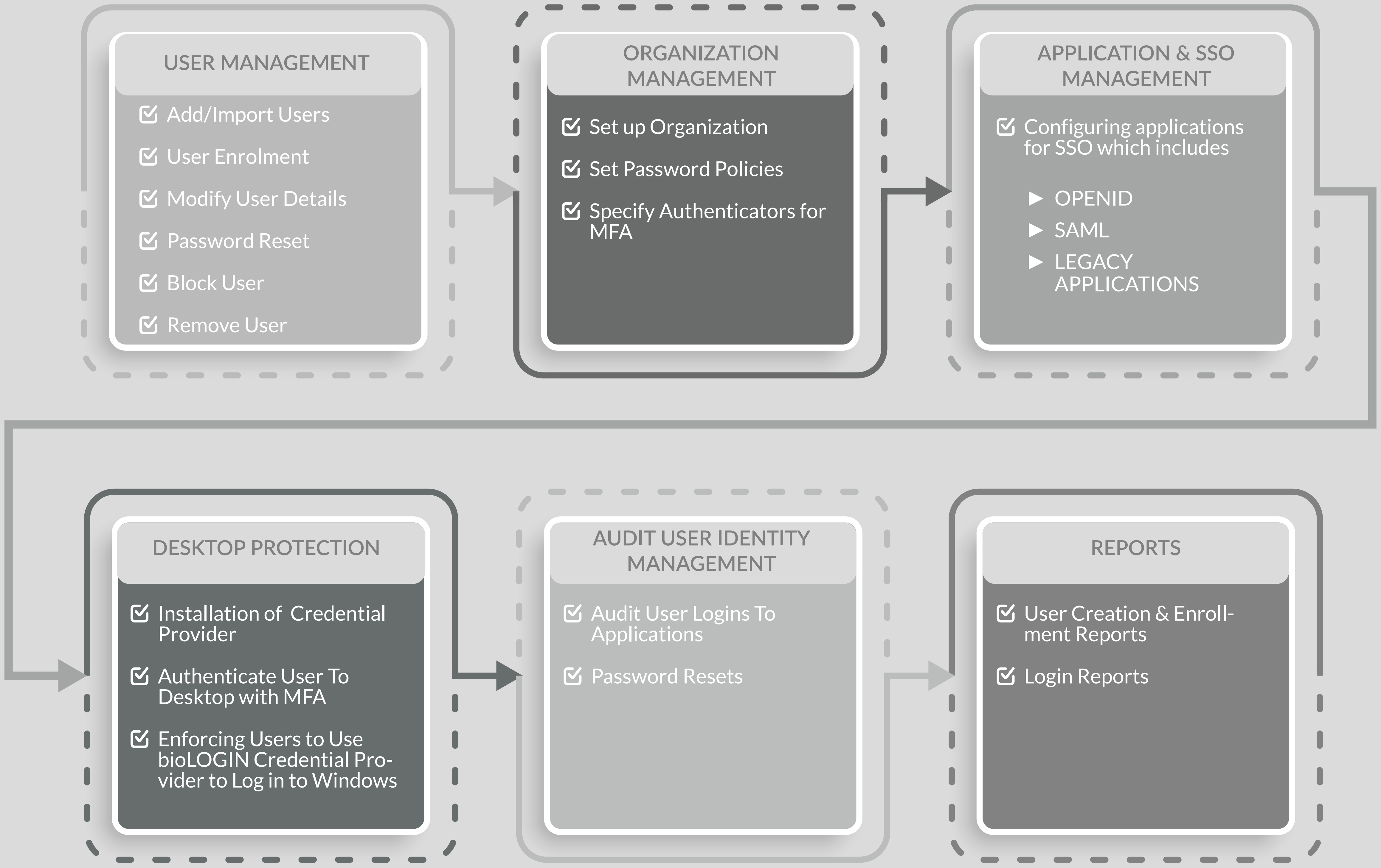
User experience is central to the success of your MFA deployment, so user convenience should remain at the forefront even as MFA helps your organization with security. The user experience of MFA can benefit from having a range of authentication methods available for users to choose from. These can include a combination of biometrics, such as fingerprint, retina scans, and facial recognition, or other options, such as hardware tokens, SMS/Text messages, call/ email verification, security questions, soft tokens, etc.

