Cisco® Identity Services Engine (ISE) 3.0

Cisco® Identity Services Engine (ISE) 3.0, a cloud-enabled approach to increase visibility into policy controls and zero-trust decision points within the workplace.

Providing secure access to trusted users and endpoints is getting harder and harder to achieve. The problem of identifying and controlling endpoints as they request access to trusted resources has been exacerbated by trends around cloud migration, mobility, and the proliferation of Internet of Things (IoT)–connected devices. But as the cloud, mobility, and IoT all possess great possibilities to unlock innovation as well as save organizational resources, these new paradigms have introduced more questions and complexity when it comes to securing data and maintaining compliance across the expanding perimeter.

Zero trust with least privilege access is a vital cybersecurity principle that addresses these challenges. It recommends granting only the minimum level of system/network access based on the least level of privilege required to allow users and endpoints to carry out their missions as required by business objectives. Unrequired access extends the network attack surface, increases the risk for the organization, and allows the lateral movement of threats. By controlling access to only what is needed to reach business outcomes, the organizational risk is reduced, and compliance is assured.

The complexity of today's networks makes the implementation of the least privilege approach to providing network access a daunting challenge. Without having the visibility to properly identify network endpoints, controlling access with segmented zones of trust is not only not recommended, but it could also cause disastrous effects in the workplace, shutting down business-critical functions, especially in IoT environments.

Solving more for customers in 3.0:

- Where and how customers consume their security has evolved, and to lead in this transition, we are kicking off our cloud-enabled approach with ISE VMs deployable from the cloud (AWS).
- Customers want fast, lightweight security, so we delivered agentless posture in ISE 3.0 to solve the internal debate between speed of delivery and protection.
- And since everyone wants "easy," we made posture simpler to deploy, revamped the UI with a focus on simplicity, and unleashed guided workflows for advanced use cases.
- Customers evolve from essential to advanced use cases to gain value and provide secure network access; we have evolved our licensing structure to match.

What's new in 3.0

Solving for visibility and enabling zero trust is why we are delivering a bold, cloud-centric approach to network access and control. ISE 3.0 focuses on three key pillars to enable customers to solve their secure access challenges and build a zero-trust workplace: **Dynamic visibility**, **Cloud-enabled security**, and **Increased simplicity**.

Dynamic visibility

Identifying and classifying network devices and resources is a critical first step in building a zero-trust strategy around network segmentation and creating zones of trust for policy decisions and enforcement. Within this recent release of ISE and across our Secure Access portfolio, we have increased our ability to see and identify what is connecting to the network to build visibility-based network segmentation and policy control into the network itself without the use of agents.

Increased flexibility with Agentless posture

To see everything and to make obtaining complete visibility and control "touchless," we are supporting an Agentless posture to ensure all devices are identified, and remain in compliance, without having to install anything on the device or endpoint. Agentless posture increases flexibility and accelerates time to value with ease of deployment while solving the internal debate between the speed of delivery of network resources and increasing risk. On top of Agentless posture, ISE 3.0 also enables running scripts on each and every endpoint connected to the network to gain better visibility.

Cloud-enabled actionable visibility

By embracing cloud-based solutions, organizations are gaining actionable visibility and increased context to inform the policy decision points in a zero-trust framework. ISE extends its open standards-based ecosystem, pxGrid, into the cloud, with pxCloud.* Customers are now able to take the knowledge from cloud-based security intelligence and analytics solutions to gain an actionable arm of defense at the network enforcement points throughout the network. This level of integration increases an organization's overall security posture with automated threat containment to prevent the lateral movement of malware, stopping sophisticated attacks such as ransomware, while future protecting existing security investments and increasing their ROI.

