USE CASE

# SECURING YOUR BRANCH DIRECT INTERNET ACCESS (DIA) CONNECTION

EXECUTIVE SUMMARY

## In today's always-on, digital world, many businesses have branches and satellite offices physically spread all over the globe.

This means that these enterprise users aren't singularly tied to a corporate network. Rather, enterprise traffic is sent over often costly WAN services to a central location irrespective of traffic destination, user type, and device. And finally, the enterprise applications being accessed have shifted from the data center to a hybrid cloud environment, making this hairpinning of traffic through a centralized location even more inefficient.

**ALMOST**

**80%**

of an enterprise's distributed workforce access the network from a branch.[1]

As a result, enterprises with branch offices increasingly rely on Direct Internet Access (DIA) to connect to the public Internet for daily and business-critical activities. An alternative to legacy WAN links and MPLS, DIA can handle the escalating bandwidth requirements dictated by cloud-first and SaaS-heavy environments while keeping both complexity and cost down.

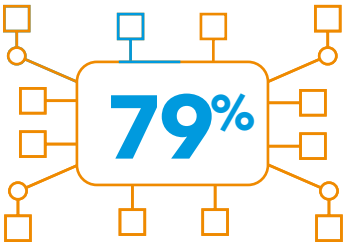
THE URGENCY

## Protecting Your DIA Connection

While DIA connectivity facilitates enhanced Internet performance and improved user experience, it requires a new approach to safeguarding web traffic. Securing corporate web traffic for branches has historically been achieved by backhauling traffic to a central point for inspection and control using on-premise hardware appliances such as enterprise firewalls or Secure Web Gateways (SWGs). But with the use of DIA, traditional security solutions that depend on these central control and inspection techniques are rendered obsolete. In their stead, a combination of firewalls, endpoint antivirus, and replicated hardware and appliance stacks at each branch — across geos — are frequently employed. These quickly become challenging for IT to manage. They are also often inconsistent in performance and costly to maintain. Ultimately, this cobbled-together defense can put a branch, and its users, at high risk.

And of course, ever-present in the background is a cyberthreat landscape that is increasingly perilous and one in which the stakes of a security breach become higher every day.

So how can you easily secure your branch DIA connection, guarding against a debilitating breach?




of business leaders report that their organization is adopting new and emerging technologies faster than they can address related security issues.[2]

**70%**

of businesses that experience a major incident either do not reopen or fail within three years.[3]

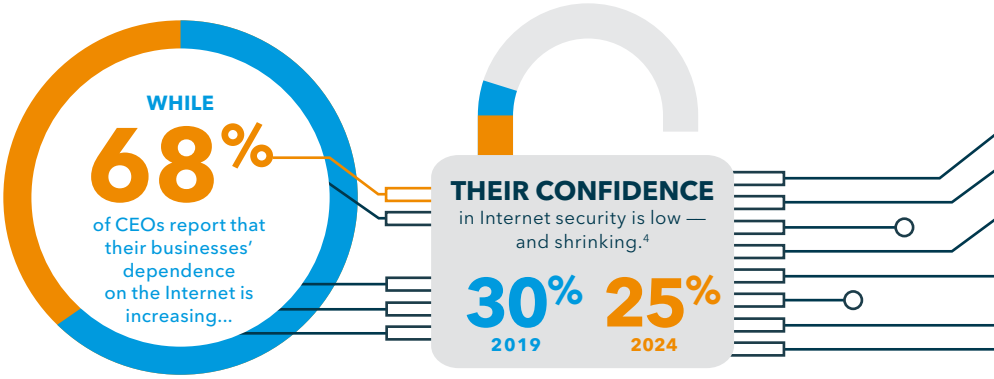
THE SOLUTION

# Using the Cloud for Secure DIA Connectivity

A cloud-based Secure Internet Gateway (SIG) is the answer. Employing such a solution enables security teams to ensure that all users and devices are safely connected to the Internet — protected against malware, ransomware, phishing, DNS data exfiltration, and advanced zero-day attacks — regardless of their affiliation, type, or location. This SIG platform will utilize live threat intelligence and leverage the Domain Name System to provide full visibility into Internet activity, stopping threats over all ports and protocols regardless of whether the user is on or off of the corporate network.

As a cloud-delivered solution, a SIG further shores up branch security through ease and immediacy of deployment, configuration, and scalability. Global, enterprise-wide updates and policy changes can be made in a matter of minutes with 100% compliance from a unified management portal. And as there's no hardware or software to install, ongoing management will be negligible.

Finally, unlike a SWG — which inspects both good and bad traffic through a proxy — a SIG uses DNS as its initial security control point, only sending risky traffic to the proxy for inspection. Safe traffic is sent directly to the Internet. This approach improves performance, eliminates latency, and reduces the volume of broken websites and applications that are the consequence of proxying all traffic. A cloud-based SIG also results in fewer security incidents and false positives, minimizing help desk requests and freeing up IT resources for other more strategic business imperatives.




Visit **akamai.com/etp** to learn more about Akamai's cloud-based and simply managed solution for protecting your branch DIA connection.

SOURCES


1) https://www.riverbed.com/document/fpo/Key-Requirements-for-SD-WAN-RVBD-WP.Final.pdf
2) Accenture Strategy 2019 Report: Securing the Digital Economy, Reinventing the Internet for Trust
3) https://dataconomy.com/2018/03/12-scenarios-of-data-breaches/
4) Accenture Strategy 2019 Report: Securing the Digital Economy, Reinventing the Internet for Trust