



# Cisco ISE

ISE

孙浩

思科安全渠道工程师

17664072014



# Agenda



- ▶ Production introduction
- ▶ Market Recognition
- ▶ POV resource



# Production introduction

# 什么是Cisco ISE

## 企业网络

## 安全



## 思科身份服务引擎 (ISE) 是思科工作场所零信任解决方案核心:

- 思科 ISE 允许企业用户为每个用户和设备提供安全网络访问，并具有企业网络安全所需的可见性和控制力。
- ISE 通过识别、分类和组合有关用户和端点的必要上下文数据来提供完整的可见性。它根据业务意图（您的安全策略）对他们进行身份验证和授权，并根据他们的角色或功能的需要授予适当级别的网络访问权限。ISE 提供网络分段以符合最小权限安全概念。
- ISE 可以简单轻松地允许端点之间的授权网络通信，同时根据用户和网络设备（包括 Active Directory 和移动或企业设备管理应用程序）的现有身份服务、进行策略管理。
- ISE 与其他思科安全产品和我们的思科安全技术联盟 (CSTA) 合作伙伴双向共享上下文用户和设备信息。ISE 可以帮助他们评估和关联漏洞和威胁，以实现自动快速威胁遏制。

# ISE 功能特性



设备管理



允许使用TACACS+或Radius, 在用户用过ssh/telnet访问网络设备时进行身份认证与命令审计

身份认证与安全接入



根据用户和/或端点的身份允许有线、无线或 VPN 访问网络资源。将 RADIUS 与 802.1X、MAB、Easy Connect 或被动 ID 结合使用

访客接入



区分公司和访客用户和设备。从热点、自助注册访客和赞助访客访问选项中进行选择

资产可见性



使用 ISE 和思科网络设备中的探测器对端点进行分类, 并通过设备分析(profiling)对其进行适当授权。实现自动不同的物联网设备类型, 并根据类型下发不同的授权(VLAN ACL 等)

终端合规安全



使用无代理状态、思科安全客户端、MDM 或 EMM 检查端点以进行验证  
在允许网络访问之前遵守策略(补丁、AV、AM、USB 等)

终端上下文信息共享



pxGrid是一个生态系统, 允许任何应用程序或供应商与 ISE 集成以获取端点身份和上下文, 以提高网络可见性并促进自动化执行。

网络分段



Group-based Policy基于组的策略允许通过使用安全组标记 (SGT) 和安全组 ACL (SGACL) 而不是 VLAN/ACL 分段来对网络进行分段。

