SOLUTION BRIEF

Identity and Access Management (IAM) Advanced Practices with Fortinet

Executive Summary

Managing identities and access entitlements while providing ease-of-use authentication, accessibility to applications, and optimal user experience to end-users is becoming increasingly challenging in a rapidly changing business and IT environment. These challenges are compounded with the disruption to society and business due to the COVID-19 pandemic. As a result, the workforce of many organizations has become even more remote and mobile.

Enabling effective access rights for every user to protect the organization from cyber adversaries must evolve. They must keep up as an organization's security guardrails rapidly move from protected network perimeters out to the new home office branch. According to the 2020 Verizon DBIR[1], passwords continue to be a weak link. The "Use of Stolen Credentials" is the #1 "Top Hacking Action" and password dumping malware is on the list of "Top Threat Actions."

The Fortinet identity and access management (IAM) solution gives organizations the ability to centrally control and manage the life cycle of user access to critical information, both in the cloud and on-premises. It provides strong authentication through the use of multi-factor authentication (MFA) for identity assurance, audit trails for business regulatory compliance, end-user single sign-on (SSO) to various resources without repeated authentication to increase security while enhancing end-user experience, and X.509 certificate management for onboarding guests and bring-your-own-device (BYOD) policies. The Fortinet IAM solution is available in physical, virtual, and cloud-hosted form factors for deployment on-premises or in the cloud that fulfills your organization's business needs.

Solution for Disparate Access Management Systems

Most organizations are using a multitude of disparate systems across departments to manage employees, contractors, partners, guest identities, and data access. For example, a human resources department may use a variety of software solutions to identify employees and contractors and provide access to various resources. The marketing department may be integrated with third-party partner applications and using a variety of software to analyze and execute data and workflows based on user identity data gathered through collaborative partnership initiatives. And meanwhile, IT may use multiple systems, including multiple IAM systems, to provide secure access to the organization for a variety of users and devices. In total, the number of disparate systems and resulting siloed data housed within a modern enterprise are cause for alarm. Not only do disparate systems create an arduous, non-unified experience for end-users, they increase risk and make risk assessments more difficult. Also, managing disjointed systems requires a vast amount of IT time and resources.

An effective IAM system provides centralized authentication, SSO, and authorization enforcement for targeted applications that are hosted on-premises or in the cloud. These

Over 80% of breaches[2] result from "Use of Stolen Credentials" or brute force.

"Password Dumper"[3] is the top malware variant focusing on credential theft.

44 million accounts[4] were left vulnerable due to compromised accounts or credential theft.

and similar functions ease IT operations, administration, and maintenance, remove the risks of unforeseeable gaps between systems, and provide secure access for the organization—while providing end-users with a consistent and improved experience during the authentication and sign-on process.

Organizations across the globe and across all verticals are increasingly adopting the Fortinet IAM solution. Fortinet IAM is comprised of FortiAuthenticator, FortiToken, and FortiToken Cloud—an "MFA-as-a-service" solution that helps organizations adopt and implement advanced IAM practices.

Fortinet IAM: FortiAuthenticator—A Source of Identity with Centralized Management

At the center of the Fortinet IAM is FortiAuthenticator. FortiAuthenticator functions as an organization's source of identity, and is deeply integrated into the Fortinet Security Fabric. FortiAuthenticator strengthens an organization's user access by simplifying and centralizing the life-cycle management and storage of user identity information obtained from various systems of record. Through integration with existing Active Directory (AD), Lightweight Directory Access Protocol (LDAP) authentication systems, or cloud-based identity stores, FortiAuthenticator provides user authentication, including MFA, certificate-based and adaptive authentication, and SSO controls for organizations to assure identity and enable access rights for all users, at any time, and from anywhere, whether through corporate wired, wireless, or remote virtual private network (VPN) connections.

FortiAuthenticator is built with high availability (HA) designed to ensure business continuity and resiliency. HA deployment is simple and it functions seamlessly during a failover, whether for maintenance or during an unexpected failure. FortiAuthenticator also includes user self-registration and password recovery options, allowing users to reset their password without engaging the help desk, which can represent a significant cost savings for many organizations.