Implement MFA Across the Enterprise –

The MFA solution you opt for needs to be scalable so it can be deployed across your enterprise and grow as your business does. Deploying MFA in silos is an exercise in futility and you should take care to ensure that all your access points are covered under MFA. This also includes all workloads in the cloud. Your security practices need to be consistent across the organization with special care devoted to MFA for remote network access for distributed employees and business partners in today's work environment. Your MFA deployment should ideally cover all end users (including privileged users), cloud and on-premises applications, VPN, server logins, and privilege elevation.

Achieving MFA compliance through fast and easy deployment process ...Cont'd

Deployment of bioLOGIN MFA provides a fine-grained approach to ensure strict adherence to access policies. Each component has been designed such that the functionalities cover all aspects of Multi Factor Authentication.



USER MANAGEMENT

- ☑ Add/Import Users
- ☑ User Enrolment
- ☑ Modify User Details
- ☑ Password Reset
- ☑ Block User
- ☑ Remove User

ORGANIZATION MANAGEMENT

- ☑ Set up Organization
- ☑ Set Password Policies
- ☑ Specify Authenticators for MFA

APPLICATION & SSO MANAGEMENT

- ☑ Configuring applications for SSO which includes
  - ▶ OPENID
  - ▶ SAML
  - ▶ LEGACY APPLICATIONS

DESKTOP PROTECTION

- ☑ Installation of Credential Provider
- ☑ Authenticate User To Desktop with MFA
- ☑ Enforcing Users to Use bioLOGIN Credential Provider to Log in to Windows