Cisco SDA/DNAC



ISE 与 DNA Center 集成, 实现网络结构自动化, 并使用软件定义的访问 (SDA) 在整个网络基础设施中实施策略

BYOD



允许员工通过简单的入职流程注册设备并下载证书进行身份验证, 从而使用自己的设备访问网络资源

威胁遏制

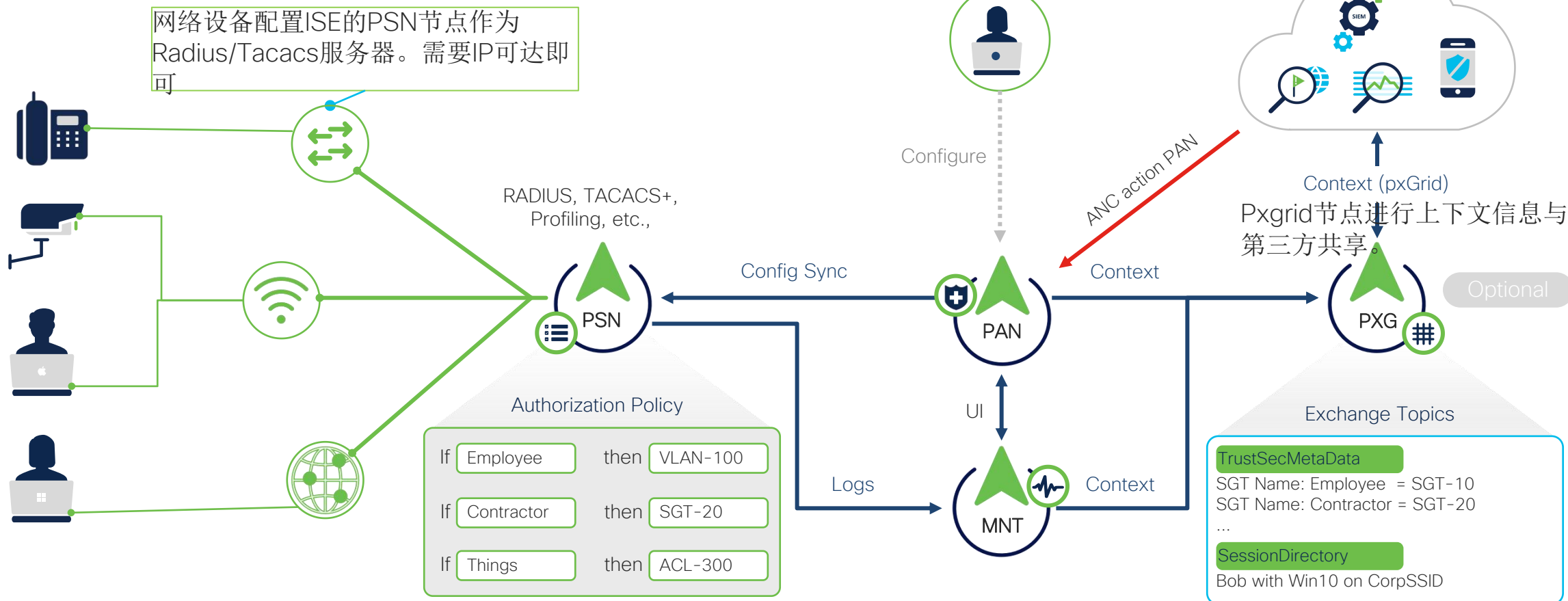


使用威胁分析工具(例如Cisco Cognitive Threat Analytics)对端点威胁评分进行评分并根据结果允许网络访问

# ISE 各节点工作方式及原理

管理员通过HTTPS访问PAN进行管理。

Partner Eco System  
SIEM, MDM, NBA, IPS, IPAM, etc.

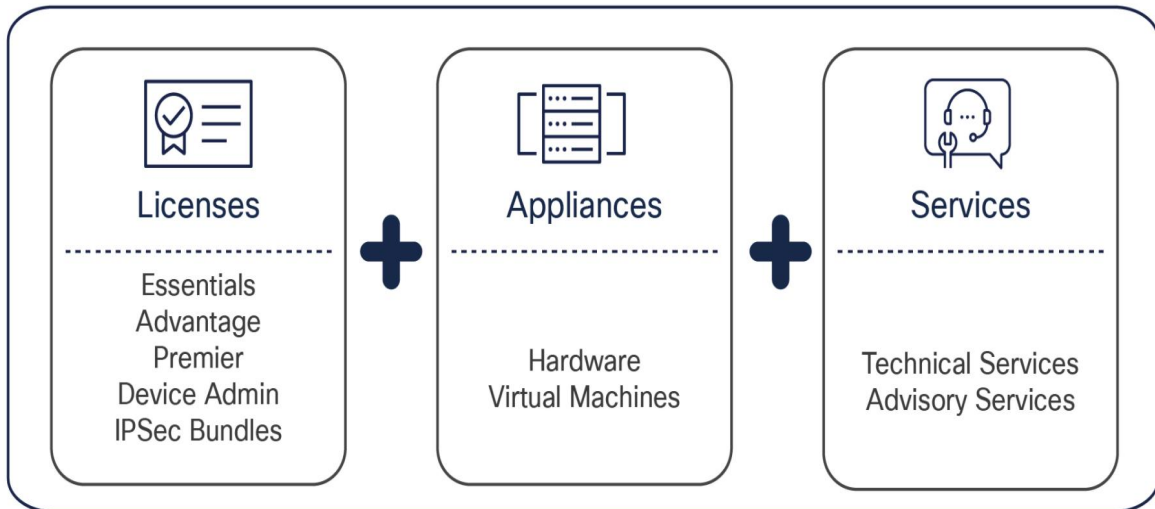


PSN根据用户的身份信息，结合多重身份信息条（condition）进行授权。

MNT通过Syslog搜集其他节点的日志信息，PAN通过UI进行查看

\*PSNs can optionally be behind a load-balancer and can be accessed via Load Balancer Virtual IP address (VIPs)

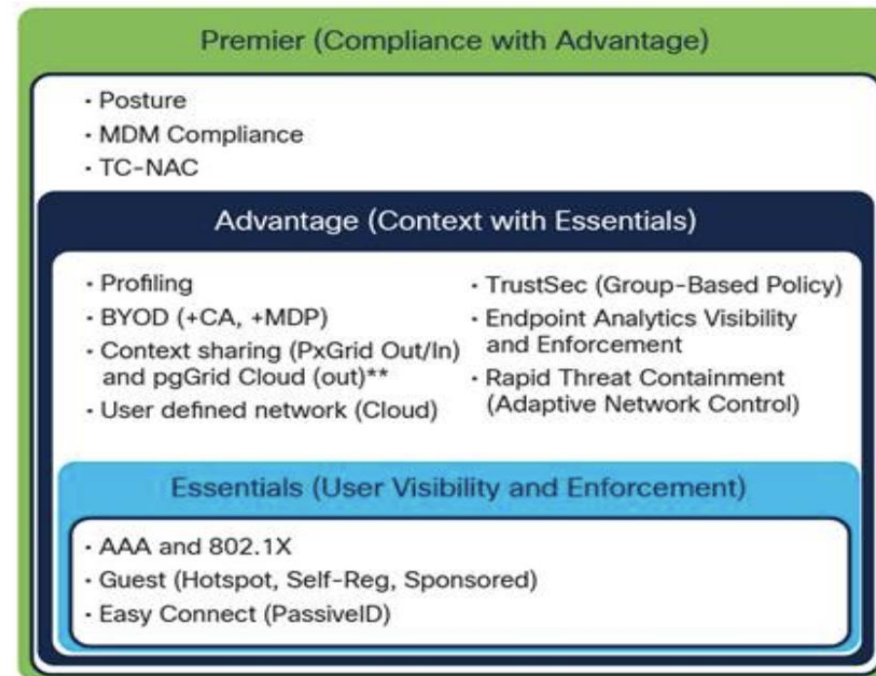
# ISE购买方式



- ISE的license计算方式为功能+并发终端数量。例如客户A有1000个终端需要Posture功能（如右图所示对应Premier license）则需要1000个premier license
- ISE license采用嵌套娃娃模型，这意味着较高层许可证包含所有较低层功能。
- 思科 ISE 可以部署在物理和虚拟设备的任意组合上，以及 AWS、Azure 和 Oracle 云中的 IaaS 实例上

