Providing employees with secure access to enterprise applications deployed behind the firewall is a core requirement for all businesses. Increasingly, enterprises must also deal with the riskier proposition of providing this same access to third parties, including their contractors, partners, suppliers, and customers. Enabling secure application access, whether hosted in a public cloud or private data center, is a complex, cumbersome task requiring on-premise hardware and software such as Application Delivery Controllers (ADCs), Virtual Private Networks (VPN), Identity Management Systems (IAM), and more. Yet with all of these technologies, enterprises are exposed to a variety of security risks, now compounded by the growing network presence of untrusted third-party users. Fortunately, Akamai’s Enterprise Application Access solves these problems and helps enterprises transform remote access to meet today’s mobile and cloud-centric requirements while improving an organization’s overall security posture.

**Enterprise Application Access**

Enterprise Application Access is a new approach to remote access. It provides a unique, secure, and more convenient alternative to traditional remote-access technologies such as VPNs, RDP, and proxies. With Enterprise Application Access, no one can get to applications directly because they are hidden from the Internet and public exposure. A unique cloud architecture closes all inbound firewall ports while providing authenticated end users access to only their specific applications. Enterprise Application Access integrates data path protection, identity access, application security, and management visibility and control into a single service.

Enterprise Application Access can be deployed in minutes through a unified portal with a single point of control, in any network environment, and at a fraction of the cost of traditional solutions. The result is a secure-access delivery model that enables a zero CapEx, low OpEx model for critical workloads deployed in any environment.

**How it Works**

Enterprise Application Access provides secure access as a service that eliminates the need to punch holes in the network perimeter. Instead, users access applications through the cloud, which stops and secures user access far outside your network. With Enterprise Application Access, there is no direct path into your applications. Instead, Enterprise Application Access dials out a secure, mutually authenticated TLS connection from within your network or cloud and brings the application to the user.

Since there are no tunnels, there is no path for malware to land inside your network and potentially spread to sensitive or privileged systems. All user connections are stopped in the cloud, terminating on secure proxies while applying strong authentication and security controls. You can add your own security controls for increased protection of highly sensitive applications.

Enterprise Application Access makes accessing applications fast and intuitive for end users. Forget the support calls for poor application performance, VPN connectivity issues, and device incompatibilities. Enterprise Application Access optimizes applications and presents them in any browser on any user device — and with enterprise-grade single-sign-on and intelligent multi-factor authentication, security is no longer a burden for users or IT.

Enterprise networks are not a problem for Enterprise Application Access. With one-click integrations for Active Directory, SAML providers, CDNs, forward proxies, SIEM tools, and other infrastructures, custom scripting and integration are eliminated. Scaling and deploying apps across public and private infrastructures is a snap with built-in high-availability capabilities, server load balancing, and automatic application routing.
ENTERPRISE APPLICATION ACCESS

The Rise and Risks of Independent Workers: Why this is an Urgent Problem
Why is this new paradigm for application access required? It is essential that outside contractors and suppliers have access to specific internal private corporate applications to be productive. Today, this usually means giving them VPN access. But any kind of third-party access creates additional points of entry to an organization’s network, increasing the overall risk that critical corporate information – proprietary documents or customer data – could fall into the wrong hands. Unfortunately, the abuse of third-party access is a significant source of data breaches today, including:

• According to a 2016 Trustwave report, from 2015 to 2016, data breaches due to third-party remote access rose from 12.5% to 29.7%
• CyberArk’s 2016 Threat Landscape Survey found that 49% of organizations allow third-party vendors remote access to internal networks
• Accidental breaches caused by third-party suppliers accounted for 30% of overall breaches according to Beazley’s Breach Insights in 2017
• Global Workplace Analytics reports by 2020, more than 40% of the U.S. workforce will be contingent workers

The Challenge: Managing Remote Application Access is Painfully Complex
The growth of third parties, employees, and even customers accessing corporate applications, combined with the skyrocketing growth of data breaches, has also lead to massive, untenable operational demands on 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 secure-access technology is a chronic pain.

These systems are currently 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 application 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 third parties are doing on your network. All of these fragmented factors lead to increased risk for your organization.

The implications to your organization are enormous, with the complexity and increased risk resulting in lost:

• Time – IT, security, and management teams are losing time — time that could be spent on higher-priority projects — because they are preoccupied with the monitoring and management of employee and third-party access
• Productivity – Employees and contractors lose productivity due to delays in onboarding and subsequent changes, such as adding access to new applications. You want your workers productive in minutes, not days or weeks
• Data – The inability to effectively monitor access activity on your network could easily lead to a network breach, resulting in the loss of data or intellectual property
• Money – Ponemon’s 2016 Cost of Data Breach Study reports the average cost of a data breach is over $7 million
• Corporate Reputation – Ponemon Institute’s research shows the negative press associated with a data breach may lead to fewer customer acquisitions and a higher churn rate of employees

MARKET CONDITIONS
In today’s connected mobile world, companies are using outside resources more than ever to help stay competitive. For example:

• The Bureau of Labor Statistics classifies more than 10 million workers, comprising 7.4% of the U.S. workforce, as independent contractors.
• According to Gartner, the supply chain management (SCM) market will exceed $13 billion in total software revenue by the end of 2017, up 11 percent from 2016.
• Today’s environment also has another truth: the number of enterprise breaches — and their risks and costs — continues to grow, seemingly unabated.
• Ponemon’s 2016 Cost of Data Breach Study reports the average cost of a data breach is over $7 million.
• In 2016, U.S. companies and government agencies suffered a record 1,093 data breaches, a 40 percent increase from 2015, according to the Identity Theft Resource Center.
Akamai Transforms Remote Access, Putting you Back in Control

Approaching the problem in a fundamentally different way, Akamai now offers Enterprise Application Access — an SaaS service that delivers access to applications without providing users access to your entire network. With Enterprise Application Access, 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. The elimination of the complexity results in fundamentally better security.

Enterprise Application Access removes the chronic pain suffered by IT teams associated with managing third-party access. It is easy to deploy, provision, change, and monitor. Enterprise Application Access removes all the complexity: no device software, no software upgrades or updates, and no additional hardware. User management difficulties — from onboarding to offboarding — are a breeze. As a central point of entry and control, Enterprise Application Access provides a single management pane for detailed audit, visibility, control, and compliance reporting. The result is painless, secure application access.

The Akamai Ecosystem

Akamai makes the Internet fast, reliable and secure. Our comprehensive solutions are built on the globally distributed Akamai Intelligent Platform, managed through the unified, customizable Luna Control Center for visibility and control, and supported by Professional Services experts who get you up and running easily and inspire innovation as your strategies evolve.