ivanti

The Zero Trust Secure Access Checklist

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

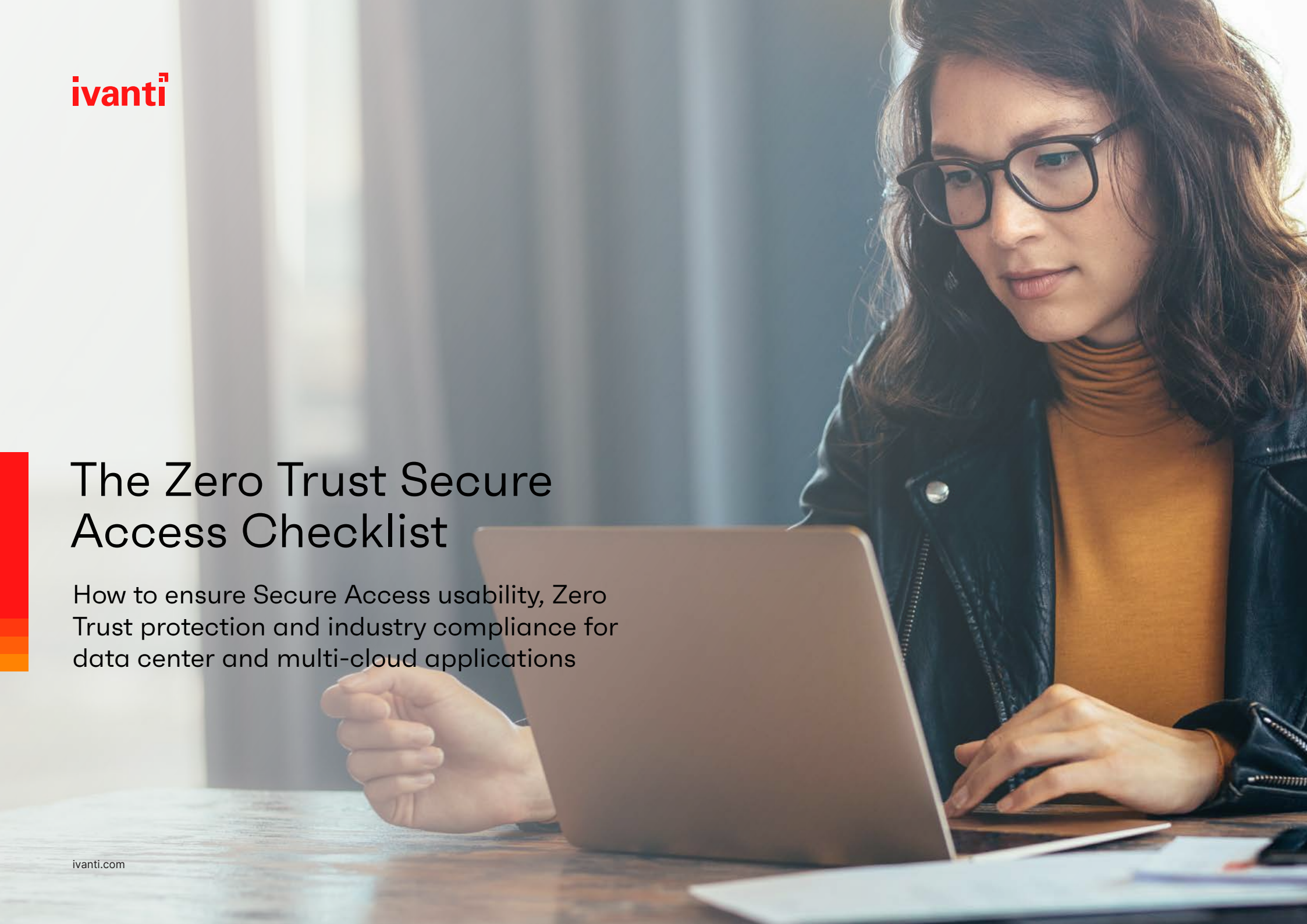


Table of Contents

Secure Access in a Zero Trust World

Secure Access ensures that in a Zero Trust world only authenticated users with compliant devices can connect to authorized applications and information at any time, from any location, 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. However, with new cyber threats and security breaches in the headlines, companies must also ensure a balance between productivity and security.