<p>Enable guest network access at ease</p> <p>Guest and secure WiFi</p>	<p>Intent based network access across wired, wireless and VPN</p> <p>Secure Access</p>	<p>See what's on your network and where they are located</p> <p>Asset visibility</p>	<p>Enforcing access based on asset visibility</p> <p>Asset enforcement</p>
<p>Deeper visibility and control on desktop and mobile device apps</p> <p>Compliance</p>	<p>ISE Use-Cases</p>		<p>Onboarding and management of wired and wireless BYOD</p> <p>Byod</p>
<p>Share real-time threat intelligence to automate threat response</p> <p>Threat containment</p>	<p>Software defined segmentation without VLANs or IP based policies</p> <p>Segmentation</p>	<p>Exchange context between technology partners for better fidelity</p> <p>Integrations</p>	<p>Role-based network device administration over TACACS+</p> <p>Device admin</p>

## ISE使用场景

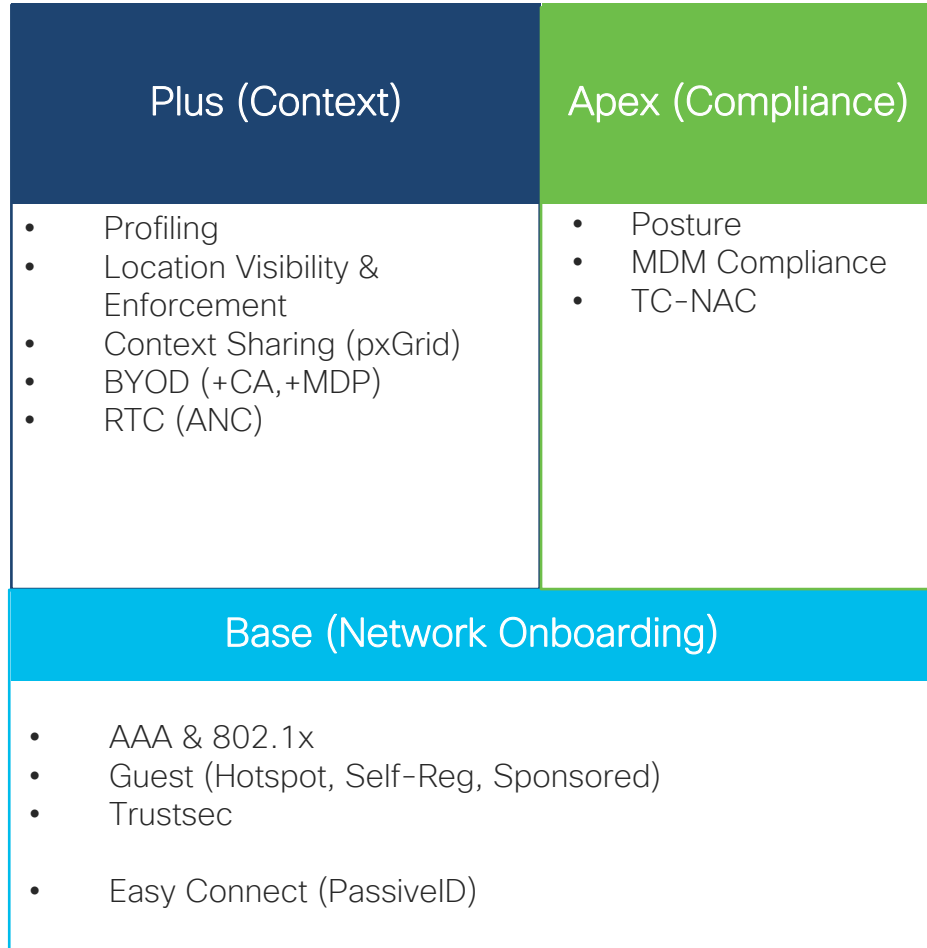


## ISE功能license

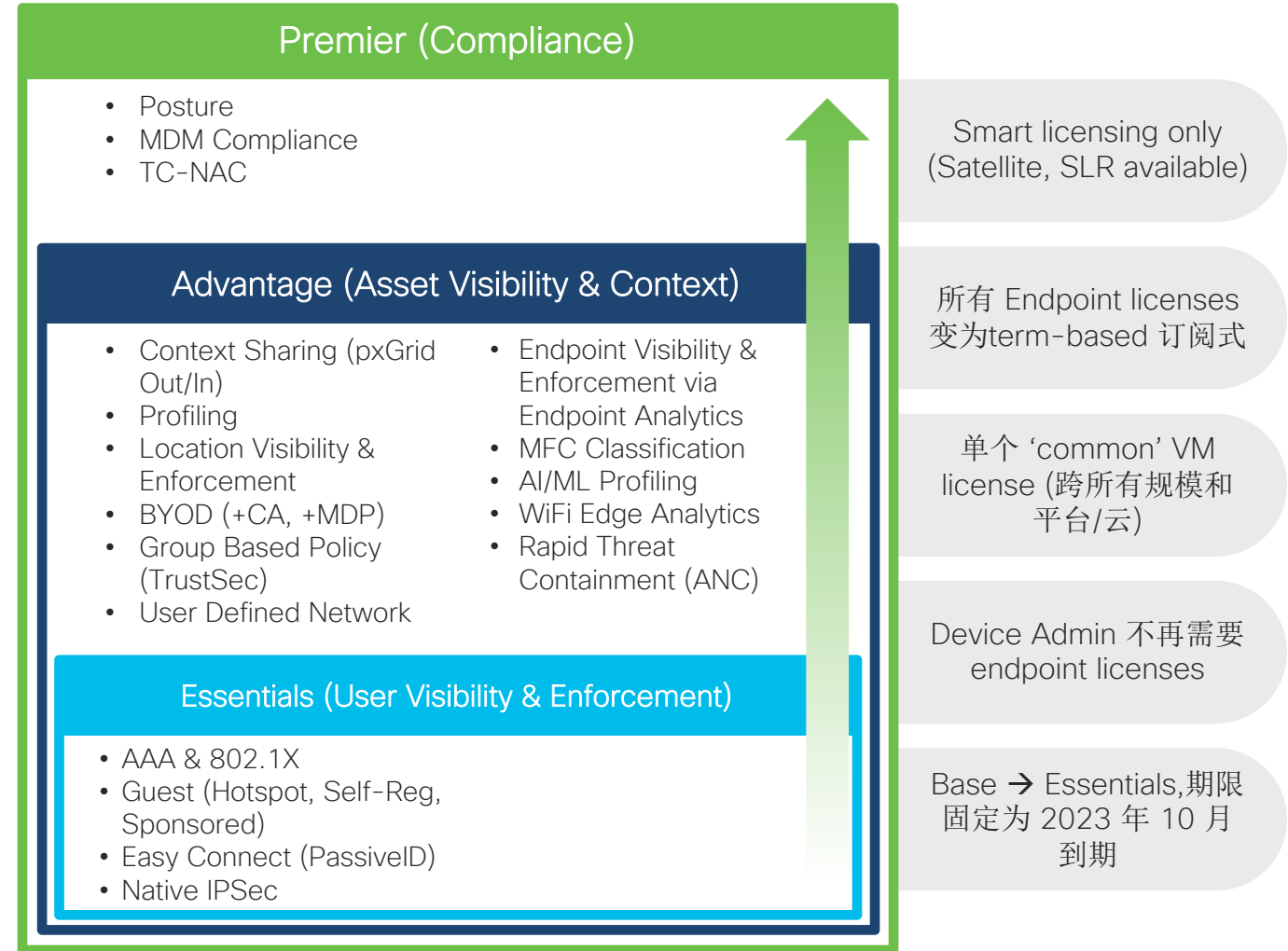


# ISE 3.x Licensing 模型 <https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html> Cisco ISE Licensing Guide

## 2.x (Lego) Model



## 3.x (Nested-Doll) Model







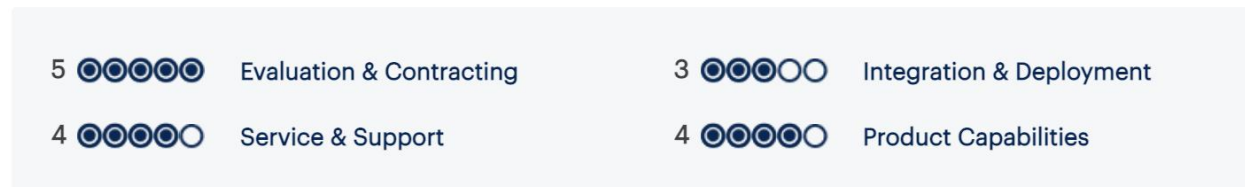
# Market Recognition

# Gartner Network Access Control (NAC) Reviews and Ratings No:1

## 整体评价:

该排名评价思科 *ISE* 是市场上最好的网络访问控制解决方案。它有助于了解哪些端点正在运行到我们的网络中并限制访客系统，可以有效地控制未经授权终端接入的与系统访问。

该排名从以下四个维度对 *NAC* (*Network Access Control*) 解决方案进行衡量，思科 *ISE* 在多个维度取得 4~5 分（满分为 5 分）



## 参考链接:

<https://www.gartner.com/reviews/market/network-access-control/vendor/cisco/product/cisco-ise/review/view/4424440>

