Top Concerns C-Level Executives Should Have About Hybrid and Remote Security

FEBRUARY 2025

EBOOK

Contents

Introduction

Cyberattacks grew by a staggering 30% YoY[1] globally in Q2 2024. The increased adoption of remote work has expanded the attack surface and left organizations vulnerable to a broad range of threats. According to Zscaler's ThreatLabz Encrypted Attacks Report, the Zscaler cloud blocked an unprecedented 32.1 billion attacks embedded in TLS/SSL traffic, with encrypted threats accounting for 87.2% of all blocked attacks—a 10.3% year-over-year increase.[2] This data highlights the growing reliance on encryption by threat actors to conceal their malicious activities.

Legacy technologies like firewalls and virtual private networks (VPNs) are no longer sufficient to protect company data, applications, and networks, giving decision-makers and those at the top a hefty list of concerns when it comes to securing remote work environments. Leaders are under constant pressure to minimize the risk of breaches, ensure compliance with regulations and industry standards, and prevent the theft of valuable data such as intellectual property or trade secrets.

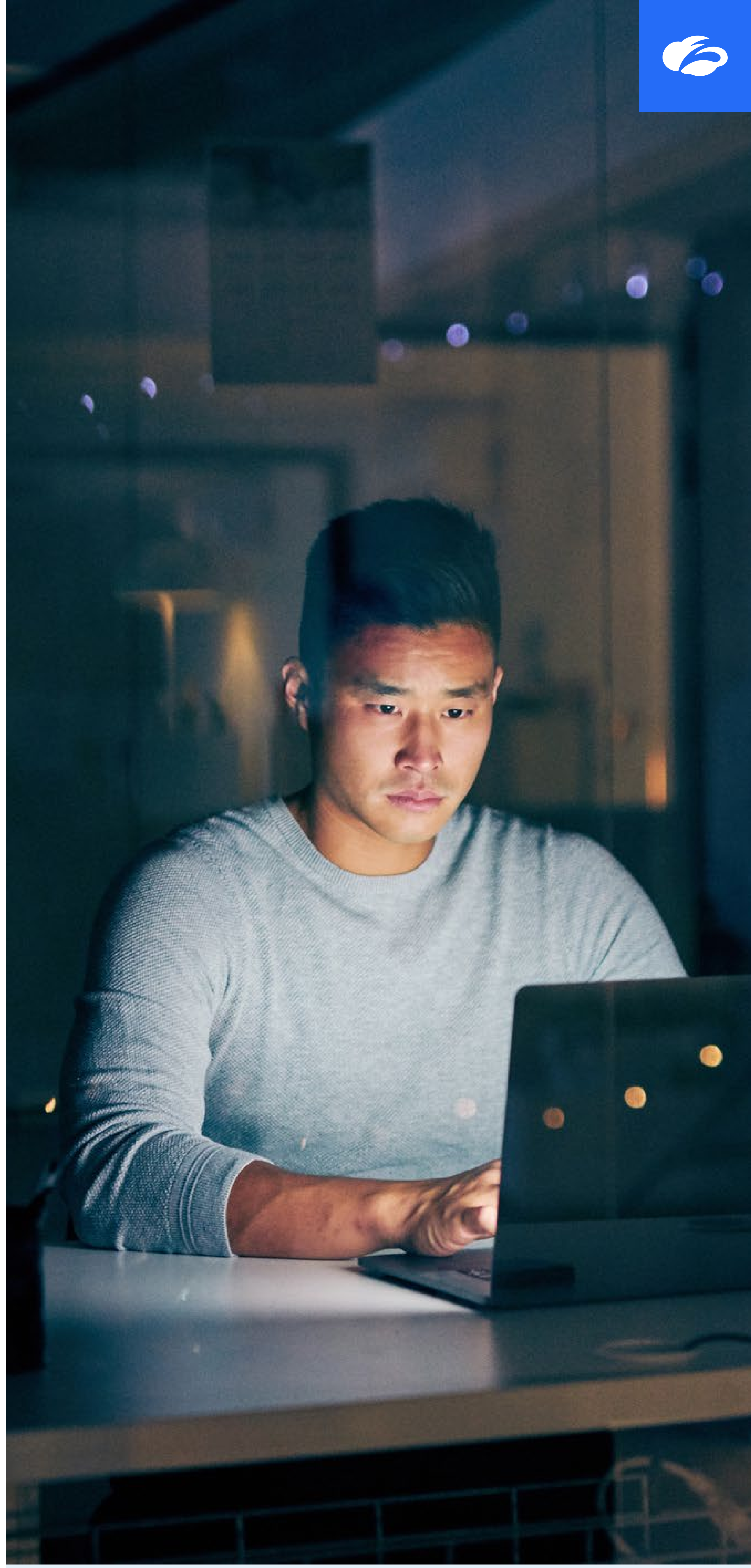
The good news is that cloud-based zero trust solutions are designed to safeguard the networks of organizations running remote and hybrid workforces. With the right technology, executives can eliminate these main concerns.

