IBM Security and Zscaler

Enable your anywhere workforce with everywhere security

Highlights
Enable SSO authentication and automatic provisioning of user and admin accounts

Verify the identity of users and the integrity of devices at runtime

Use identity and device context to authorize secure connections for corporate resources

Monitor suspicious behavior and automate policy updates to eliminate threats in near real-time

Confidently running a business means empowering workers to be productive by allowing them to work from anywhere, on any device, while granting them secured access to the applications and data they need to do their job. In a cloud-first world where data and applications are no longer hosted in single data centers, traditional security perimeters are challenged.

Both a zero trust security approach and analytics are needed to protect today's enterprises.

IBM Security® offers a wide-range of industry-leading security capabilities including identity and access management (IBM Security Verify), unified endpoint management (IBM Security MaaS360®), and threat management for security operations (IBM Security QRadar® and IBM Cloud Pak® for Security). The combination of IBM Security and Zscaler makes it easier for security teams to take a zero trust approach to security modernization and enables businesses to focus on key initiatives like securing their hybrid workforce, protecting their hybrid cloud, and reducing the risk of business disruption.

By integrating the suite of IBM Security products with Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), organizations are provided a holistic technical foundation for implementing a zero trust architecture.

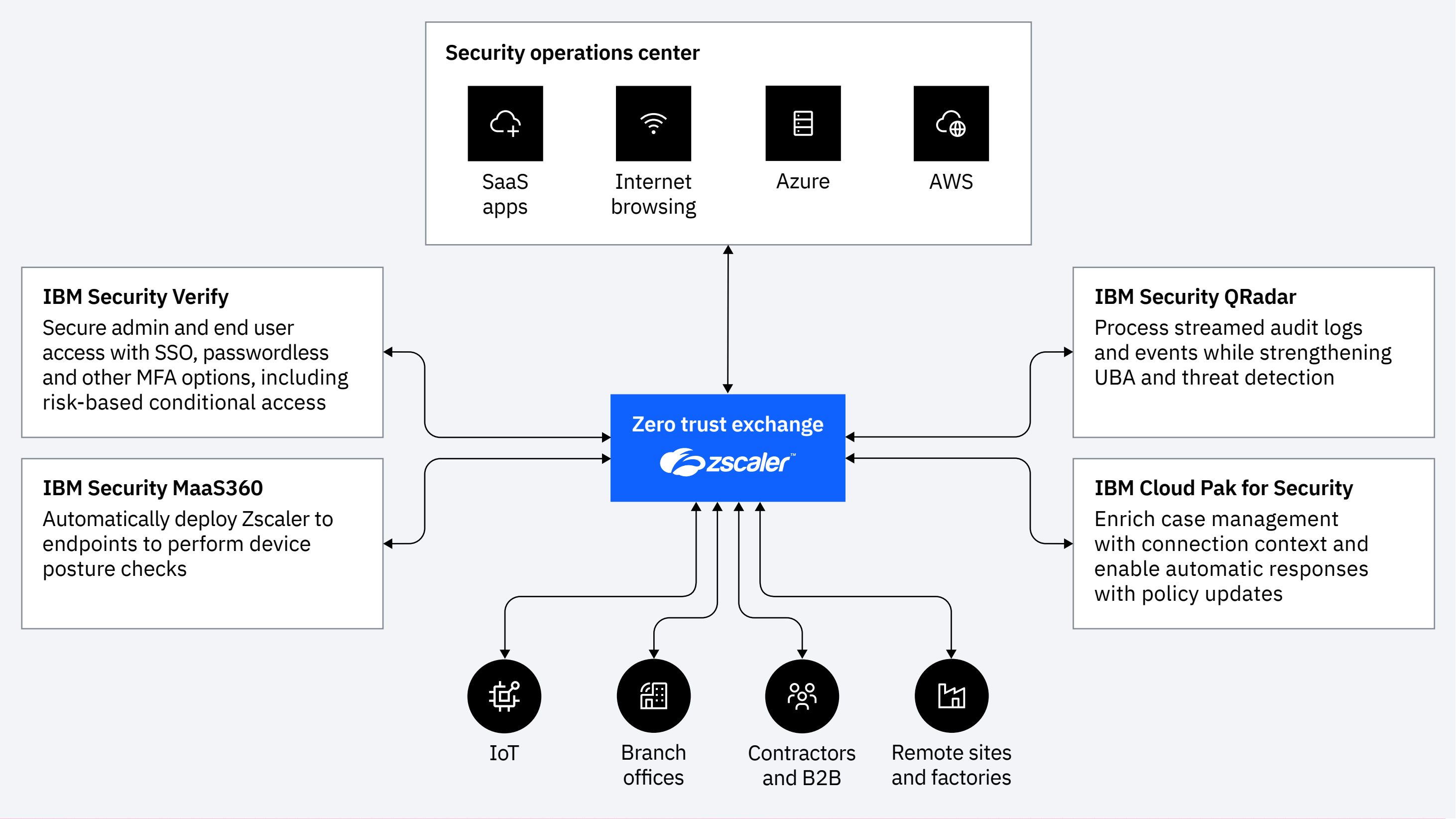
Security operations center
SaaS apps
Internet browsing
Azure
AWS
IBM Security Verify
Secure admin and end user access with SSO, passwordless and other MFA options, including risk-based conditional access
IBM Security MaaS360
Automatically deploy Zscaler to endpoints to perform device posture checks
Zero trust exchange
zscaler
IBM Security QRadar
Process streamed audit logs and events while strengthening UBA and threat detection
IBM Cloud Pak for Security
Enrich case management with connection context and enable automatic responses with policy updates
IoT
Branch offices
Contractors and B2B
Remote sites and factories