### Network Access Control (NAC) Reviews and Ratings

Email Page PDF

Overview Products Gartner Research

#### What is Network Access Control (NAC)?

Gartner defines network access control (NAC) as technologies that enable organizations to implement policies for controlling access to corporate infrastructure by both user-oriented devices and Internet of Things (IoT) devices. Policies may be based on ... See More

How these categories and markets are defined

#### Products In Network Access Control (NAC) Category

Filter By: Company Size Industry Region

<50M USD 50M-1B USD 1B-10B USD 10B+ USD Gov't/PS/Ed

Products 1 - 20 | View by Vendor Review weighting Reviewed in Last 12 Months Number of Ratings, High to Low

4.4 ★★★★★ 432 Ratings

5 Star 40%  
4 Star 52%  
3 Star 7%  
2 Star 0%  
1 Star 0%

**Cisco ISE**  
by Cisco

"CISCO IDENTITY SERVICES ENGINE:THE BEST NAC SOLUTION"

Cisco ISE is the best network access control solution in the market. It helps to gain the visibility about what ...

Read Reviews

Competitors and Alternatives  
Cisco vs HPE (Aruba)  
Cisco vs Fortinet  
Cisco vs ForeScout  
See All Alternatives

4.4 ★★★★★ 261 Ratings

5 Star 48%  
4 Star 44%  
3 Star 6%  
2 Star 2%  
1 Star 0%

**The ForeScout Platform**  
by ForeScout

"ForeScout NAC: The Ups and Downs"

ForeScout NAC is one of the best NAC solutions there in comparison with other brands like FortiNAC or Cisco ISE.

Read Reviews

Competitors and Alternatives  
ForeScout vs Cisco  
ForeScout vs HPE (Aruba)  
ForeScout vs Fortinet  
See All Alternatives

4.4 ★★★★★ 194 Ratings

5 Star 46%  
4 Star 45%  
3 Star 8%  
2 Star 1%  
1 Star 1%

**Aruba ClearPass Policy Manager**  
by HPE (Aruba)

"Securely connecting the business with personal devices."

The experience is excellent. Due to the need to perform remote work, the company needed a solution to ...

Read Reviews

Competitors and Alternatives  
HPE (Aruba) vs Cisco  
HPE (Aruba) vs Fortinet  
HPE (Aruba) vs ForeScout  
See All Alternatives

# Forrester: The Total Economic Impact of ISE

## 整体评价:

投资ISE后，受访者均表示更快、更高效地提供了更细粒度的访问。这减少了安全事件，从而减少了业务用户的停机时间以及识别、隔离和补救违规行为的相关成本和工作量。ISE 还可以提高业务成果，例如通过保持业务用户的工作效率来增加收入、减少可能影响客户或损害品牌声誉的与安全相关的中断，以及通过访客访问和扩大自带设备 (BYOD) 策略来加强协作。

## 参考链接:

[https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/total-economic-](https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/total-economic-impact-ise.pdf)

[impact-ise.pdf](https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/total-economic-impact-ise.pdf)



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EXECUTIVE SUMMARY

Reduction in access-related security events

**50%**

security events by 50%. Fewer events reduce user downtime during remediation. Fewer events also mean that the composite organization does not need to add people to the security team to achieve the desired level of protection and responsiveness. Together, these benefits are worth \$442,000 over three years. This benefit does not include other potential costs of a breach such as lost revenue, fines, and brand reputation damage because it varies greatly depending on the size and nature of a breach and on company specifics such as industry and size.

**KEY FINDINGS**

**Quantified benefits.** Risk-adjusted present value (PV) quantified benefits, as applied to the composite organization, include:

- **Reduction in applicable security breaches by 50% and avoidance of 25% increase in staffing for the associated security team.** This study focuses on security events ISE helps protect against such as rogue devices, devices not fully updated with access, and people inadvertently accessing network resources they should not. It excludes other threats such as phishing attacks that ISE is not designed to address, even though ISE integration with a solution such as Cisco Secure Analytics enables an automated response to these other threats. ISE is implemented at the beginning of the study's three-year period and reduces applicable
- **Avoidance of 66% increase in staffing for the IT network operations team.** ISE provides tools to streamline and automate many processes associated with access and management. They also provide better reporting and analytics, which saves time and helps IT make proactive changes to avoid future problems. Additionally, there is reduced effort supporting users who are having difficulties accessing networks. The existing network operations team avoids adding two additional resources to support growth and achieve the level of service it does with ISE. The three-year value is \$348,000.

**“Combining ISE with SDA is going to make our security model much stronger. It will also greatly simplify life for the security team.”**