Traditionally, this has been a difficult goal given that security was predicated primarily on 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 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, simple user experience in mind that also provides Zero Trust protection. 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 that align with an ever- changing environment. Zero Trust assumes that nothing inside or outside of the enterprise perimeter should be trusted and the network must verify anyone and anything trying to connect before granting access. Connectivity is only granted after identity is authenticated, the security posture of the connected device is verified, and the user or thing is authorized to access the desired application, service or information.

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

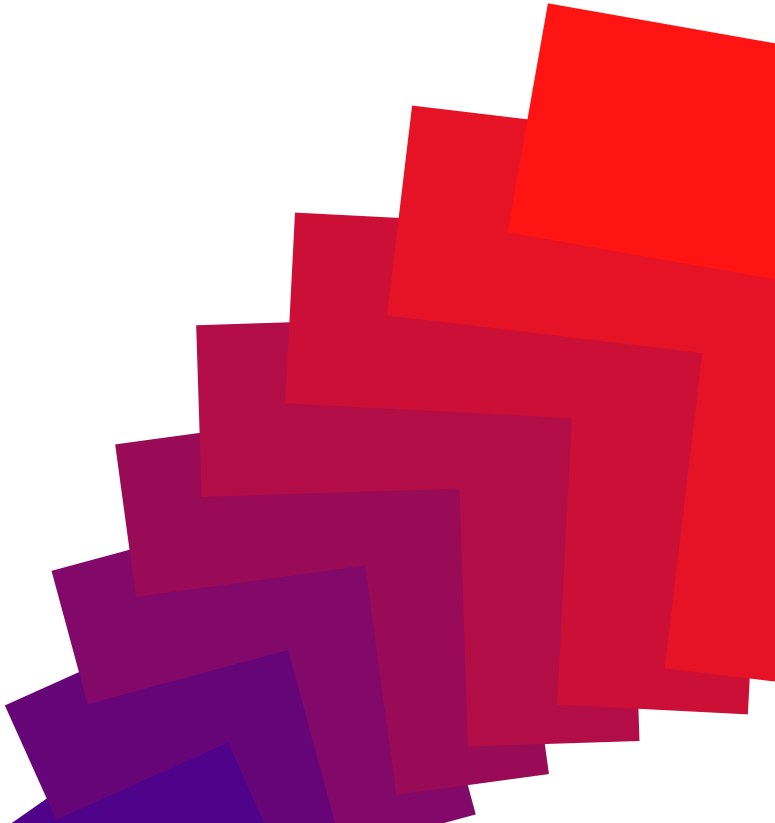
The Importance of Zero Trust Visibility and Compliance

Financial Consequences:

Companies that contained a breach in less than 30 days saved over $1 million verses those that took more than 30 days to resolve. (Ponemon and IBM, 2018)

Exploding Ransomware

In 2016 Microsoft reported that ransomware cost approximately $325 million in damages and it is predicted to rise to $11.5 billion by 2019 with a ransomware attack taking place every 14 seconds. (Cybersecurity Ventures, 2018)



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 cyber threats and data leakage in the headlines, 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. 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 Cloud computing and hybrid IT environments are the norm.

The traditional data center environment has morphed into a blended enterprise, cloud and cloud service environment. In this new world, IT resources are typically deployed in an enterprise's own private cloud or leverage third-party public clouds, including Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings.

Even though multi-cloud has become the new normal, cloud security still may not be as trusted as traditional data center protection. After all, 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 extend proven data center security to the cloud.

4 Use of multiple security silos for enterprise access.

Hybrid IT environments contribute heavily to this 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. 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 afterthought at best – frequently leaving IoT devices vulnerable to attack and misuse.

Typically, organizations are unaware of these devices, and the myriad of ways they are connecting to their internal systems and data. With the rise of Industry 4.0, which uses IoT and cloud to boost manufacturing output, cybersecurity concerns are now bleeding over from IT into the operational technology (OT) domain. Hackers now 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 IoT, organizations need to redesign their security architecture for IT and OT 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 Zero Trust Secure Access solution?

