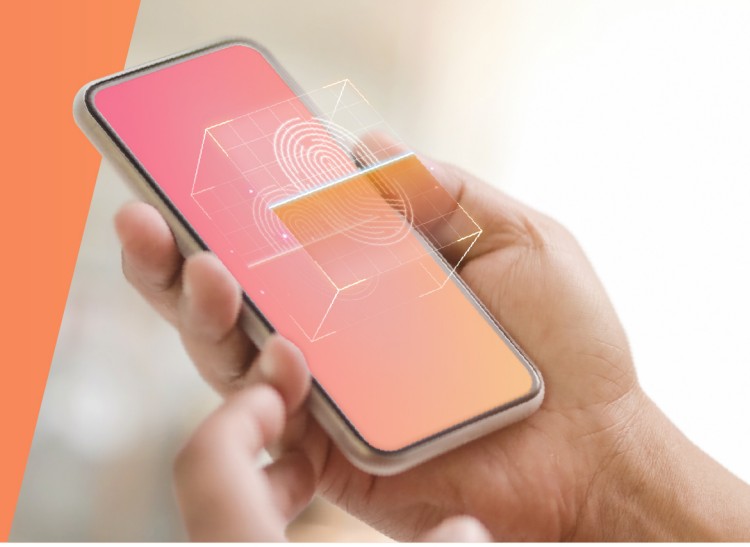
GlobalDots
Cloud Innovation Hunters

The Fastest Zero Trust Browsing & Application Access Solution



Risks beyond the perimeter

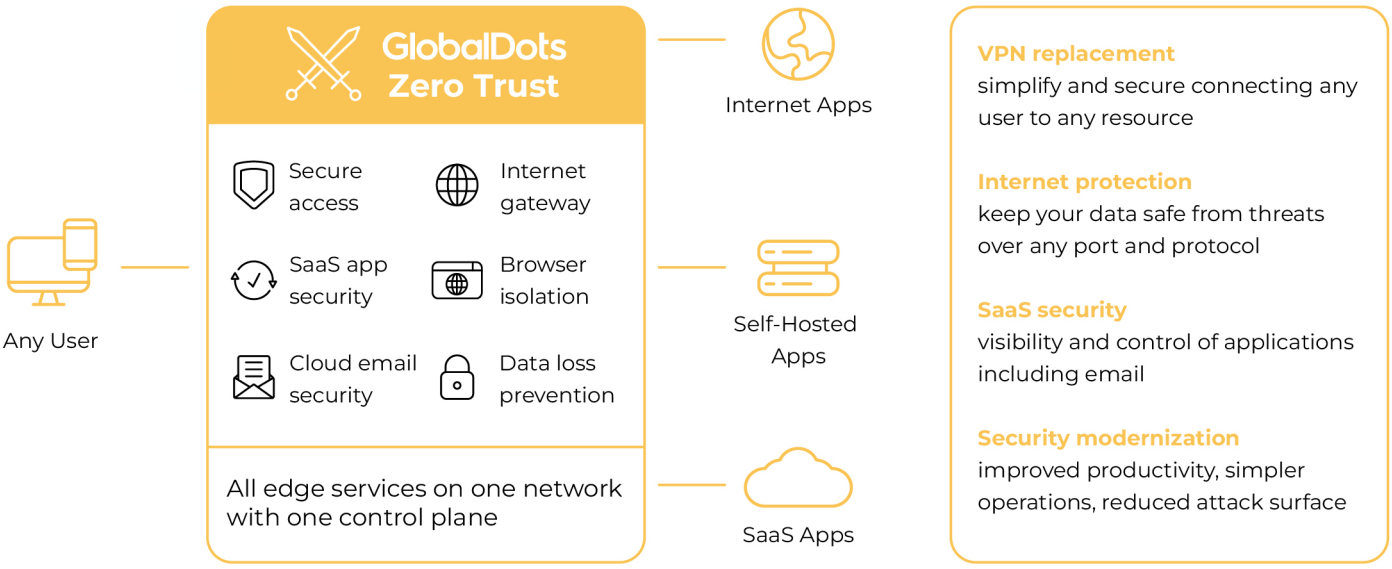
When applications and users left the walls of the corporate perimeter, security teams had to compromise on how to keep data safe. Location-centric methods of securing traffic (like VPNs, firewalls, and web proxies) have broken down under pressure, leaving organizations with limited visibility, conflicting configurations, and excessive risk.