— Network engineering services assistant director, higher education organization

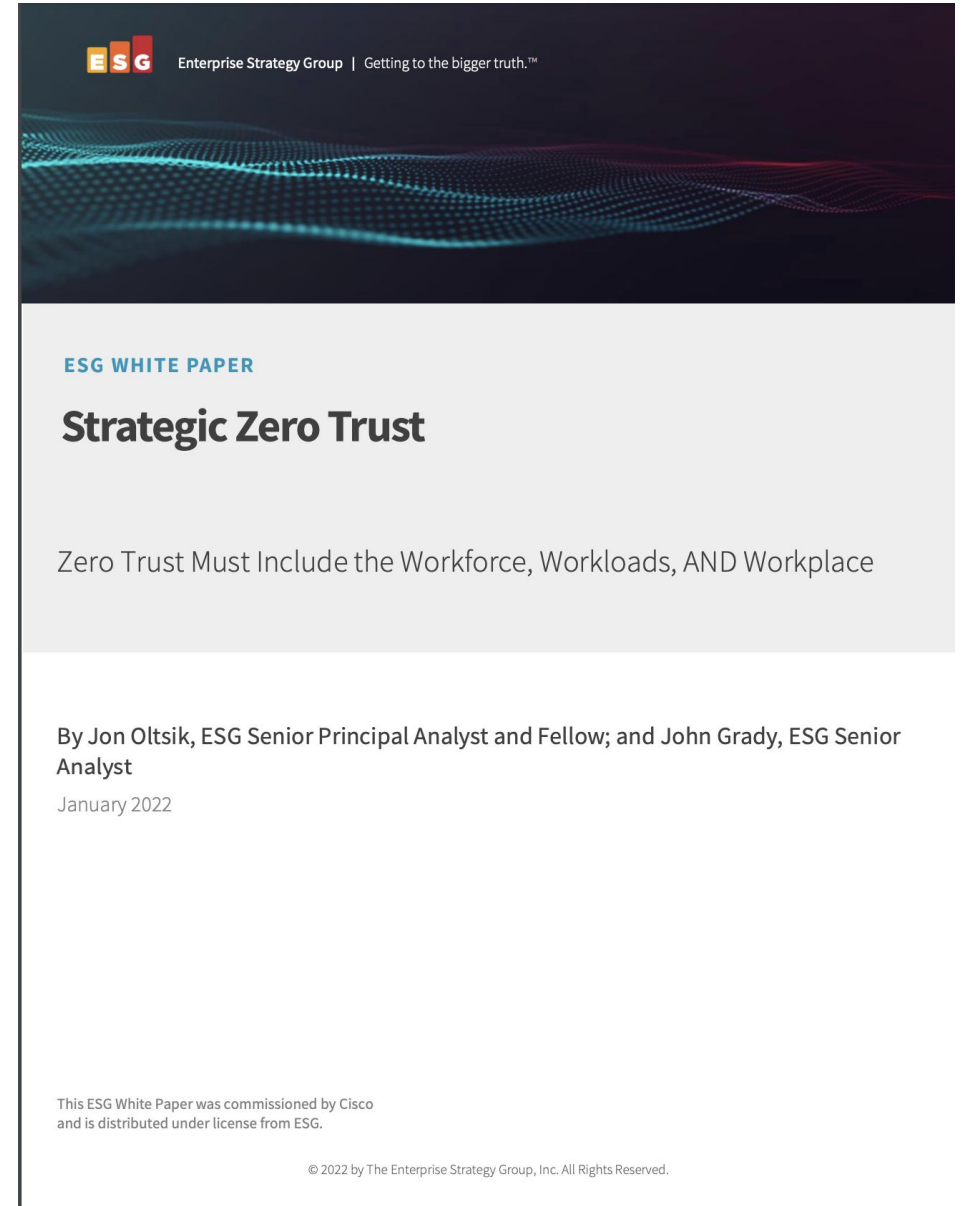
# Enterprise Strategy Group Zero Trust White Paper

## Cisco for the Zero Trust Workplace

该白皮书介绍到许多组织都拥有大量思科网络和安全技术，工作场所零信任的支柱是思科身份服务引擎 (ISE)。ISE 可以创建动态且自动化的方法来进行设备发现、分析、策略创建和实施（通过思科基于组的策略[以前称为 TrustSec]）。这导致了基于工作场所的 IT 和运营技术的软件定义访问和微分段。

### 参考链接：

<https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/esg-zt-workplace-wp.pdf?ccid=cc001033&dtid=odicdc000016&oid=wprsc027709>





# POV & Demo resource

# ISE Cisco DemoZone

Cisco ISE  
Zero trust workplace  
Secure network access across  
Wireless  
Wired  
VPN Connections



## Cisco Identity Services Engine Demo

Learn how you can centrally manage events and policies and analyze threats with Cisco Identity Services Engine (ISE).

[Access Demos](#)

[Related Demos](#)

[Contact Cisco](#) ▾

### Ready to take demos to the next level?

A Cisco.com login is required to access demos. If you don't have one, we provide directions on the login screen for creating one. If you need help with any of these demos, contact [dCloud support](#).



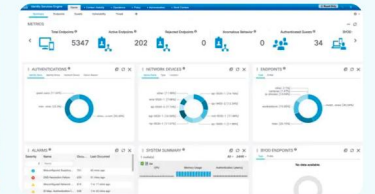
#### Cisco ISE walk-through

Let our technical experts walk you through Cisco ISE and all it has to offer.



#### Cisco ISE podcast

Steve Caimi and Paul Burdette discuss Cisco ISE and how it can help keep your organization safe.



#### Cisco ISE live instant demo

Get hands-on experience in centrally managing events and policies and analysing threats with Cisco ISE.

