Pulse Secure®

The Secure Access Checklist

How to ensure Secure Access usability, protection and compliance for data center and multi-cloud

Access without Compromise

Secure Access ensures that authorized users can securely connect to applications and information at any time, from any location, using any device, over any network.

Secure Access is critical for today's workforce as it is an enabler of digital transformation, empowering employees, customers, peers, and partners to work, communicate, and collaborate seamlessly.

Traditionally, security has been primarily about control: IT administrators enforce rules to meet business requirements and adhere to compliance obligations. This approach can result in a less-than-optimal user experience (UX), causing users to seek workarounds in order to get their jobs done. The growth of shadow IT is proof positive that users are very adept at leveraging unsecured personal devices or unsanctioned cloud services to address the tasks at hand.

Secure Access, in contrast, is designed with a seamless, protected user experience in mind. It is a model based on enablement rather than restriction. The objective is to deliver simple and frictionless access to enterprise information, applications and services without compromising security – all while making it easy and flexible for IT to implement, manage and adapt security policies to align with an ever-changing environment and evolving business requirements.

To make the move effectively from a control-based approach to an access-based approach, it is critical for businesses to understand the trends that are impacting Secure Access today, and the elements required to ensure global security while delivering any-means access.

Secure Access at a Glance

Secure Access mitigates business risk to corporate data, applications and IT assets by:

Enhancing user and device visibility and insight

Prohibiting access by unauthorized users

Eliminating the risk of compromised devices

Preventing the use of non-secure network connections

Blocking the spread of insider threats and infections

Reducing Internet of Things (IoT) exposures

The Importance of Secure Access Visibility and Compliance

Hidden Breaches

97% of organizations have experienced a breach; of those breached, the breach went undetected for an average of 134 days (Gigamon, 2015)

Exploding Ransomware

Ransomware damage costs exceeded $5 billion in 2017, up more than 15X from 2015, and it is predicted that ransomware will attack a business every 14 seconds by the end of 2019 (Cybersecurity Ventures, 2017)

Trends Shaping the Delivery of Secure Access

IT teams are on a constant treadmill of change, driven by five major trends.

1. **The consumerization of IT is revolutionizing.** It has completely changed the nature of today's workplace and contributing to digital business transformation. Enterprises are confronted with proliferation of smart devices and online apps. Millennials, who will represent almost fifty percent of the workforce by 2020, are tech savvy and accustomed to a rich, on-the-go personal digital experience – and they expect a similar digital experience at work using their own mobile devices. Enterprises are challenged to support workforce dynamics and deliver this consumer-like user experience for their employees without compromising key compliance and security requirements.

2. **Networks are increasingly under attack.** With new cyberthreats and data leakage in the headlines on a regular basis, security breaches have reached crisis proportions. Reducing the Mean-Time-to-Detect (MTTD) and Mean-Time-To-Respond (MTTR) to vulnerabilities and incidents has never been more important for organizations than it is now. Visibility, real-time prevention and automated response are critical for IT to combat threats that are the result of insider activity, privilege misuse, non-compliant and unsanctioned devices and device loss.

3. **The rise of cloud computing and hybrid IT environments.** The traditional data center-based application environment is morphing rapidly into a blended enterprise, cloud and cloud service environment. In this new world, IT resources can take the form of an enterprise's own private cloud or of third-party public clouds, including Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings.

   For many organizations, multi-cloud has become the new normal. While it would be nice to believe that the cloud is intrinsically secure, it's not that simple. The primary product offering of cloud providers such as Google and Amazon Web Services (AWS) is space, processing power and bandwidth – not security. To ensure appropriate and protected connectivity to applications and information, businesses need Secure Access solutions that can support a hybrid IT implementation.

4. **Use of multiple security silos for enterprise access.** Hybrid IT environments contribute heavily to the fourth trend as IT extends existing data center security policies to cover IaaS and SaaS situations. Unfortunately, the use of point solutions to address access security within different computing environments frequently leaves gaps, limits visibility and yields inconsistent policies. This also often results in a complex and frustrating user experience. In a 2017 report by ESG, 66% of cybersecurity and IT professionals agreed or strongly agreed that security analytics and operations effectiveness is limited because it is based upon multiple independent point tools.

