AKAMAI SOLUTIONS BRIEF

3 REASONS IT NEEDS A NEW APPROACH FOR **THIRD-PARTY REMOTE ACCESS TO SHAREPOINT**

Akamai
FASTER FORWARD

As a centralized content management and collaboration system, Microsoft's SharePoint Platform is used by tens of thousands of enterprises worldwide to share information with employees and third parties. But according to Dimensional Research, 97% of SharePoint stakeholders have security concerns when providing remote access to third parties such as contractors, suppliers, franchisees, partners, and customers. Despite these concerns, 76% of companies still grant these third parties remote access to internal systems.

Given the increased number of data breaches, security concerns are warranted. Existing secure-access technologies are proving increasingly ineffective due to IT landscape disruptions caused by cloud computing and mobile users. Enterprises need a better approach to securing remote access to SharePoint than simply patching and fixing old technologies. Defining a new approach will require that we examine three key pain points impacting the enterprise in this scenario: Complexity, User Experience, and Security.

1. Complexity

The confluence of the growth of third parties accessing corporate applications, together with the skyrocketing growth of data breaches caused by third parties, has led to significant operational demands on enterprise IT, network, and security teams. To securely enable vital information sharing, IT organizations have to navigate and manage a complex maze of people, processes, and technologies.

Deploying, configuring, and maintaining remote access technology is a chronic pain. IT has to touch many systems — including directories, firewalls, VPNs, VDI, end-user devices, etc. — to ensure that remote users can access the applications their jobs require.

Complicating this is the fact that SharePoint is not a 'set it and forget it' technology; it is highly customized for each customer's requirements. A SharePoint implementation requires specialists to manage, monitor, and secure the portal. But according to Dimensional Research, 64% of organizations don't have consistent, ongoing monitoring of SharePoint access.

These systems are now dealt with on a piecemeal basis, requiring constant maintenance updates and human intervention. There is no one central place to manage and control the technologies associated with access. There is no convenient, simple, and fast approach to manage the software, hardware, technologies, policies, and security associated with keeping consultants and supply-chain partners secure. There is no central visibility as to what remote users are doing on your network. All of these complexities lead to increased risk for your organization.

.

2. End-User Experience

It is hardly a secret that SharePoint connections run slowly over a VPN. There are many reasons for this, including VPN traffic tromboning - where traffic originates at a certain point, is forced to follow a particular path on the network, and then turns back to a destination close to where it originated. This can increase latency by 30 to 80ms, often with congestion, leading to sluggish, unpredictable application performance. Conflicts can also arise between different VPN clients and SharePoint, causing either SharePoint to block the VPN or vice versa.

Beyond being a user satisfaction issue, this is a vitally important topic for IT management, because third-party user productivity lost to degraded systems has a direct impact on an organizations' ability to meet financial, manufacturing, and services objectives. If users are waiting for pages to load, dealing with networking issues, opening support tickets, or spending time on the phone with IT help desks, productivity decreases.

3. Security

VPNs have been the de facto solution for enabling secure user access to enterprise applications, including SharePoint, for 20+ years. The core VPN security model has not fundamentally changed: a VPN connects authenticated remote users to an organization's entire internal network. But VPNs have several serious security drawbacks.

VPNs give devices — and their users — full network access privileges whether they need it or not. If your company has a significant number of remote users and third parties who are accessing internal corporate applications, a VPN is a poor solution. After all, you don't want to give users carte blanche to the network when all they need is access to a few specific applications.

Defining a New Access Architecture

To address these three pain points, enterprises need a new architecture for providing remote access to their SharePoint application portals. Whether running in a private data center or a hybrid cloud environment, SharePoint needs to be delivered to users with greater security and simplicity. Enterprises need a new access architecture that meets today's challenges by:

- Limiting user access to only the SharePoint front end, not the network
- Enabling highly secure access to SharePoint while decreasing IT support requirements
- Delivering a high-performance, simplified user experience

THE ENTERPRISE APPLICATION ACCESS SOLUTION

Enterprise Application Access (EAA) delivers a new remote access approach that meets and exceeds the requirements of this new access architecture for all applications hosted behind data center firewalls and hybrid cloud environments – including SharePoint. EAA's solution is secure, simple, and convenient. Unlike existing network security approaches, EAA:

- Ensures SharePoint application users only get access to the SharePoint portal – and nothing else on the network. EAA's unique dual-cloud architecture closes all inbound access to your infrastructure, reducing your attack surface. No one can get to apps directly; applications are hidden from the Internet and public exposure
- Provides secure access to SharePoint in minutes. Initial deployment and ongoing support are a snap as there are no network changes, endpoint clients, or truck rolls required. The IT workload is lightened substantially, enabling teams to work on more strategic initiatives
- Enables a fast, seamless, and hassle-free end-user experience. Instead of using a cumbersome VPN client, end users gain access to applications through any browser or mobile app; they simply enter their credentials - username, password, and optional multi-factor authentication – to identify themselves and are dynamically provisioned access to private enterprise applications

Akamai Transforms Remote Access, Putting you Back in Control

Approaching the problem in a fundamentally different way, Enterprise Application Access is an SaaS service that delivers access to applications like SharePoint without providing user access to your entire network. With EAA, you get a centralized managed solution that does not require external hardware or software. Managing and controlling third-party — as well as customer and employee — access becomes simple and uncluttered, and with the elimination of complexity comes fundamentally better security.

EAA removes the chronic pain suffered by IT teams associated with managing internal and third-party access to SharePoint. It is easy to deploy, provision, change, and monitor. EAA removes all the complexity: no device software, no software upgrades or updates, and no additional hardware. As a central point of entry and control, EAA provides a single management pane for detailed audit, visibility, control, and compliance reporting. The result is a new approach for third-party remote access to SharePoint applications.

Akamai FASTER FORWARD

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable, and secure for its customers. The company's advanced web performance, mobile performance, cloud security, and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise, and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.