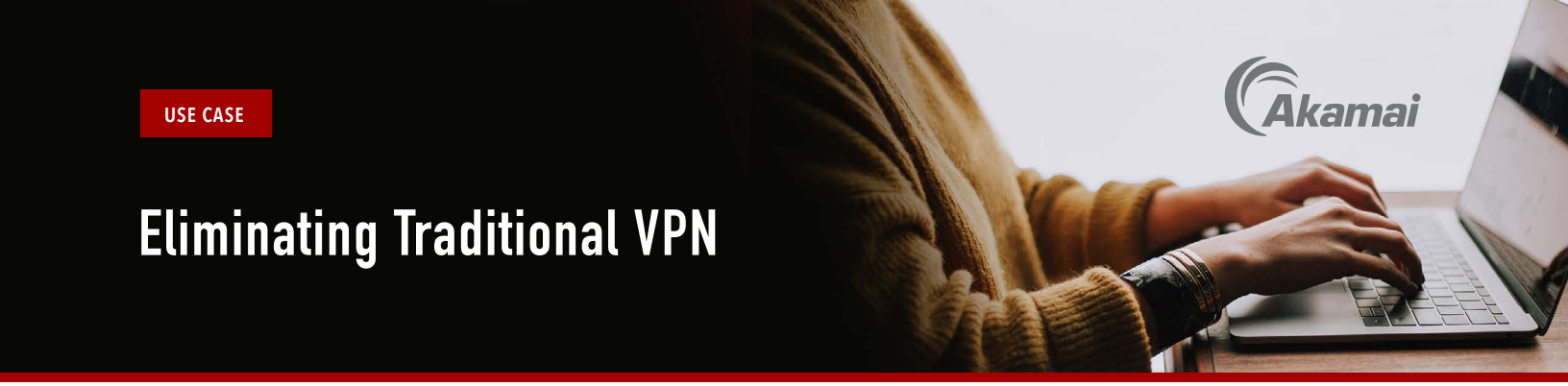
USE CASE

Eliminating Traditional VPN



Executive Summary

The corporate perimeter no longer exists.

We are all acutely aware that workforces are mobile and consist not only of full-time employees, that business is cloud-first, and that enterprise architectures are growing more and more complex. Simultaneously, we know that the cyber threat landscape is increasingly perilous and that the stakes of a security breach become higher every day. Despite the fact that legacy remote access technologies are ill suited for today's perimeter-less digital businesses, many companies continue to use laborious and insecure virtual private networks (VPNs) to provide network connectivity. How do you change in order to protect your network from a breach?

62%
OF COMPANIES REPORT THAT
IT ISSUES
ARE A MAJOR BARRIER
TO DIGITAL TRANSFORMATION INITIATIVES.[1]

THERE WAS A
38% INCREASE
IN APPLICATION LAYER ATTACKS FROM 2016 TO 2017.[2]

What worked years ago — from a management, performance, and security perspective — simply cannot be trusted today. Instead, a modern access solution that supports evolved architectures and a zero trust security model is needed, limiting and customizing access on an application versus network level, authenticating and authorizing every device and user before permissions are granted.

The Inefficiencies and Risks of Traditional VPN

From a technology management perspective, VPNs are highly demanding. They require configuration, deployment, troubleshooting, monitoring, and decommissioning … for each user. As VPNs are ostensibly the gatekeepers of the entire corporate network, they require constant attention. And a number of additional systems are needed to actually support a VPN to deliver daily connectivity, onboarding, offboarding, and general monitoring.

Furthermore, these legacy solutions rely on aging and cumbersome hardware and software, and as a result, can be quite difficult to integrate with the many other components of an enterprise's technology and security stack. The continuous bandwidth required to keep VPNs afloat is not only costly, but also often taps senior IT resources, distracting them from more proactive, impactful, and innovative business imperatives.

As businesses evolve and transition at an unprecedented rate — incorporation, investors, growth, mergers, acquisitions, IPOs, divestitures, failure, and/or success — so too must their technologies and infrastructure. Yet traditional VPNs cannot easily support the demands of such pivots and scaling.