5. **The Internet of Things (IoT) is exploding.** Printers, smart TVs, personal WiFi, security cameras, sensors, and other peripheral devices are becoming commonplace at work. These devices are all connected via laptops, desktops, smartphones, or directly on enterprise networks and often further connected through IP networks to other corporate and third-party resources. The security of these systems, from changing default passwords to installing patches, is often an afterthough at best – leaving most IoT devices vulnerable to attack and misuse. Typically, organizations are unaware of these devices, and the myriad ways the are connecting to their internal systems and data. Hackers therefore view IoT as a new opportunity for targeted attacks, taking advantage of security weaknesses and employee ignorance alike. To gain control of the risks posed by the IoT, organizations need end-to-end visibility, contextual awareness, and real-time action.

The Requirements of a Secure Access Solution

What are the critical elements of any successful Secure Access solution?

Integrated mobile security	First, a Secure Access solution must **enable enterprise mobility** to boost workforce productivity. This requires the means to enable visibility and compliance controls in as transparent way and across different devices and operating systems. This involves simplifying the secure use of mobile devices by offering automated, self-service onboarding of devices – whether they are laptops, smartphones, or tablets – regardless of user location and device ownership. Mobility enablement also requires the ability to ensure compliance by isolating work applications and data from private applications. Lastly, a Secure Access solution must support always-on and per-app virtual private networking.
Simple and easy-to-use UX	A Secure Access solution must also take into consideration users' consumer-based expectations for a **simple, integrated user experience** (UX). For example, end users want the convenience of Single Sign On (SSO) to applications across devices, operating systems and application infrastructures. IT administrators demand an intuitive and flexible way to orchestrate all elements of access security – freeing them from the need to correlate data and actions across multiple security systems and consoles. Additionally, a best-in-class Secure Access solution will optimize the user experience by leveraging an integrated Application Delivery Control (ADC) solution, guaranteeing timely response to meet any demand, regardless of whether users access applications on site or remotely.
End-to-end hybrid IT security	The increase in cyberattacks coupled with the move to hybrid IT environments means that a Secure Access solution must offer **end-to-end hybrid IT security**. Such a solution should combine SSO authentication with role-based and device-compliant authorized access to applications, whether the applications are hosted in enterprise data centers, private clouds, or public clouds, or are delivered as SaaS. The solution needs to provide user, device and application visibility across the hybrid IT environment, as well as ensure enterprise-wide compliance, reporting and mitigation of security issues.

The Importance of Secure Access Visibility and Compliance

Unpatched Devices:
More than 1 in 4 financial devices is operating with known vulnerabilities for which security updates are available (Symantec, 2017)

Unauthorized Access:
An average of 44% of network-connected printers within organizations are insecure in terms of unauthorized access to data stored in the printer mass storage (HP, 2015)

Unified and scalable platform	The difficulties associated with multiple security siloes can be mitigated by adopting a **unified Secure Access platform**. A unified platform provides appropriate application access that supports physical and virtual IT resources across on-premise and cloud environments and across classic PCs and mobile devices. Such a unified platform must be sufficiently scalable to handle the steady expansion of connections, applications and workloads over time, as well as the bursts of capacity required during times of peak usage such as for natural disasters and man-made emergencies.
Unified policy engine for users, devices and applications	**Policy unification** is another way to combat the gaps that can be created by multiple security siloes. Unlike siloed solutions, policy unification enables rules to be written once and automatically applied enterprise-wide. The unified policy engine must be context-aware to enable the enforcement of granular policies based on user, role, device, location, time, network and application, as well as endpoint security state. To minimize IT administrative workloads and ensure interoperability with third-party solutions, policy enforcement should be standards-based.
Seamless integration across multiple vendor solutions	Establishing a unified platform and a unified police engine is made easier and effective by partnering with a single vendor who can **orchestrate Secure Access controls across multiple vendor solutions**. To minimize IT administrative workloads, bi-directional interoperability should be standards-based and support a variety of third-party solutions. Applying this approach allows a single vendor to incorporate new technologies as they become available and enable greater enterprise availability, resiliency, elasticity and scalability.
Extensibility to new endpoints, services and applications	Finally, as demonstrated by the proliferation of IoT devices, a Secure Access solution must be **intelligent and adaptable**. Within a corporate network, a Secure Access platform must facilitate accounting for and applying policy to both sanctioned and unsanctioned IoT devices – monitoring activity and protecting network resource use. In addition, there will be applications that require IoT accessability and management of IoT devices – requiring Secure Access functionalities such as device profiling and classification, advanced analytics and policy-based control. Overall, Secure Access solutions must be sufficiently flexible to accommodate future use cases without compromising availability, performance, compliance, or security.