With risks now persisting everywhere, organizations are turning towards Zero Trust delivered in the cloud to adapt.

Adopt Internet-native Zero Trust

GlobalDots offers a security platform that increases visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, traffic is verified, filtered, inspected, and isolated from threats.

It runs on one of the world's fastest Anycast networks across 275+ cities in 100+ countries to deploy faster and perform better than other providers.



Business benefits

Reduce excessive trust

Protect apps with identity and context-based Zero Trust rules. Block ransomware, phishing and other online threats. Isolate endpoints from risks by executing untrusted web code far away from devices.

Eliminate complexity

Reduce reliance on legacy point products and apply standard security controls to all traffic — regardless of how that connection starts or where in the network stack it lives.

Restore visibility

Comprehensive logs for DNS, HTTP, SSH, network, and Shadow IT activity. Monitor user activity across all apps. Send logs to multiple of your preferred cloud storage and analytics tools.

VPN replacement and augmentation (ZTNA)

A faster, easier, and safer way to connect remote users to apps

Challenge: Slow, complex, and risky VPNs

Traditional VPNs are increasingly a liability.
Sluggish performance hurts end user productivity.
Administrators struggle with unwieldy configuration. Plus, VPNs make it easy for malware to spread laterally across a network.

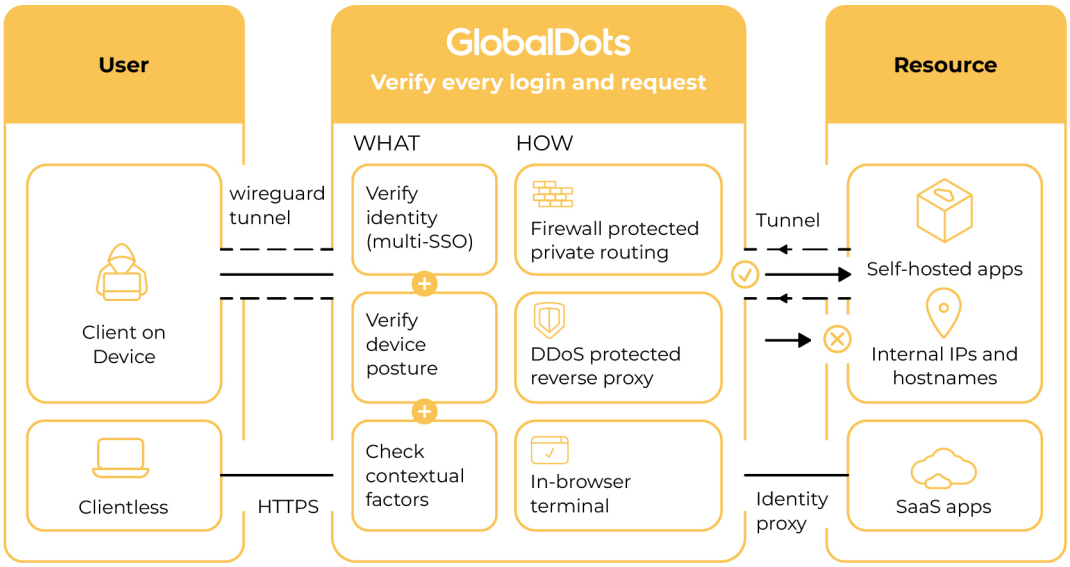
Accelerated cloud adoption and hybrid work have further exposed these flaws and made VPNs more vulnerable.