<https://www.cisco.com/site/us/en/products/security/identity-services-engine/demos.html>

### 3 easy steps to launch the demo

#### Download the demo guide

Follow the instructions in the guide. If you face issues, clear the cache, log off, and log in again.

[Download the guide](#) >

#### Access the demo interface

Access the ISE demo UI to connect to the dCloud and instant demo servers. Then log in as:  
username: admin  
password: C1sco12345

[Access interface now](#) >

#### Log in and start exploring

When connected to the instant demo server, follow the PDF guide or explore the experience yourself.

[Contact dCloud Support for help](#) >



# Dcloud ISE Instant Demo

## Cisco Identity Services Engine (ISE) 3.1 - Instant Demo

ID: cisco-identity-services-engine-ise-3-1-instant-demo Published Date: 09-Jun-2022 23:14 Instant Demo Enterprise Networks

Enterprise Network Security English

**Attention Cisco Team!** Request the Global Virtual Engineering team to deliver this demo to your customer [here](#).

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, Cisco Wireless Controllers, Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE 3.1 acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

NOTE: Please download the story guide from the Related Content link below and click View to access the demo.

★ Favorite [Copy](#) [Related Documents](#)

View

## Scenarios

- [Network Visibility](#)
- [Search for a User or Endpoint](#)
- [What are the Unknown Endpoints on my Network?](#)
- [View Live Authentications](#)
- [Network Device Management](#)
- [ISE Policy Sets](#)
- [Scalable Group Tags \(SGTs\) and Software Defined Access \(SDA\)](#)
- [Logical Profiling Dashlets](#)
- [Tunnel Extensible Authentication Protocol \(TEAP\)](#)
- [Prevent AD Lockout](#)
- [802.1X Authentication Against Azure](#)
- [Guest Access](#)
- [Posture AV/AM Min Version](#)
- [Agentless Posture](#)
- [Endpoint Remediation Scripts](#)
- [BYOD](#)
- [Mobile Device Management \(MDM\)](#)
- [TC-NAC](#)
- [VPN](#)
- [Health Checks](#)
- [Enhanced Audit Logging](#)

## 关于ISE Instant Demo:

该demo提供ISE功能展示使用，可为用户展示包括资产可见性、终端准入、访客接入、终端管合规性、TrustSec等场景。

SE或Partner SE可通过CCO登陆Dcloud访问，并根据其Demo Guide 向用户展示相关功能。

## Dcloud instant Demo适用场合:

适合初次接触客户。向客户介绍ISE的功能及使用场景。



# 客户PoC测试

## PoC Lab 适用场合:

PoC 实验室适合对 ISE 有初步了解并希望在自己的真实环境中测试使用场景的客户。该测试的目的是验证ISE与客户当前使用的第三方网络设备之间的兼容性。您可以在 BOX 上的许多用户 POV 中找到我们之前的经验

<https://cisco.app.box.com/folder/43635154508?v=gcsec-resource>

## 资源准备:

ISE可以部署在Vmware、KVM等虚拟化平台上，建议使用虚拟化部署方式进行测试，具体服务器资源需求可参考《ISE安装部署指南》（Cisco Identity Services Engine Installation Guide, Release 3.0）

Table 1. OVA Template Reservations

OVA Template Type	Number of CPUs	CPU Reservation (In GHz)	Memory (In GB)	Memory Reservation (In GB)
Evaluation	4	No reservation.	16	No reservation.
Small	16	16	32	32
Medium	24	24	96	96
Large	24	24	256	256

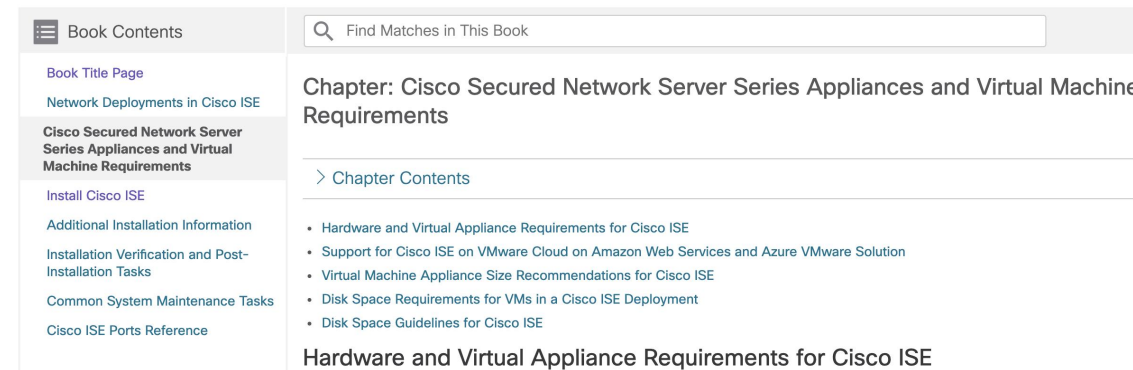
## ISE 虚拟化安装指南:

[https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/install\\_guide/b\\_ise\\_InstallationGuide30/b\\_ise\\_InstallationGuide30\\_chapter\\_2.html](https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/install_guide/b_ise_InstallationGuide30/b_ise_InstallationGuide30_chapter_2.html)



## Security Box POC参考材料

Cisco Identity Services Engine Installation Guide, Release 3.0



# 测试license

Administration · System

Evaluation Mode 89 Days

Deployment **Licensing** Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

UDI Details

ISE虚拟化版本安装后即可获得90天的试用license，无需申请

Product Identifier (PID) ISE-VM-K9  
Version Identifier (VID) V01  
Serial Number (SN) 6IM0FCCEC

License Type

Choose Registration Details to acquire pre-purchased license entitlements. Choose Permanent License Reservation to enable all Cisco ISE licenses. Enter the required details to enable Cisco ISE licenses. When you click Register, you agree to the terms and conditions detailed in [Smart Licensing Resources](#).