AI-augmented visibility through integration with AI endpoint analytics

Dynamic visibility extends beyond a static list, simple identifiers, or single levels of authentication such as ID/password or MAC address. Single identifiers, when coupled together, can start to build the identity of a user or endpoint. ISE uses Cisco AI Endpoint Analytics to track multiple data sources while leveraging machine learning to automatically analyze and classify unknown devices based on their behavior, adding a new level of assurance to the identity of the endpoint. Device profiles are continuously and dynamically updated via a baseline of behavior, posture, and threat analytics from our pxGrid ecosystem to ensure levels of trust are maintained to limit organizational risk and maintain compliance.

Visibility for now and the future

We have increased the capabilities within ISE to improve device identification and classification with increased support for MDM (mobile device management) and MUD (manufacture usage description) as well as overcoming challenges with shared MAC addresses with Unique Device ID. ISE extended integrations into solutions such as Cisco Cyber Vision, and Cisco DNA Center™ increases and automates visibility and control into IoT devices to ensure visibility-based segmentation can be implemented without disrupting business objectives.

Cloud-enabled security

Customers can now take ISE to the cloud. With cloud-supported deployments, integration with cloud-native solutions, and identity directories, ISE is giving organizations the flexibility they require to enable cloud-first strategies while providing secure access and supporting zero trust.

Enabling a cloud-centric approach

Organizations are looking to the cloud first as they build their infrastructure as well as deploy services and solutions. ISE is enabling this strategic approach with pxCloud*, our open and standards-based integration platform. pxCloud* now enables integration with cloud-native software-as-a-service (SaaS) security solutions. Organizations will now be able to enhance their security visibility and intelligence to gain more context as they look to automate threat containment and improve policy decisions and enforcement without having to deploy anything on-premises.

ISE in and with the cloud

ISE is now deployable from the cloud to enable customers' cloud-first approach and to increase customer flexibility in the deployment of ISE to provide secure access. We have also integrated with Azure AD to better support our customers migrating into the cloud through single sign-on to expand our cloud-centric strategy. Furthermore, with ISE 3.0, customers can deploy an ISE node in an ESX infrastructure running on AWS.

Cloud-enabled actionable visibility

With increased visibility and context from the cloud, organizations are now better informed to confidently create access policies to reduce organization risk, without risking business objectives and preventing the connection. With cloud-enabled visibility, customers gain an active arm of protection from passive security solutions to automate threat containment. Customers can now bring together silos of visibility and intelligence to extend interoperability and take a platform approach in solving their secure access challenges.

Open integrations to extended ecosystem

pxCloud extends the ISE ecosystem and furthers our open and interoperable stance within solving customers' challenges. The ISE ecosystem of trusted and validated partners confirms Cisco's commitment to overcoming complexity in the network with solutions that are interoperable and support a platform approach to gain simplicity, automation, and accelerate value.