Zero Trust Network Access (ZTNA)

Our ZTNA service, augments or replaces VPN clients by protecting any application, in any onpremise network, public cloud, or SaaS environment.

Access works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules limiting access to corporate applications, private IP spaces, and hostnames.

How it works



Clientless deployment for web, SSH or VNC-based selfhosted apps accessible via a browser.

Deploy with Our device client to connect to internal IPs, hostnames and non-web apps.

Key use cases

Support remote work and BYOD initiatives

- Verify access for all users, wherever they are, based on identity, device posture, authentication method, and other contextual factors.
- Enforce these Zero Trust policies for your hybrid workforce. Support bringyour-own-device (BYOD) initiatives by securing both managed or unmanaged devices.

Streamline third party access with flexibility

- Speed up access setup for contractors, suppliers, agencies, collaborators, etc.
- Onboard multiple identity providers (IDPs) at once. Set least privilege rules based on the IDPs they already use.
- Avoid provisioning SSO licenses, deploying VPNs, or creating one-off permissions.

Simplify administrative config and support

- Add new users, identity providers, or Zero Trust rules in minutes.
- Unlock new productivity by reducing employee onboarding time and moving away from IP-Based access configuration.
  No need to hire dedicated staff to manage VPNs.

Internet threat and data protection (SWG & RBI)

Filter, inspect, and isolate Internet-bound traffic

Challenge: Evolving threat landscape

Leveling up security while keeping users productive has never been trickier. Remote work means more unmanaged devices storing more sensitive data locally. Meanwhile, ransomware, phishing, shadow IT, and other internet-based threats have been exploding in volume and sophistication.

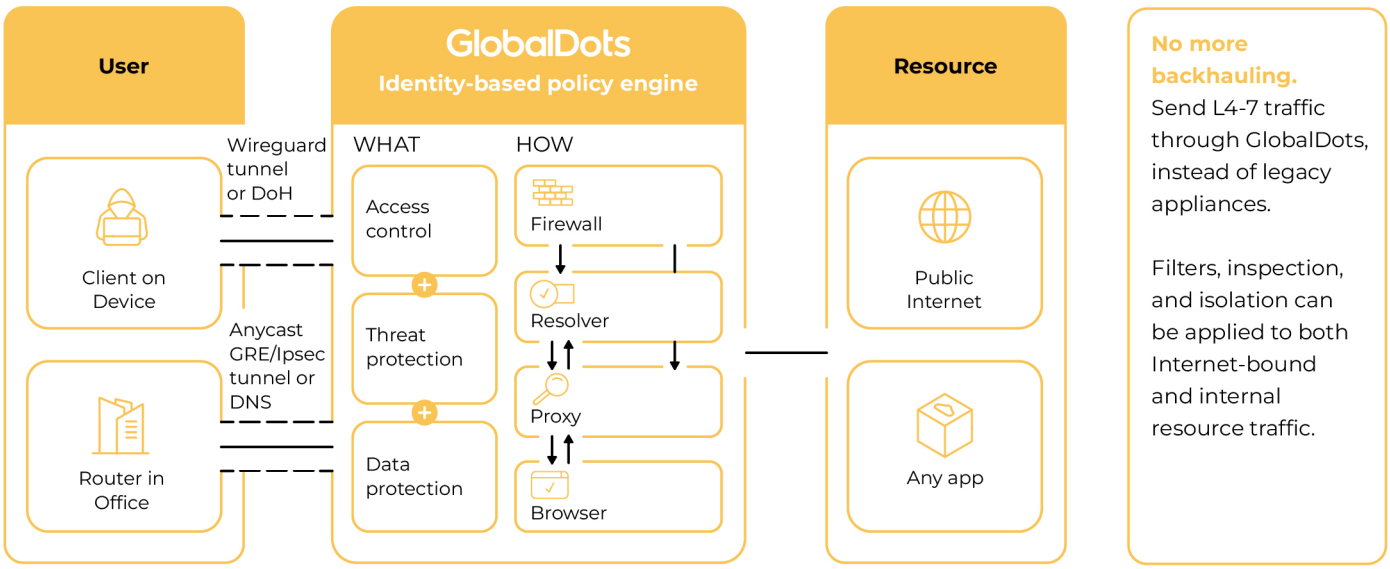
Relying on legacy point solutions and data backups is a risky strategy to guard against the next ransomware threat.