73% **OF ORGANIZATIONS**
REPORT THAT NEARLY ALL OF THEIR APPS WILL BE **SaaS** BY 2020.[3]

74%
OF WORKERS
SAY THAT EMPLOYERS
DO NOT GIVE THEM ACCESS
TO THE LATEST TECHNOLOGY THAT WOULD IMPROVE WORKFORCE EFFECTIVENESS AND EFFICIENCY.[4]

And as more day-to-day operations migrate to the cloud, IT must support, maintain, and replicate stacks of hardware and software across different environments and multiple geographies to operationalize this. The task of delivering customizable access to IaaS, SaaS, and on-premise applications often proves too complex for traditional access solutions.

Eliminating Traditional VPN

ONLY 18% OF COMPANIES

PROVIDE WORKERS WITH THE APPLICATIONS THAT THEY WANT AND NEED — *AND* MAKE THESE APPS ACCESSIBLE ANYWHERE, ANYTIME, ON ANY DEVICE.[5]

In addition to IT challenges, VPNs create headaches for the end user. Connectivity failures, latency, timeouts, disjointed authentication and authorization measures, and erroneous access denials mean a decrease in productivity. This frequently leads to disengagement at an individual level, and will certainly result in an overtaxed help desk.

Lastly, VPNs were not designed with corporate security and privacy as key drivers; rather, they were created as a necessary method of connecting to an organization's internal infrastructure via external, untrusted networks. By their very nature, VPNs punch a hole in the network firewall and typically provide unfettered network access. In the event of a breach, this permits lateral movement and allows access to applications and data beyond those admissible per the user credentials. Traditional VPNs lack intelligence. They can't accurately confirm or validate the identities of those who are trying to access your network or provide a continuously adaptive go/no go based on multi-factor authentication (MFA). It's simply a matter of correct or incorrect user credentials.

TRADITIONAL VPNs LACK INTELLIGENCE.

THEY CAN'T ACCURATELY CONFIRM OR VALIDATE THE IDENTITIES OF THOSE WHO ARE TRYING TO ACCESS YOUR NETWORK.

Traditional VPN Elimination: Using the Cloud for Secure, Simple Remote Access

A traditional VPN, and its plethora of complexities, doesn't align well with the requirements of today's mobile, diverse, and distributed businesses. Configuration, deployment, use, and decommissioning of access should be simple, for both IT and users. And this agility can't come at the cost of security.

Simpler and safer access solutions that can help you move to a zero trust security model already exist in the cloud. These cloud-native tools enable IT to close all inbound firewall ports, and can combine intelligence into decision making — looking at users, devices, and locations, as well as patterns of access, which uplevels security. This is the surest way to achieve seamless, universal access to customized applications, complete with preferred device compatibility and reduced administrative complexities. And through this cloud access architecture, data path protection, identity and access management (IAM), application security and acceleration, single sign-on (SSO), MFA, and more are easily and immediately integrated, managed, monitored, and updated.

Read **"The 4 Benefits of VPN Elimination"** to learn more about adopting a zero trust security model, or visit **akamai.com/eaa** to learn more about Akamai's cloud-based, centrally managed, and easily scalable alternative to an outdated VPN.

SOURCES

1) The Digital Workplace Report: Transforming Your Business, https://www.dimensiondata.com/microsites/-/media/95C5923C59FD4437B870929D3396F891.ashx

2) Akamai SOTI/Security Report, Summer 2018, https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

3) The 2017 State of the SaaS-Powered Workplace Report, https://www.bettercloud.com/monitor/state-of-the-saas-powered-workplace-report/

4) The Staples Business Advantage Workplace Index: Measuring Workplace Trends and Work Culture, https://go.staplesadvantage.com/workplaceindex2016

5) The Impact of a Digitally Empowered Workforce, https://www.vmware.com/radius/report-impact-digitally-empowered-workforce/

Akamai