Overview of critical network and remote security issues

Remote work operations can weaken businesses' control over data and the integrity of their security architecture. Employees may use unmanaged devices that may not have security software installed or be actively monitored to access company resources, including critical applications.

Additionally, security professionals don't have complete visibility into how remote employees handle sensitive data and whether they delete it after use. Employees might store data on their personal devices, making them vulnerable to ransomware attacks, data breaches, and other threats.

The shift to cloud-based applications expands the attack surface further, complicating the security of your digital infrastructure.



The evolving digital security landscape

In the pre-pandemic world, firewalls and VPNs may have been enough to secure a company's networks and sensitive data. However, remote and hybrid work have driven the need for a complete transformation in how organizations safeguard their digital environments today.

Latest trends in digital security and remote work

Remote employees inevitably need company resources to do their jobs, regardless of their locations, and many organizations have adopted cloud-based software-as-a-service (SaaS) applications to support remote work and improve productivity. Deploying SaaS across a dispersed network of employees results in a wider attack surface and increases the risk of unauthorized access and security breaches.

Cybercriminals have also developed more sophisticated tactics — including credential stuffing and zero-day attacks — upping the ante for the C-suite when it comes to cybersecurity. In fact, the United States remains the top target of ransomware, experiencing 49.95% of overall attacks, followed by the United Kingdom, Germany, Canada, and France.[3] Besides eroding brand reputation and customer trust, these attacks put your business at risk of non-compliance with data privacy and security regulations — not to mention financial peril.

In light of these trends, C-level executives and security leaders are adopting new security measures, such as:

- **Zero trust architecture**, which works on the principle of "never trust, always verify." All users and devices, including Bring Your Own Device (BYOD), must be verified.
- **Artificial intelligence (AI) and machine learning (ML)-powered threat detection**, which helps proactively identify and mitigate sophisticated cyberattacks.
- **Application segmentation**, which prevents lateral threat movement.
- **Endpoint security**, which focuses on safeguarding the devices used by remote employees. AI-powered solutions can detect and block threats before they impact endpoints, ensuring better protection for distributed workforces.

Major organizational security concerns for leaders

With the prevalence of remote and hybrid work, growing dependence on cloud-based solutions, business leaders and CISOs must think beyond perimeter-based security.

Protecting sensitive data

When employees access business data through unsecured networks and save it on personal devices, it amplifies the risk of unauthorized access and data mishandling. Safeguarding sensitive data in remote work environments involves:

- **End-to-end encryption** to protect data at rest and in transit, particularly when it's transferred over unsecured channels.
- **Identity and access management** to ensure only authorized employees can access and use necessary data.
- **Data loss prevention** techniques to mitigate accidental data exposure and breaches.

Managing insider threats

Accidental and intentional actions from on-site and remote employees can compromise system security. For example, a new employee might fall prey to a phishing scam, or a disgruntled employee may misuse confidential company data. Role-based access control, least-privilege access policies, and behavioral analytics can help minimize the risk of insider threats.

Ensuring compliance with regulations

Dozens of governments have implemented data protection and privacy laws to protect consumers' personal information, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Additionally, there are industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA). In remote work environments, maintaining compliance with these regulatory requirements involves thorough governance strategies.

Strategies to address leadership concerns

Several strategies can be adopted by C-level executives to address the complex security challenges of the modern work environment.

Implementing robust identity and access management

Identity and access management (IAM) is an effective method of preventing unauthorized access to your organization's network and systems. It ensures that only the right people have access to the applications and data they need to do their jobs.

IAM minimizes the attack surface — reducing unnecessary exposure to sensitive data. Unlike perimeter-based security methods, IAM involves stricter access controls regardless of a user's device and location. Leaders should consider implementing a platform that supports flexible IAM solutions and integration.

Enhancing threat detection and response capabilities

As cybercriminals evolve their strategies, security leaders must upgrade theirs as well to thwart attacks with advanced threat detection and response. Implement solutions that use AI and ML models to monitor network traffic and user behavior to detect deviations automatically.

AI and ML also augment zero trust solutions that isolate compromised devices and files in real-time, enabling quick responses to threats and supporting a more proactive cybersecurity approach. ML algorithms can also highlight potential vulnerabilities while identifying and blocking emerging threats.

Regular security training and awareness programs

Security policies and tools are only as good as the people using them. Case in point: 80% of CISOs believe that employee negligence and human risk will be major cybersecurity concerns by 2026[4]. Employees in remote work environments are particularly vulnerable because they can't always reach out to security professionals in person for help, causing delays and irreversible damage.