SWG with Zero Trust Browsing

Our Secure Web Gateway (SWG), protects users with identity-based web filtering, plus natively-integrated remote browser isolation (RBI).

Start with DNS filtering to achieve quick time-to-value for remote or office users. Next, apply more comprehensive HTTPS inspection, and finally, extend RBI controls to embrace Zero Trust for all Internet activity.

How it works



Key use cases

Stop ransomware

Block ransomware sites and domains based on our global network intelligence. Isolate browsing on risky sites to bolster protection.

Combine SWG filtering and RBI with default-deny, ZTNA to mitigate the risk of ransomware infection spreading laterally and escalating privileges across your network.

Block phishing

Filter known and ‘new’ / ‘newly seen’ phishing domains. Isolate browsing to stop harmful payloads from executing locally. Stop submission of sensitive information on suspicious phishing sites via RBI’s keyboard input controls.

Prevent data leakage

Implement data loss prevention (DLP) with file type controls that can stop users from uploading files to sites.

Deploy Zero Trust browsing to control and protect the data that lives within web-based apps. Control user actions within the browser – like download, upload, copy-paste, keyboard input, and printing functionalities.

SaaS security (CASB)

Streamline SaaS security for more visibility and control, with less overhead

Challenge: SaaS app proliferation

Modern workforces rely on SaaS applications now more than ever. But SaaS apps are each configured differently, require different security considerations, and operate outside the safeguards of the traditional perimeter.

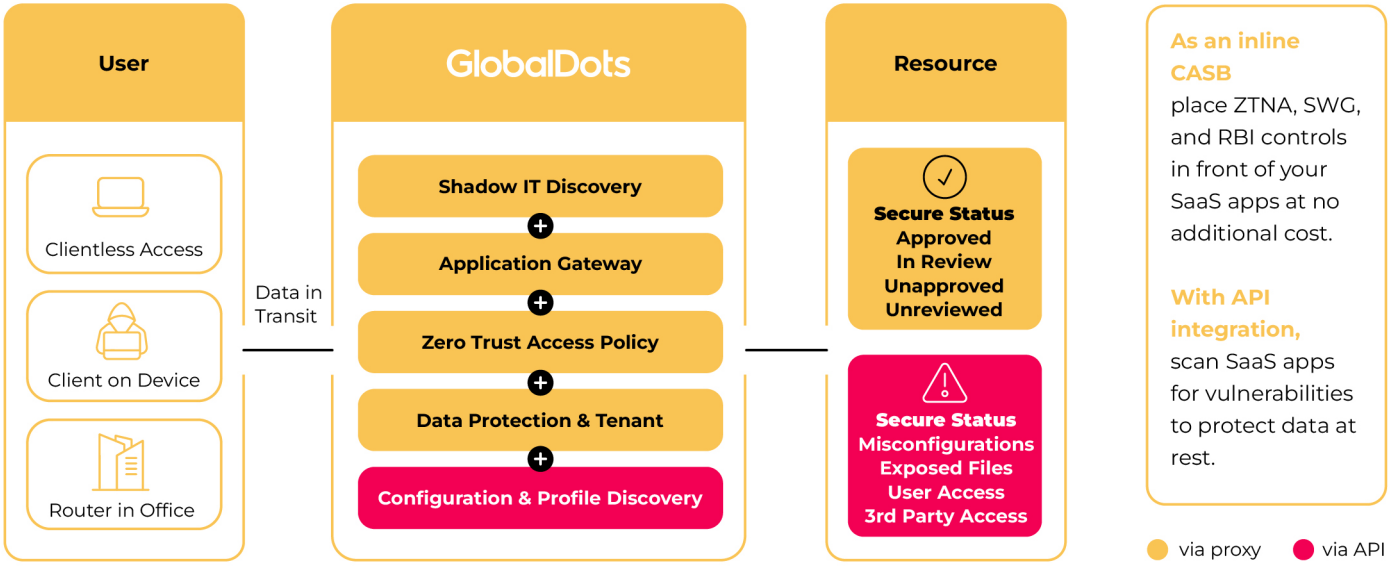
As organizations adopt dozens and even hundreds of SaaS apps, it comes increasingly challenging to maintain consistent security, visibility, and performance.

