Use case

Zero trust, total confidence

Help make sure your devices and users meet your mobile security authentication requirements—before they access the network.

Never trust. Always verify.

In today's hybrid, cloud and mobile world, threats can come from anywhere. Without the traditional office network, a smarter approach to security is needed. Zero trust is built on a simple, smart idea: Never trust, always verify. That means users, devices and requests are granted to the network, sensitive data or your business-critical applications. The result is a strong framework that helps reduce risk, provide threat protection, and enforce policies and compliance requirements.

From open access to secure checkpoints

Challenges

Businesses face a fast-changing digital landscape where cyberthreats can disrupt operations and erode customer trust. Businesses need a security strategy that addresses a range of challenges, such as:

- **Dealing with limited visibility**
  Businesses often lack clear insight into user activity and device access, making it harder to identify issues before they escalate.
- **Managing diverse users and locations**
  Companies need visibility in order to set and enforce network access requirements for mobile devices for employees, contractors and staff.
- **Reducing downtime caused by cyberthreats**
  System outages, even brief ones, can disrupt workflows, delay customer orders and reduce overall efficiency.
- **Maintaining compliance and trust**
  Without consistent, automated processes, it can be difficult to maintain access reviews and certifications required for compliance.

Here's the rundown.

16%
of businesses have protections against zero-day exploits.[1]

47%
Large enterprises lead in zero trust adoption at 47%, compared to 38% for small- and medium-sized businesses.[2]

35%
Manufacturing and energy organizations have only 35% zero trust adoption—lower than the average response of 43%.[3]

22%
In the exploitation of vulnerabilities attack action, the percentage of edge devices and virtual private networks as targets is 22%, up from just 3% in the previous year.[4]

verizon business

Solutions and benefits

Adopting a zero trust approach offers more than just enhanced security. It brings a host of practical advantages that can help improve operations. With a "never trust, always verify" principle, zero trust delivers security from the inside out, providing a robust framework to address the specific challenges faced by small- and medium-sized businesses.

Verify before providing network access.	Implement a zero trust strategy that requires continuous verification and authorization. Using identity and access management services helps verify every user and device, reduce risk and keep critical systems secure.
Create fast, secure access.	Set and enforce network access policies for both users and devices.
Support automatic compliance.	Get automated access reviews and certifications that can help you meet regulatory requirements while shifting from on-premises systems to the cloud, ensuring a smooth and secure migration.
Modernize with confidence.	Set role-based access controls so each user can only reach the applications and data they need, creating a safer, more controlled path to digital transformation.

What's the cost of a cybersecurity breach?

36%
More than a third of surveyed organizations experienced cyber insurance penalties due to a security compromise.[5]

$115K
The median amount paid to ransomware groups in 2024 was a costly $115,000.[6]

Proven mobile security intelligence

The Verizon 2025 Mobile Security Index delivers a comprehensive view of the evolving mobile threat landscape. It transforms critical insights into actionable security strategies that let you benchmark your defenses, spot emerging risks and strengthen your mobile security posture. Get the report at verizon.com/mobilesecurityindex.

Why Verizon

The future of mobile security goes deeper than the perimeter, verifying access at every step. Verizon delivers industry-leading identity and access management solutions and end-to-end connectivity solutions to help you build your zero trust framework. Our portfolio includes:

- **Verizon Mobile Device Management:** A solution to help you manage and secure your mobile devices with remote, touchless onboarding and automatic device enrollment
- **Zero Trust Dynamic Access:** A solution to help block user, app and data attacks while giving trusted users secure access from virtually anywhere they connect to the network
- **Secure Access Service Edge (SASE) Management:** A management tool that allows users and applications to access your network securely – in the office, in the cloud and at the edge
- **Managed Identity and Access Management (IAM) with Accenture:** Artificial intelligence-powered solutions that verify users with multifactor authentication, single sign-on and more

Let's build your mobile defense plan.

We can help you create a zero trust strategy that helps protect your users, devices and connections. Contact your Verizon Account Representative, who can help you strengthen your mobile security defenses.

1. "2025 Mobile Security Index," Verizon, Oct 22, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf
2. Ibid.
3. Ibid.
4. "2025 Data Breach Investigations Report," Verizon, Apr 22, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
5. "2025 Mobile Security Index," Verizon, Oct 22, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf
6. "2025 Data Breach Investigations Report," Verizon, Apr 22, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

verizon business