To mitigate these scenarios, organizations can implement ongoing security training programs that familiarize employees with existing, emerging, and evolving threats and best practices that empower them to stay vigilant against an ever-changing threat landscape. Educate your team about remote work best practices, password hygiene, and safe data handling. Also, conduct training sessions regularly to refresh employees on company-wide cybersecurity protocols and readily available resources of what to do if their devices, data, and access to applications are compromised.

Leveraging Zscaler solutions for in office, hybrid, and remote security

Zscaler's cloud-based zero trust solutions are designed to help business leaders secure any work environments today and into the future as threats evolve. The Zscaler Zero Trust Exchange™ includes the following core solutions to ensure teams have comprehensive security:

Zscaler Internet Access (ZIA)

Zscaler Internet Access is a cloud-native, AI-powered, zero-trust solution that helps reinforce digital security for remote workforces. Using a zero trust proxy architecture that inspects 100% of TLS/SSL traffic at scale, with direct user-to-app connections based on identity, context, and business policies, ZIA ensures seamless and secure access to SaaS and web-based apps with the following key capabilities:

- **Cloud-native Secure Web Gateway (SWG)** delivers a safe, fast web experience while detecting and preventing advanced attacks with real-time, AI-powered analysis and URL filtering.
- **AI/ML-based Advanced Threat Prevention** to stop advanced threats like botnets, ransomware, command-and-control, risky file sharing, malicious active content, cross-site scripting, fraud sites, and more.
- **AI-powered URL filtering** ensures safe web app browsing sessions for your users by stopping advanced threats—like phishing and ransomware—and applying acceptable use policy.
- **Cloud Access Security Broker (CASB)** secures cloud apps, protects data, stops threats, and ensures compliance across your SaaS and IaaS environments with integrated protection.
- **Data Loss Prevention (DLP)** protects data in motion with full inline inspection, including Exact Data Match (EDM), Indexed Document Matching (IDM), and machine learning.
- **Dynamic risk-based policy** stops active attacks and future-proofs your defenses with continuous user, device, app, and content risk analysis fueling dynamic access controls.
- **Zero Trust Firewall** enables fast, secure on- and off-network connections and local internet breakouts for user traffic across all ports and protocols, without any hardware or software updates to manage
- **AI-powered Browser Isolation** renders web sessions as pixels-only in the user's browser, delivering a near-native web experience without the risk of data loss or device infection.
- **DNS Security** filters risky and malicious domains and stops the use of DNS tunneling to transfer malicious payloads and sensitive data.

Zscaler Private Access (ZPA)

Zscaler Private Access is the industry's first AI-powered zero trust network access (ZTNA) solution and is a cloud-native offering that delivers zero trust access for all users. By offering direct connectivity to private applications while minimizing the attack surface, ZPA eliminates lateral threat movement using AI-powered user-to-app segmentation and protects against sophisticated attacks with integrated traffic inspection and application and data protection. Some of ZPA's key capabilities that can secure the hybrid workforce include:

- **AI-Powered App Segmentation** discovers applications automatically and provides AI-generated recommendations on app segments and policies to reduce your attack surface and prevent lateral movement.
- **Workload-to-Workload Segmentation** secures cloud workload communications across hybrid and multicloud environments such as AWS and Azure.
- **Privileged Remote Access** gives remote workers and third parties clientless remote access to sensitive RDP, SSH, and VNC production systems.
- **Private Service Edge** brings ZTNA to on-premises users with direct user-to-app, least-privileged access to private applications.
- **Business Continuity** ensures uninterrupted, policy-enforced access to mission-critical applications during connectivity outages and black swan events.
- **Extranet Application Support** enables zero trust access to business partner and vendor applications hosted in their networks.
- **Digital Experience Monitoring** optimizes your digital experiences to keep users productive by rapidly detecting and resolving app, network, and device issues.

Advanced security features

Zscaler offers several advanced features, including:

- **SSL/TLS inspection** at scale for complete data protection and user-to-app inspection.
- **AI-powered inline threat detection** to shut down attack vectors before they reach their target.
- **Risk360™** for intuitive risk visualizations, factors, details, and reporting so you can take immediate action to mitigate risks.

How to secure your team with Zscaler

If you want to strengthen the security of your remote work environment, you must consider a shift away from legacy cybersecurity solutions. The Zscaler zero trust platform offers several ways to ease the transition.

Transforming from firewalls to zero trust

Firewalls and VPNs are ineffective in the modern business environment because they expand your corporate network — giving attackers more avenues for entry. In contrast, the Zscaler Zero Trust Exchange™ acts as an intelligent switchboard, inspecting both inbound and outbound traffic to and from user devices to detect and block threats while securely brokering connections to apps and cloud resources.