Smart Licensing Registration  
 Permanent License Reservation  
 Specific License Reservation

> [Registration Details](#)

Licenses

Select relevant licenses and click Enable to acquire the pre-purchased license's entitlements. Select relevant licenses and click Disable to release unused entitlements. Click Refresh to reauthorize the enabled licenses.

[Enable](#) [Disable](#) [Refresh](#)

100 x

1 x

Premier

Advantage

Essentials

Device Admin Appliance License

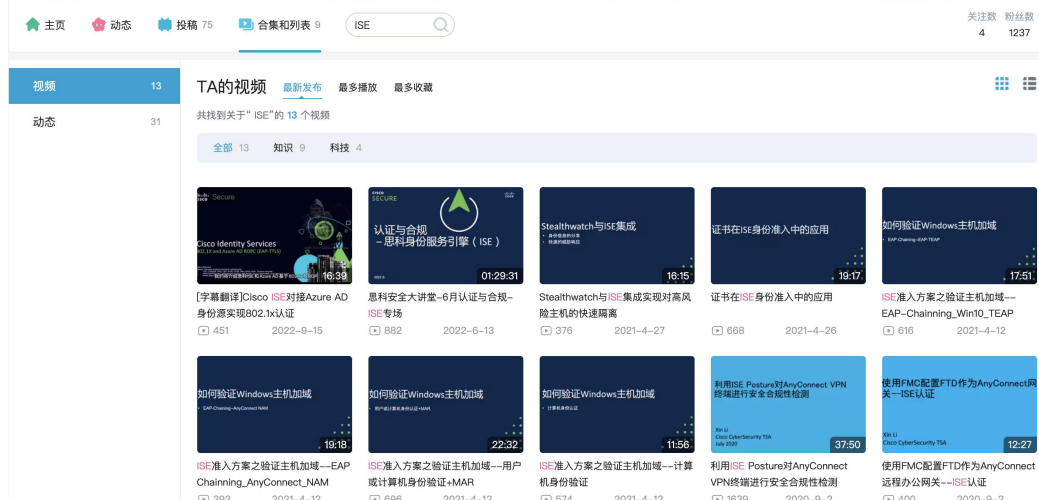
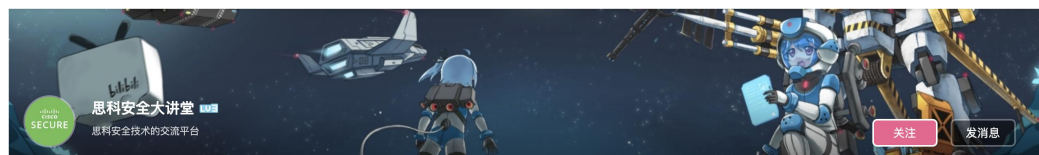
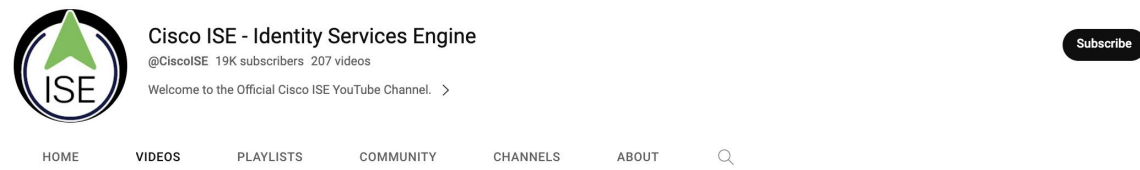
TACACS+

	License	Status	Compliance	Consumption	Days Out of Compliance	Last Authorization
▼ Tier						
<input type="checkbox"/>	Essential	Enabled	Evaluation	<a href="#">0</a>	-	-
<input type="checkbox"/>	Advantage	Enabled	Evaluation	<a href="#">0</a>	-	-
<input type="checkbox"/>	Premier	Enabled	Evaluation	<a href="#">0</a>	-	-
<input type="checkbox"/>	Device Admin	Enabled	Evaluation	1	-	-

# 视频资源

YouTube ISE 频道——站搜索用户“Cisco ISE - Identity Services Engine”；里面有超过200个ISE相关视频，涉及功能发布、功能演示、ISE场景演示等。

哔哩哔哩安全大讲堂——站内搜索“思科安全大讲堂”并在该用户视频列表搜索ISE即可获得。里面包含很多ISE集成案例与集体的配置步骤。





**cisco** Secure