IBM Security and Zscaler

IBM can help you build your security capabilities so your business can thrive

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 secured connections for corporate resources

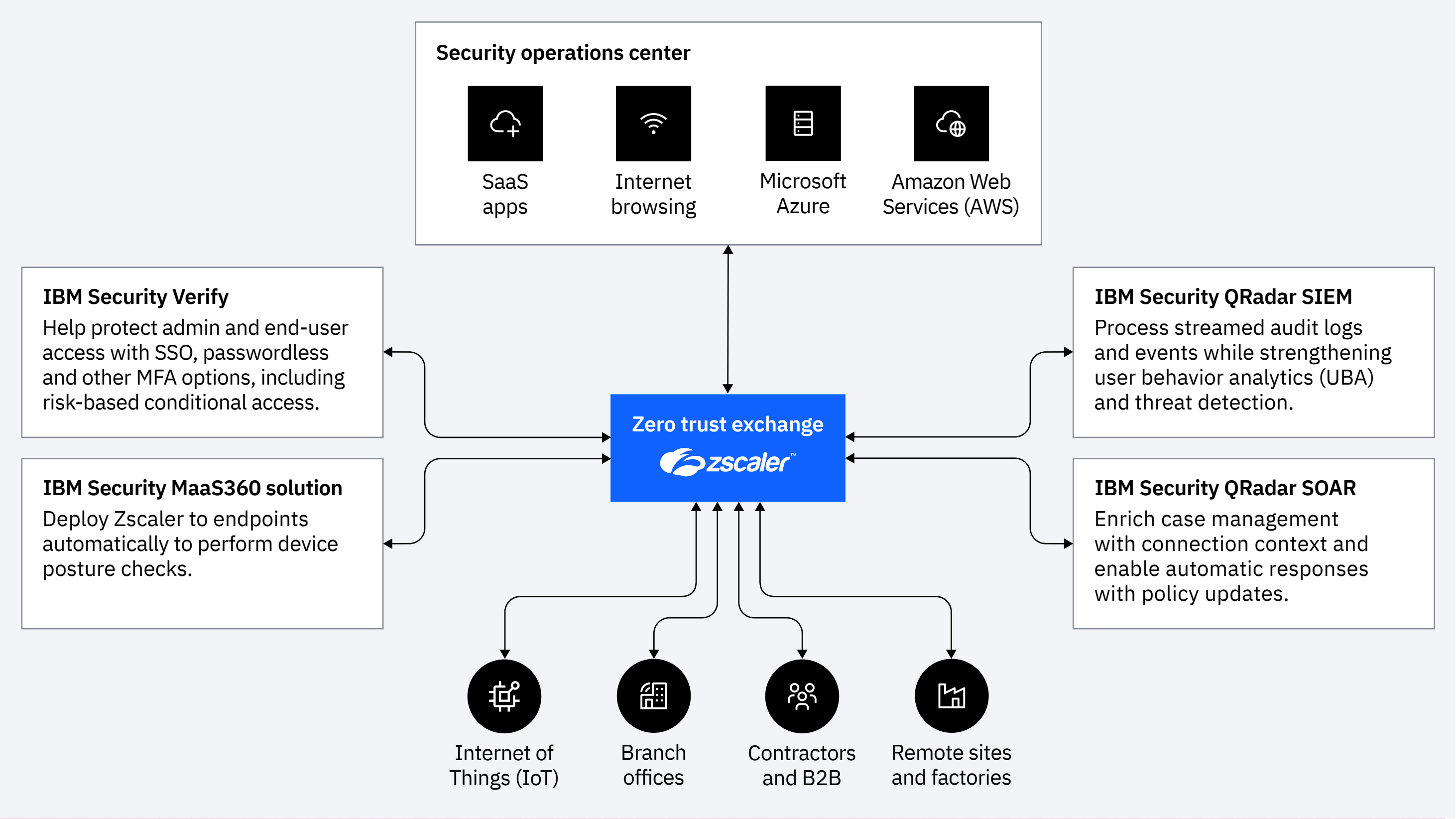
Monitor suspicious behavior and automate policy updates to help detect threats in near-real time

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 can help protect today's enterprises.

IBM Security® offers a wide-range of security capabilities, including IBM Security Verify identity and access management, IBM Security MaaS360® unified endpoint management, and IBM Security QRadar® SIEM and IBM Security QRadar SOAR threat management for security operations. The integration of IBM Security and Zscaler can support your security team's implementation of 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.

IBM Security products can integrate with an organizations's existing Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) products, to help them achieve a holistic technical foundation for implementing a zero trust architecture.


Security operations center

SaaS apps

Internet browsing

Microsoft Azure

Amazon Web Services (AWS)

IBM Security Verify
Help protect admin and end-user access with SSO, passwordless and other MFA options, including risk-based conditional access.

IBM Security MaaS360 solution
Deploy Zscaler to endpoints automatically to perform device posture checks.

IBM Security QRadar SIEM
Process streamed audit logs and events while strengthening user behavior analytics (UBA) and threat detection.

IBM Security QRadar SOAR
Enrich case management with connection context and enable automatic responses with policy updates.

Figure 1. IBM Security and Zscaler integration

Enable SSO authentication and automatic provisioning of user and admin accounts
Single sign-on (SSO) authentication can help provide the right people with 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 can further simplify the process, while allowing employees to access multiple applications seamlessly in a security-rich environment. Traditional identity and access management (IAM) capabilities like SSO, multifactor authentication (MFA), and account provisioning and deprovisioning are available with IBM Security Verify.

Verify the identity of users and the integrity of devices at runtime
Beyond SSO and MFA, IBM Security Verify is a modernized, modular identity as a service (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 can centralize workforce and consumer IAM for hybrid cloud deployment.

Adaptive access capabilities in IBM Security Verify asses 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 secured connections for corporate resources
The IBM Security Verify 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 solution provides device posture information to help confirm that both mobile and traditional endpoints are aligned with corporate policy.

Monitor suspicious behavior and automate policy updates to help detect threats in near-real time
ZIA and ZPA send detailed telemetry about user activity, threats and connections to IBM Security QRadar SIEM. Zscaler integrates with IBM Security QRadar SIEM on Cloud using Cloud NSS, simplifying the process of data ingestion. By combining this connection context with other telemetry sources, such as identity, endpoint, cloud and application workloads, QRadar SIEM can detect potentially malicious activity and drive automated responses through IBM Security QRadar SOAR 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.

The 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 software as a service (SaaS), and are conveniently delivered through popular cloud marketplaces like AWS and Microsoft Azure.

- IBM Security Verify
- IBM Security MaaS360 solution
- IBM Security QRadar
- IBM Security QRadar SOAR

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 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.

Why Zscaler?
Zscaler accelerates digital transformation so clients can be more agile, efficient, resilient and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by helping to secure the connection among users, devices and applications in different locations. Distributed across more than 150 data centers globally, the security service edge (SSE)-based Zero Trust Exchange is one of the world's largest in-line cloud security platforms.

For more information:
To learn more about IBM Security and Zscaler contact your IBM representative or IBM Business Partner, or view the related press release.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
October 2022

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.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

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.

Zscaler is not an IBM product or offering. Zscaler is sold or licensed, as the case may be, to users under Zscaler’s terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for Zscaler is the direct responsibility of and is provided directly to users by Zscaler.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.