Cloud Access Security Broker (CASB)

GlobalDots' CASB service gives comprehensive visibility and control over SaaS apps, so you can easily prevent data leaks and compliance violations.

Block insider threats, risky data sharing, and bad actors. Log every HTTP request to reveal unsanctioned SaaS applications. Scan SaaS apps to detect misconfigurations and suspicious activity.

How it works



Key use cases

Apply tenant and data protection controls

Apply tenant control through HTTP gateway policies to prevent users from accessing and storing data in the wrong versions of popular SaaS apps, either inadvertently or maliciously.

Control user actions (e.g. copy/paste, downloads, printing, etc.) within webbased SaaS applications to minimize the risk of data loss.

Mitigate and control Shadow IT

Minimize the risks introduced by unapproved SaaS applications.

GlobalDots aggregates and automatically categorizes all HTTP requests in our activity log by application type. Administrators can then set the status and track the usage of both approved and unapproved apps across your organization.

Identify new threats and misconfigurations

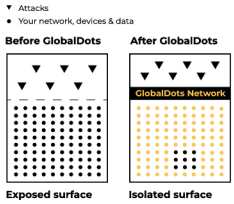
Connect to popular SaaS apps (Google Workspace, Microsoft 365, etc.) via API and scan for risks.

Empower your IT and security teams with visibility into permissions, misconfigurations, improper access, and control issues that could leave their data and employees at risk.

5 ways Zero Trust saves your business time and money

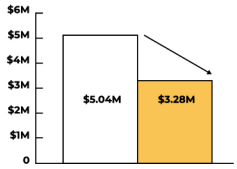
Reduce attack surface

91%



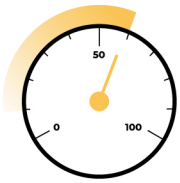
Reduce breach costs

35%



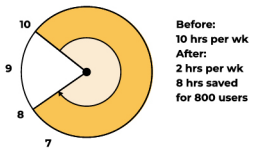
Accelerate employee onboarding

60%



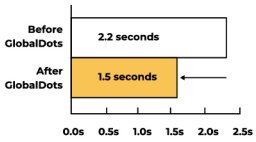
Reduce IT ticket burden

80%



Reduce user latency

39%



About GlobalDots

GlobalDots is a 20-year world leader in cloud and web innovation, connecting over 1,000 global businesses with the latest technologies. Our ever-growing solution portfolio contains over 95 innovative technologies, including: Security, Performance, DevOps, FinOps & Cloud Management, Corporate IT, and advanced AI/ML models. Led by a team of innovation-driven engineers & architects, GlobalDots offers easy end-to-end technology adoption. Proactively introducing newer and better solutions, it helps businesses maintain a scalable, up-to-date technology posture, in a quickly-changing world

Trusted by

BOSCH nuvei SentinelOne Payoneer WiX monday.com

Lufthansa Playtika FIAT AppsFlyer SimilarWeb

GlobalDots
Cloud Innovation Hunters

Contact Us

Follow Us