✓ **Integrated mobile security**	First, a Zero Trust Secure Access solution must **enable enterprise mobility** to boost workforce productivity. This requires enabling visibility and compliance controls in a transparent way across different devices and operating systems. It 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 in BYOD scenarios. Lastly, a Secure Access solution must support always.
✓ **Simple and easy-to-use UX**	A Zero Trust 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 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 & visibility**	The increase in cyber attacks coupled with the move to hybrid IT environments means that a Zero Trust 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. Software Defined Perimeter (SDP) offers a compelling, "Zero Trust" architecture that can be applied to new or existing hybrid IT deployments. SDP prescribes an "authenticate and verify first" approach that renders resources invisible or inaccessible to all users and devices until an explicit authentication, compliance check, and authorization have been completed. The overall result is a "dark cloud" where the attack surface of the network is diminished because hackers can't attack what they can't see.

The Importance of Zero Trust Visibility and Compliance

Unpatched Devices:

Ransomware vulnerable: more than 1 in 4 financial devices is operating with known vulnerabilities for which security updates are available (Symantec, 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)

Vulnerable Data:

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

Expanding IoT:

Communications and interoperability between OT and IT systems increase vulnerability for manufacturing systems, as highlighted by WannaCry ransomware which halted or reduced the output of at least five Renault-Nissan car plants. (Business Insider, 2017)

✓ **Unified and scalable platform**	The difficulties associated with multiple security silos can be mitigated by adopting a **unified Zero Trust Secure Access platform**. A unified platform provides appropriate application access that supports physical and virtual IT resources across on-premise and cloud environments. It must also provide endpoint coverage across classic PCs, mobile and even IoT devices, requiring the application of agent and agentless Client technology.
✓ **Unified policy engine for users, devices, and applications**	Policy unification is another way to combat the gaps that can be created by multiple security silos. Unlike siloed solutions, policy unification enables rules to be written once and automatically applied enterprise-wide. SDP architectures offer a unified and centralized policy engine that is context-aware, enabling 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 policy engine is made easier and effective by partnering with a single vendor who can orchestrate Zero Trust 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 growing need for IoT and multi-cloud security, a Zero Trust Secure Access solution must be intelligent and adaptable. The solution must be able to discover, segment and monitor sanctioned and unsanctioned IoT devices on the network and private cloud employing advanced device profiling, classification, analytics and threat response. Furthermore, as IOT devices interface with corporate application including IT and OT (Operational Technology) convergence, Secure Access functionality must be sufficiently flexible to accommodate future use cases without compromising availability, performance, compliance, or security.

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 solution 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 Zero Trust enforcement.

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.

Delivering Enterprise Secure Access

At Ivanti, 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. Now with SDP, Ivanti is further advancing Secure Access with mandatory Zero Trust policy enforcement and the rendering of IT assets "dark" to hackers.

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

- **Simple and easy-to-use UX**
  IT can use the 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 and Zero Trust access, the Client dramatically simplifies the user experience and increases user productivity. SDP applications and apply access security to IOT devices where a client is not needed or possible to use.

- **End-to-end hybrid IT security**
  The Ivanti solution is an easy to deploy and use system that provides 360-degree visibility with security enforcement to control hybrid IT connectivity. The Ivanti solution can be deployed using an SDP architecture designed to unify security between cloud or non-cloud resources and internal or external users. To ensure security, rigorous authentication and authorization is built into the architecture before a connection is established – and each connection is one-to-one and on-demand. This provides a needsbased access model with invisible or "dark" service or network segments, thereby dramatically reducing the attack surface for hackers.

- **Unified and scalable platform**
  Secure Access solutions from Ivanti are powered by the 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.

- **Centralized policy engine for user, devices and applications**
  Administrators can configure contextual access policies with Ivanti 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**
  Ivanti boosts the security intelligence of next generation firewalls, access points, switches and SIEMS by providing enhanced identity and device context for granular enforcement and automated mitigation. The Ivanti 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 Ivanti solution extends existing security policies for a single security standard that uniformly protects both the data center and cloud. Advanced SDP capabilities can quickly add Zero-Trust “authenticate first, connect second” connectivity and bolster the corporate network against modern security threats and lateral spread. Additionally, our solution is also helping existing customers secure and harness IoT devices, further demonstrating that their trusted Ivanti solution can protect enterprise information no matter where it is stored or how it is accessed.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com