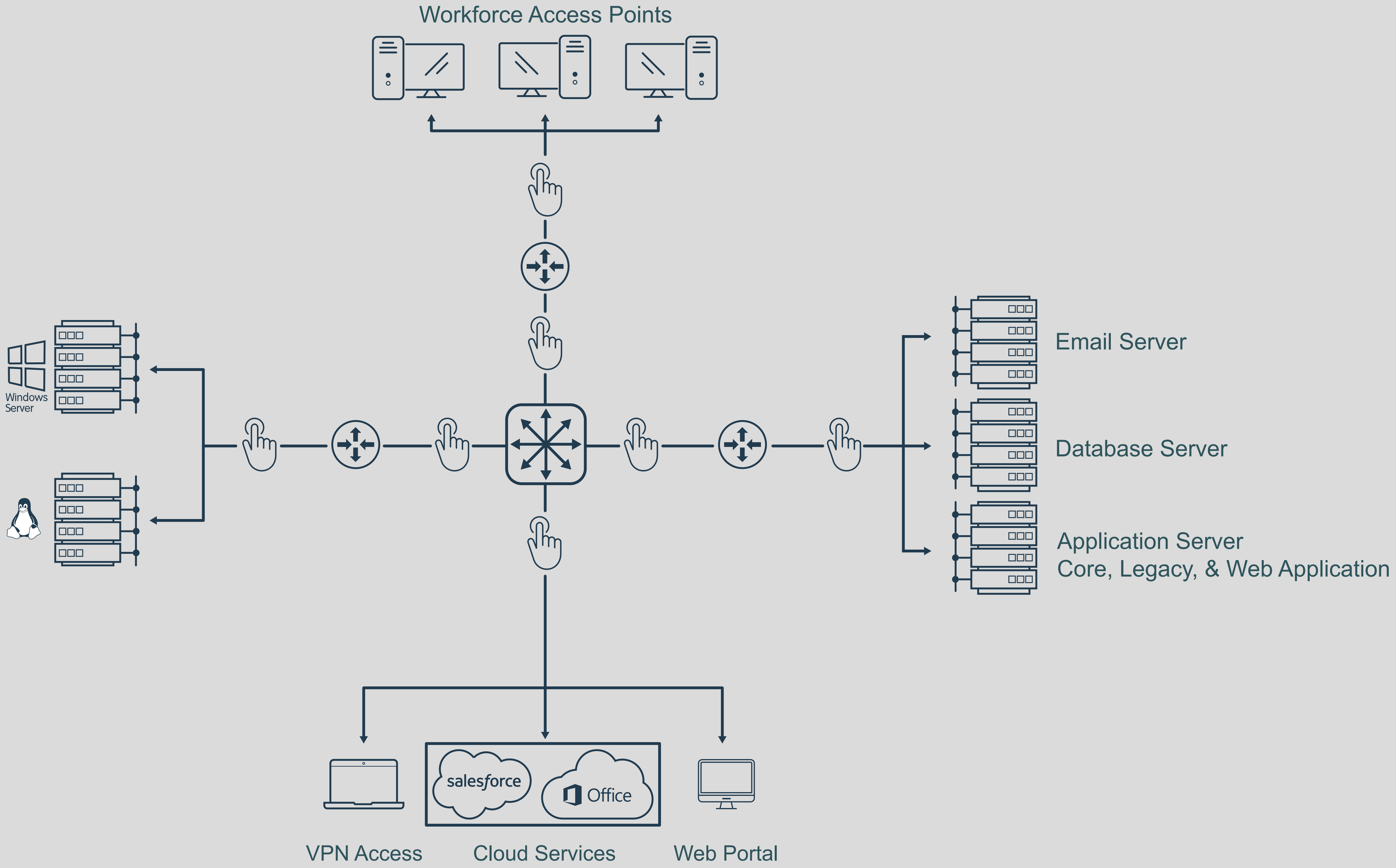
AUDIT USER IDENTITY MANAGEMENT

- ☑ Audit User Logins To Applications
- ☑ Password Resets

REPORTS

- ☑ User Creation & Enrollment Reports
- ☑ Login Reports

bioLOGIN MFA Solution for Enterprise-wide Security

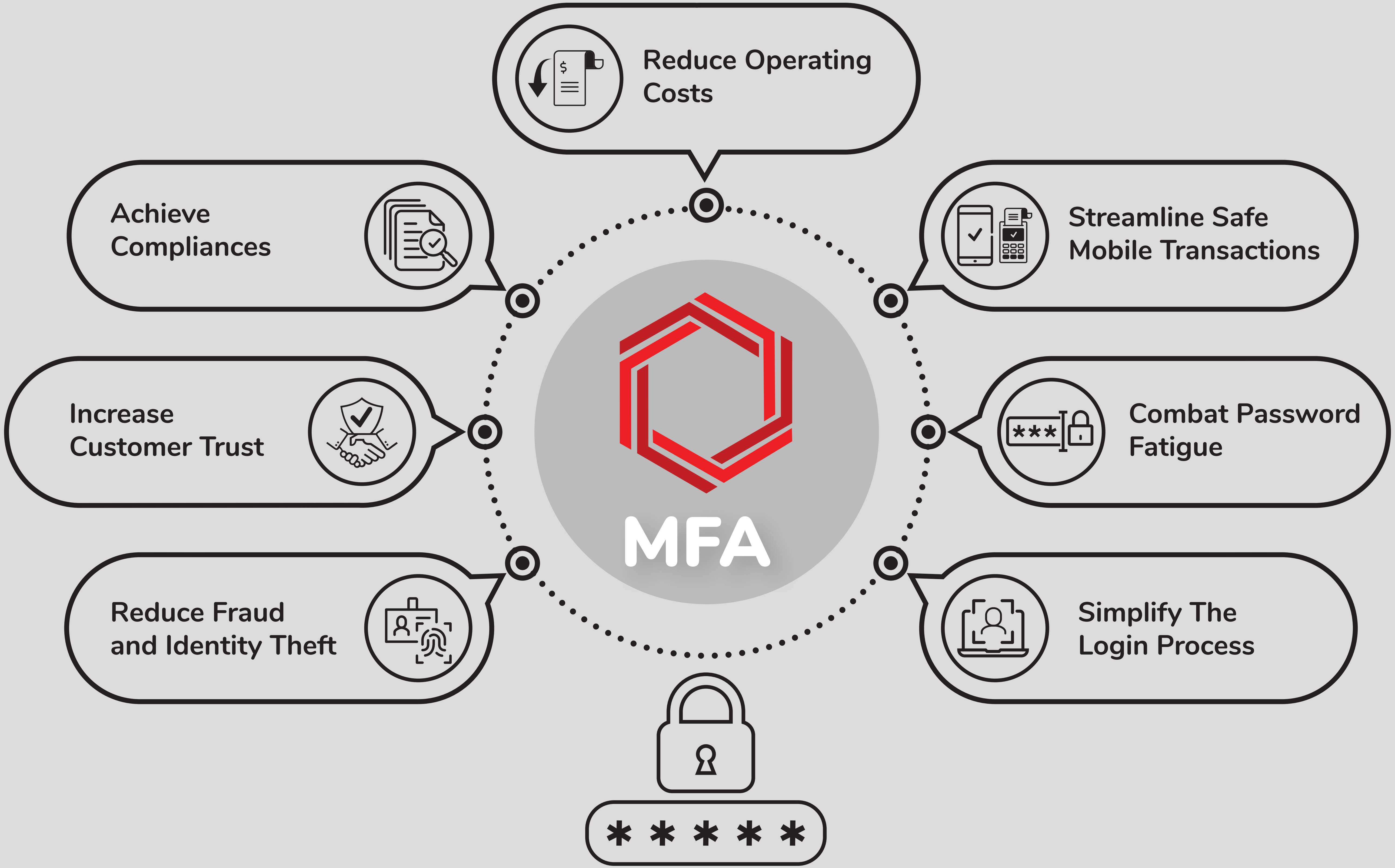


bioLOGIN MFA can be deployed across the whole enterprise to secure workforce client endpoints, servers, web portals, VPN access, network infrastructures (such as switches and routers) and 3rd party cloud-based services using MFA. This removes the attack surfaces hackers can use to penetrate your organization.

bioLOGIN Compliance Chart for Multi Factor Authentication

Components	Functionality	Compliance
Cloud Email	All employees accessing email through web or cloud services	Fully Compliant
Remote Network Access	All remote access provided to employees contractors and third party service providers	Fully Compliant
Internal & Remote Admin Access	☑ All internal & remote admin access to the directory services (Active Directory, LDAP, etc.) ☑ All internal & remote admin access to network backup environments ☑ All internal & remote admin access to network infrastructures (firewalls, routers, switches, etc.) ☑ All internal & remote admin access to the organization’s endpoints/servers	Fully Compliant

Business Benefits of Implementing bioLOGIN MFA



About Fulcrum Biometrics, Inc.

Founded in 2002, Fulcrum specializes in the development and deployment of biometric identity management solutions. Fulcrum is the world's leading independent distributor, developer, and integrator of cutting-edge biometric identification technologies and devices. Our flagship FbF® Fulcrum Biometrics Framework allows the rapid integration and enablement of multi-biometric modalities into new or existing applications, helping integrators build enterprise-sized ecosystems with secure transactions and productive work environments, by confirming identities throughout the organization.