Increased simplicity

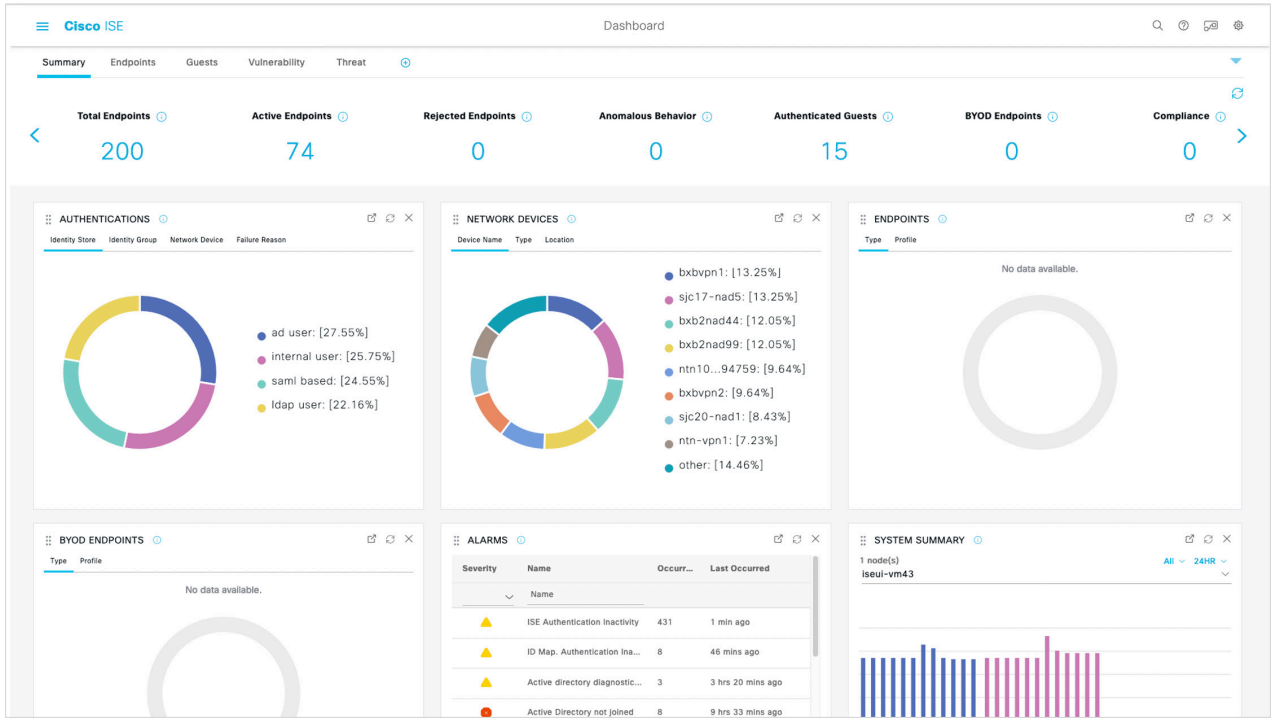
In everything we do, we need to be customer-centric. And overcoming complexity to ensure that our customers can accelerate their value is a core principle guiding our innovations and design. ISE 3.0 has answered this challenge by hardening and improving its core functions, and with a focus on interoperability and platform integrations, customers will be able to accelerate their value as well as the value of existing solutions without an increase in investment.

Simplified user experience

The first thing you will see is the new and enhanced UI, with guided workflows to enable customers to quickly configure ISE for advanced secure access use cases. Simplified workflows allow organizational flexibility to adapt to changing organizational needs, and the threat landscape. No longer will IT be caught reacting to every market shift and instead will be able to take back control of the network. An immediate benefit of guided workflows is removing the complexity barrier to achieving network segmentation, a key component of the zero-trust framework.

Easy ISE: Ease the onboard experience for customers and guests

Granting access to guests has been made simple. Guest Auto-Login gives guests the flexibility to log in, without credentials, after sponsor approval, and we have made multiple enhancements to improve on the guest user experience.



Benefits of 3.0

- **Cloud-enabled visibility:** Extend interoperability into the cloud. Enhance visibility for access decisions. Embrace the flexibility required to be cloud-driven.*
- **A simplified user experience:** A user experience with a focus on simplicity unlocks advanced use cases to rapidly accelerate value and protection.
- **Added flexibility:** Agentless posture and support for Endpoint Scripts allows the visibility required to ensure compliance. You no longer need to choose between the speed of delivery of services and protection.
- **Increased visibility through integration with AI Endpoint Analytics:** With AI-augmented visibility, customers can leverage machine learning to properly identify, classify, and verify device identification for effective policy management and network control.
- **Secure Access from the cloud:** Enable a cloud-driven approach to unifying visibility and control across campus and branch deployments with ISE from the cloud.

Resources:

- ISE Solution Overview
- Dynamic Visibility AAG
- Visibility-Driven Segmentation AAG
- Automated Threat Containment AAG

Supporting documentation

- Release Notes
- Data Sheet
- Licensing FAQ
- End-User Documentation Hub

*Feature planned for release in the first half of 2021. Please contact sales for early access.

Learn more about Cisco Identity Services Engine, please visit

www.cisco.com/go/ise