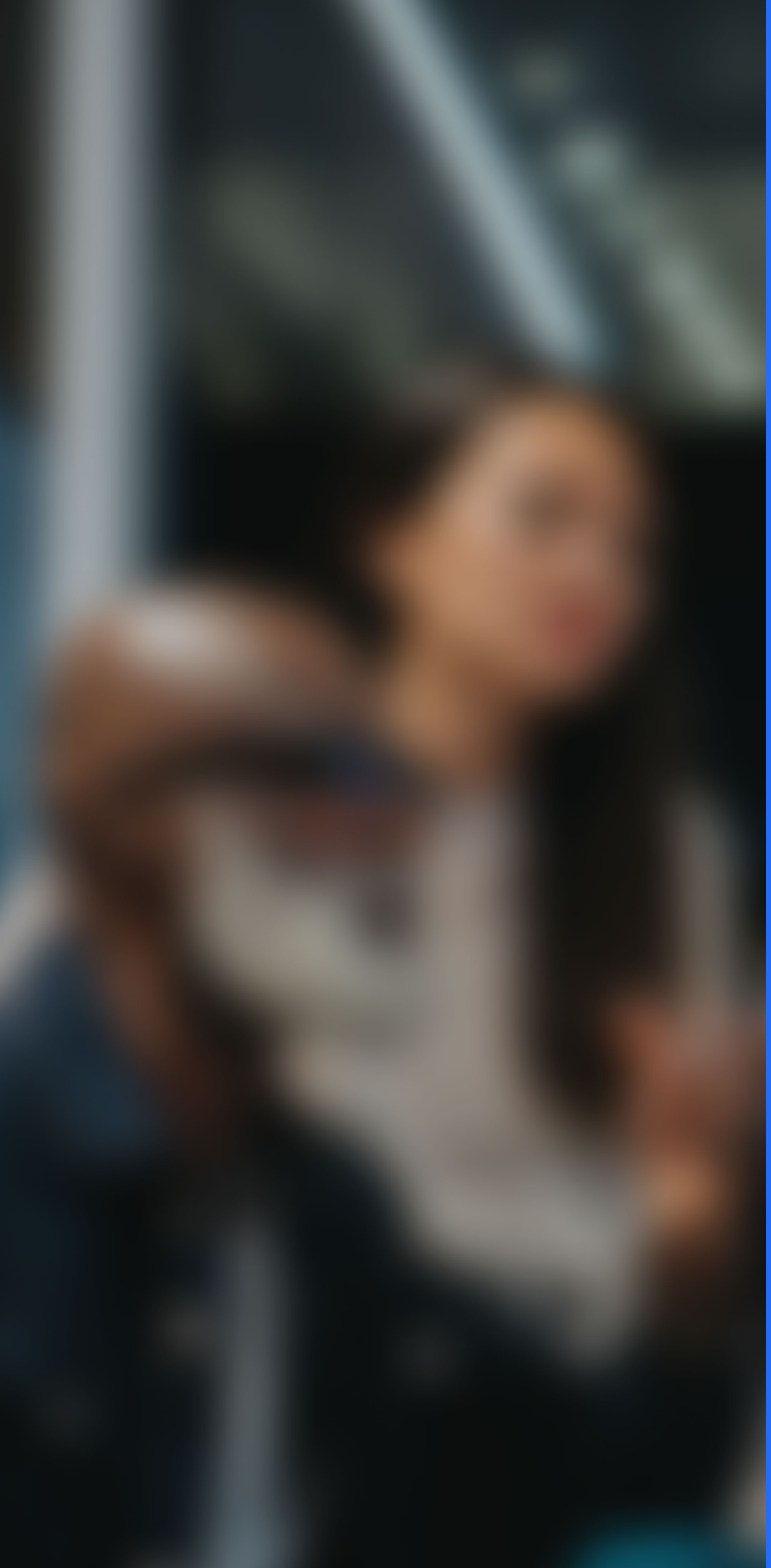
A comprehensive zero trust approach

A true zero trust approach to security requires identity-centric, context-aware access policies that are tailored to each user, device, and application. The goal is to ensure that only trusted users can access specific resources, and those users and resources are designated by your company's established controls. You can set rules in your zero trust security framework to grant users access based on location, identity, time/date, and more, and Zscaler walks you through this process so your organization gets off on the right foot with these controls.

Find out more about how Zscaler can help you transform your security posture to protect your dispersed workforce by requesting a demo.

SOURCES:

1. Intelligent CISO, Check Point Research unveils Q2 2024 cyberattack trends, highlighting global and UAE increases, July 29, 2024.
2. Zscaler, ThreatLabz 2024 Encrypted Attacks Report, 2024.
3. Zscaler, ThreatLabz 2024 Ransomware Report, 2024.
4. Infosecurity Magazine, 70% of CISOs Expect Cyber-Attacks in Next Year, Report Finds, May 21, 2024.



zscaler™ | Experience your world, secured.™