Figure 1: Benefits of IBM Security and Zscaler integration

Enable SSO authentication and automatic provisioning of user and admin accounts

Single sign-on (SSO) authentication ensures that the right people have the right access to IT resources. Protocols such as SSO and user provisioning streamline authentication processes both for employees and IT administrators. By automating SSO and user provisioning, it further simplifies the process, while allowing employees to access multiple applications securely and seamlessly. Traditional IAM capabilities like single sign-on, multi-factor authentication, and account provisioning and deprovisioning are available at the click of a button with IBM Security Verify.

Verify the identity of users and the integrity of devices at runtime

Beyond single sign-on and multifactor authentication, IBM Security Verify is a modernized, modular IDaaS that provides deep, AI-powered context for risk-based authentication and adaptive access decisions, guided experiences for developer time-to-value, and comprehensive cloud IAM capabilities. From privacy and consent management to holistic risk detection and identity analytics, IBM Security Verify centralizes workforce and consumer IAM for any hybrid cloud deployment.

Adaptive access capabilities in IBM Security Verify provide more advanced security by dynamically assessing user risk across 5 context domains: user attributes, device posture, environmental conditions, resource sensitivity, and behavioral attributes like mouse movements and keyboard strokes.

Use identity and device context to authorize secure connections for corporate resources

IBM Security Verify's user risk score is made available to ZIA and ZPA as part of conditional access decisions. As the user risk changes, the conditional access policies will automatically adapt. Similarly, IBM Security MaaS360 provides critical device posture information to ensure that both mobile and traditional endpoints are compliant with corporate policy.

Monitor suspicious behavior and automate policy updates to eliminate threats in near real-time

ZIA and ZPA send detailed telemetry about user activity, threats and connections to IBM Security QRadar. Zscaler integrates with IBM Security QRadar on Cloud using CloudNSS, simplifying the process of data ingestion. By combining this connection context with other telemetry sources such as identity, endpoint, cloud, and application workloads, QRadar can detect potentially malicious activity and drive automated responses via IBM Cloud Pak for Security to manage URL categories, allowlists, and blocklists in ZIA, and enrich cases with additional ZIA context.

Conclusion:

IBM Security believes that an open approach is required to address the fragmentation and complexity challenges facing security teams today as they adopt a zero trust strategy. To help simplify and connect security across companies' broader ecosystem of vendors, IBM is collaborating with leading technology partners.

IBM Security and Zscaler integration combines validated user identity with business policies for direct access to authorized applications and resources with the goal of helping organizations and their employees fully embrace working from anywhere while protecting enterprise data.

IBM Security products are available as traditional software or SaaS, and are conveniently delivered via popular cloud marketplaces like AWS and Azure.

- IBM Security Verify
- IBM Security MaaS360
- IBM Security QRadar
- IBM Cloud Pak for Security

Visit the IBM Security App Exchange to download integration applications.

3K+

IBM holds over 3,000 security patents.

1T+

IBM monitors more than one trillion events per month in more than 130 countries.

Why IBM?
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. IBM holds over 3,000 security patents and monitors more than one trillion events per month in more than 130 countries. To learn more, visit ibm.com/security.

Zscaler accelerates digital transformation so customers can be more agile, efficient, resilient and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

For more information:
To learn more about IBM Security and Zscaler please contact your IBM representative or IBM Business Partner, or visit newsroom.ibm.com/2021-05-05-IBM-Helps-Customers-Adopt-a-Zero-Trust-Approach-to-Security.

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
August 2022

IBM, the IBM logo, IBM Cloud Pak, MaaS360, QRadar, IBM Security, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.