The Importance of Secure Access Visibility and Compliance

Vulnerable Data:
28% of corporate data resides exclusively on laptops, smartphones, and tablets (Gartner, 2017)

Expanding IoT:
8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020 (Gartner, 2017)

Secure Access for Today and Tomorrow

Ensuring global security while delivering any-means application and data accessibility is a challenge, given the current trends of workforce mobility, dynamic and evolving threats, multi-cloud environments and IoT – all impacting IT. Through a comprehensive, flexible and intuitive Secure Access soluton that can account for user experience, endpoint diversity and threats, hybrid cloud migration, platform and policy unification and ecosystem interoperability, IT can more effectively define, implement and evolve an end-to-end Secure Access strategy.

With a Secure Access solution in place, enterprises can enforce policy compliance by employees, guests and contractors regardless of location, device type, or device ownership. Users enjoy greater productivity and the freedom to work anywhere without sacrificing access to authorized network resources and applications. IT can mitigate malware, data loss and IoT risks. And IT is empowered to optimize their resources and enable digital transformation across the enterprise.

With Secure Access protecting networks, core assets, applications, data, and more, businesses can position themselves for success — today and into the future.

Pulse Secure Delivers Enterprise Secure Access

At Pulse Secure, Secure Access is in our DNA. Put simply, we are 100% focused on delivering Secure Access solutions for people, devices, things and services. For years, enterprises of every size and industry have trusted our integrated virtual private network, network access control, and mobile security solutions to enable Secure Access seamlessly in their organizations.

Here are a just a few highlights on how our solutions addresses the Secure Access checklist:

Integrated mobile security

Pulse Workspace provides a simple-to-deploy Enterprise Mobility Management (EMM) solution that combines policy-based connectivity with a secure device container for enterprise applications. In addition, the Pulse Secure solution also integrates seamlessly with other popular EMM solutions such as MobileIron, AirWatch and Microsoft Intune.

Simple and easy-to-use UX

IT can use the Pulse Client to deliver seamless, secure and reliable user access to all company resources, in the cloud or data center, via a single client or mobile application. With advanced features such as SSO, the Pulse Client dramatically simplifies the user experience and increases user productivity.

End-to-end hybrid IT security

The Pulse Secure solution is an easy to deploy and use system that provides 360-degree visibility with security enforcement to control managed, unknown and IoT devices connecting locally or remotely to the data center or cloud. With a comprehensive and dynamic view of users and devices, IT can enforce granular policies to ensure compliance with industry regulations and corporate policies regardless of user, device or application location.

Unified and scalable platform

Secure Access solutions from Pulse Secure are powered by the Pulse Secure Appliance, designed to flexibly meet the access challenges of any enterprise with appliances that scale from 200 to 25,000 concurrent sessions and form factors that accommodate data center, office and cloud environments. Integrated ADCs help scale and bulletproof user access to time-critical information and mission-critical applications with global load balancing and geographic redundancy for both the cloud and data center.

Unified policy engine for user, devices and applications

Administrators can configure contextual access policies with Pulse Secure to manage access to the cloud and data center based on devices, locations, resources, users, groups and endpoint profiling. The solution also extends policies to the internal networks, allowing organizations to identify, profile, secure and manage internal devices, provide guest user access and secure Bring Your Own Device (BYOD) endpoints.

Seamless integration across multiple vendor solutions

Pulse Secure boosts the security intelligence of next generation firewalls, access points and switches by providing enhanced identity and device context for granular enforcement and automated mitigation. The Pulse Secure solution also interoperates with existing infrastructure investments in directories, PKI and strong authentication with extensive support for 802.1X, RADIUS, LDAP, Microsoft Active Directory, RSA Authentication Manager and others.

Extensibility to new endpoints, services and applications

As our customers move to the cloud, their Pulse Secure solution is extending their existing security policies for a single security standard that uniformly protects both the data center and cloud. Similarly, our solution is also helping existing customers secure and harness IoT devices, further demonstrating that their trusted Pulse Secure solution can protect enterprise information no matter where it is stored or how it is accessed.

Pulse Secure offers a comprehensive, unified, interoperable and scalable Secure Access platform that securely connects workers to company resources and protects company devices, regardless of location – in the data center, internal network, cloud, or mobile. That's why some of the world's largest and most security conscious organizations rely on Pulse Secure solutions and trust our expertise and know-how.

80%
of the Fortune 500

40
of the Fortune 50

13 of 15
US government cabinets

20,000+
customers with 18 million secured endpoints

200
Secure Access patents