FortiAuthenticator is available for deployment on-premises, in a virtual environment, or via the public cloud. FortiAuthenticator licensing is structured simply, with perpetual, nonrecurring costs for all features. FortiAuthenticator reporting also makes it easy to demonstrate return on investment (ROI) throughout the decision and deployment process. And with FortiAuthenticator flexible form factors, organizations can choose whichever deployment method best meets their IAM initiatives and budgets. And because of its integrated suite of solutions and powerful engines, organizations can save more than 50% annually as compared with alternative solutions.

FortiAuthenticator protects user access with advanced, streamlined Identity Access Management features such as centralized user access policy, user privilege management, MFA, SSO, audit trails, and more. By increasing user access protection, FortiAuthenticator makes it more difficult for adversaries to steal credentials, impersonate users or devices, and gain unauthorized access to applications or network resources. Additionally, its centralized management simplifies IT operations and reduces unforeseeable security gaps that can be overlooked when managing disjointed IAM systems.

Fortinet IAM: FortiToken—A Comprehensive Option for MFA

MFA is an essential security feature for any IAM solution because it enforces the verification of multiple credentials. MFA needs to include at least two of the following:

- ***Something the user knows:*** a username and password.
- ***Something the user has:*** a one-time passcode (OTP) in the form of a token or code. This is sent to the user via email or SMS, to a hardware token generator, or to an authenticator application installed on the user's smartphone.
- ***Something specific to the user:*** biometric information such as the user's fingerprint, facial recognition, or iris scan.

FortiToken (FTK) offers a widest range of OTP tokens and MFA use cases to suit any organization's needs. FTK also comes in a variety of form factors and the following options are available at a perpetual, nonrecurring cost:

- **Application:** time-based and user-friendly, with PUSH to accept/deny credentials during the MFA process. It supports either iOS or Android platforms.
- **Standalone:** a physical, tamper-resistant device with time-based OTP. These tokens come in the form of a USB stick, half credit card size, or a small keychain size, each with a large screen to display the token.
- **Email and SMS tokens**

Token activation can be performed online or offline (making it suitable for closed environments). FTKs can also be transferred between authenticating devices, such as a FortiGate or FortiAuthenticator, or between mobile devices (i.e., iOS or Android). This provides visibility,

simplifies two-factor authentication management, and increases security to protect organizations from adversaries seeking unauthorized access (even if a cyber criminal has a username and password, they cannot access the system without the other information).

FortiAuthenticator has token options for all users and scenarios to confirm user identity using MFA. With its centralized management, FortiAuthenticator and FTKs provide organizations with the ability to assure identity and control user access to corporate VPNs, network devices and resources, and on-premises or cloud-based applications.

Fortinet IAM: FortiToken Cloud—Cloud-based "MFA-as-a-Service"

FortiToken Cloud (FTC) provides everything an organization needs to adopt and manage multi-factor authentication in their FortiGate or FortiAuthenticator environment. There is no additional authenticator hardware or software required, nor any changes needed to the existing security policy on the FortiGate or FortiAuthenticator.

FTC is a subscription service available through the purchase of points. FTC points can easily scale as an organization's needs change. Through its intuitive dashboard, organizations can get a summary of useful metrics such as overall usage, active users, remaining points, and logs that capture key information about both active and closed sessions.

FortiToken Cloud makes it easier for organizations to implement MFA by extending user identity further through the verification of something the user has. MFA makes it more difficult for adversaries to gain access to corporate resources even if they have and use stolen credentials, the #1 "Top Hacking Action" and "Top Threat Actions" leading to network breaches.[5]

Fortinet Provides a Full Suite of Market-leading Security Solutions

Fortinet is a recognized leader in networking and cybersecurity technologies. The Fortinet IAM solution is an excellent value for organizations. It provides the right IAM tools combined with flexible deployment options to enable access rights for every user, ultimately protecting the business from cybersecurity breaches. The fact that it provides life-cycle management and centralized operations, administration, and maintenance, along with ease of use for end-users, makes the Fortinet IAM an easy choice for an organization's IAM advanced practices.

1 "Verizon 2020 Data Breach Investigations Report," Verizon, May 2020.

2 Ibid.

3 Ibid.

4 Catalin Cimpanu, "44 million Microsoft users reused passwords in the first three months of 2019," ZDNet, December 5, 2019.

5 "Verizon 2020 Data Breach Investigations Report," Verizon, May 2020.

November 18, 2020 8:35 AM

842719-0-0-EN

D:\Fortinet\Solution Brief\Blue Solution Brief\Fortinet IAM\sb-FA-identity-and-access-management-11182020