Fulcrum has delivered solutions in the banking, healthcare, retail, and government segments in more than 100 countries and is growing its global footprint as it partners with global Fujitsu entities and systems integrators. Fulcrum has branch offices in San Antonio, Foothill Ranch, New Delhi, Johannesburg, and London.

As of April, 2020, Fulcrum is a wholly owned subsidiary of Fujitsu Frontech North America Inc., a leading provider of innovative technology and IT-based business strategies and applications. Fulcrum is now part of the larger Fujitsu Limited family with global revenues of $35 billion and servicing customers in more than 100 countries worldwide.

Fulcrum Biometrics, Inc (USA)
16108 University Oak
San Antonio, TX 78249
Office: +1 800-430-4601
Intl: +1 210-257-5615
sales@fulcrumbiometrics.com

Fulcrum Biometrics Southern Africa (Pty) Ltd
Block A, Regent Hill Office Park
Corner Leslie & Turley Roads
Lonehill, 2062, Johannesburg
GPS: -26.023195, 28.021488
Office: 011-702-8550
Intl: +27-11-702-8550
sales@fulcrumbiometrics.com

Fulcrum Biometrics India Pvt. Ltd.
802, Udyog Vihar, Phase - V
Gurgaon - Haryana, INDIA 122016
Office: +91-124-4145414
indiasales@fulcrumbiometrics.com

Fulcrum Biometrics Limited
(Formerly Delaney Biometrics)
15 Manor Courtyard
Hughenden Ave, High Wycombe, HP13 5RE
Office: +44 (0)1342-810-810
sales@fulcrumbiometrics.com

Fujitsu Frontech North America, Inc.
27121 Towne Center Drive, Suite 100
Foothill Ranch, California 92610
Office: 1(877) 766-7545
sales@fulcrumbiometrics.com