数字化时代基于意图的自动化安全网络架构

Kevin Skahill Cisco全球产品管理高级总监

FIT 2018我们聊了什么？

如何快速发现和控制问题？

加密流量中的恶意软件

安全和隐私

检测精度

以威胁为中心

通过基于情报的攻击防范策略达到基本的安全成熟度，主要包含侦测、调查和修复三个阶段。

What We Discussed at FIT 2018

How do you find and contain problems fast?

Malware in Encrypted Traffic

Security AND Privacy

Detection Accuracy

Threat-Centric

Basic security maturity to prevent attacks via an intelligence-based policy — then detect, investigate, and remediate

企业正在为各种场景开放数据访问权限

任何用户

- ✓ 雇员
- ✓ 承包商
- ✓ 合作伙伴

任意设备

- ✓ 企业下发
- ✓ 自带
- ✓ 物联网

各型应用

- ✓ 数据中心
- ✓ 多云
- ✓ SaaS

不同地点

- ✓ 内部部署
- ✓ 通过VPN
- ✓ 线下

Enterprises are enabling data access between…

Any User

- ✓ Employee
- ✓ Contractor
- ✓ Partner

Any Device

- ✓ Corporate-Issued
- ✓ Bring-Your-Own
- ✓ IoT

Any App

- ✓ Data Center
- ✓ Multi-Cloud
- ✓ SaaS

In Any Location

- ✓ On-Premises
- ✓ On-VPN
- ✓ Off-Network

全新挑战和机遇带来了全新的业务需求

数据访问审查

全面掌握访问数据的用户、设备和工作负载信息，定位高风险点。

灵活的第三方接入管理

企业发生并购、资产剥离等业务变化以及供应链和承包商等方面的原因，迫使企业IT部门构建刚性冗余环境来降低网络安全风险。

恶意网络访问管控

防火墙能够御敌于外，但是无法阻止攻击者通过被盗的账户和密码登录系统。

New Challenges and Opportunity to enable Business

Scoping Data Access

Can you discover all users, devices, and workloads accessing your data to learn where breach risk is highest.

Agile Third-party Access

M&A, divestitures, supply chains and contractors force IT to setup rigid, redundant environments to mitigate risk.

Hostile Network Access

Firewalls stop attackers hacking trust boundaries, but cannot stop attackers logging in via stolen passwords.

关于安全的一个新思路

FIT 2019

Forrester Gartner Google

¿ START ?

趋势推动

ZTX(Zero-Trust eXtended)软件定义边界（SDP）和ARTA (持续自适应风险与信任评估)

BeyondCord

路线图不明

很多安全理念解释起来都很简单，但很多人都觉得无从下手

需要数年时间

仅仅是简单的购买和部署技术是不可能全部发挥出上述安全模型的作用

A new way to think about security

FIT 2019

Forrester Gartner Google

¿ START ?

Trending Approaches

ZTX (Zero-Trust eXtended)
SD-Perimeter and CARTA
(Continuous Adaptive Risk and Trust Assessment)
BeyondCorp

Unclear Guidance

While these security mindsets are simple enough to explain, many find it tricky to decide where and how to begin.

A Multi-Year Journey

There is no single technology to buy and implement that will deliver 100% of any of these security models.

需要转变思维来解决问题

地点 ≠ 信任

不允许基于请求来自网络或DC的数据访问

信任流失

不要只依赖于用户、设备和工作负载信任的一次性验证

限制访问

优先将对于高风险数据的访问限制在最短时间和最小权限

自动化策略

根据情景动态调整访问策略以提高效率并简化流程

Mindsets are changing to address these problems

Location ≠ Trust

Don't grant access to data based on where requests originate in the network or DC.

Trust Erosion

Don't rely only on one-time verification of user, device, and workload trust.

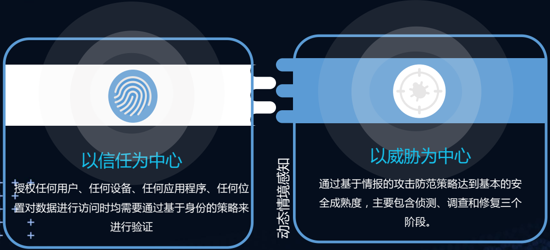
Restrict Access

Prioritize enforcing the least privileges for the least time for your high-risk data.

Automate Policy

Adjust access using dynamic context to improve policy efficacy and simplicity.

互补的安全体系



以信任为中心

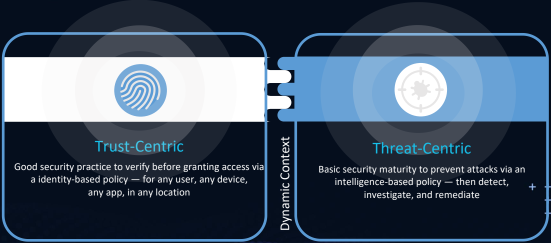
授权任何用户、任何设备、任何应用程序、任何位置对数据进行访问时均需要通过基于身份的策略来进行验证

动态情境感知

以威胁为中心

通过基于情报的攻击防范策略达到基本的安全成熟度，主要包含侦测、调查和修复三个阶段。

Complementary security approaches



Trust-Centric

Good security practice to verify before granting access via a identity-based policy — for any user, any device, any app, in any location

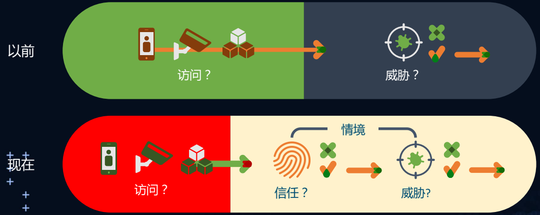
Dynamic Context

Threat-Centric

Basic security maturity to prevent attacks via an intelligence-based policy — then detect, investigate, and remediate

根据访问风险授予相应的信任和威胁级别

FIT 2019


以前

访问？

威胁？

现在

访问？

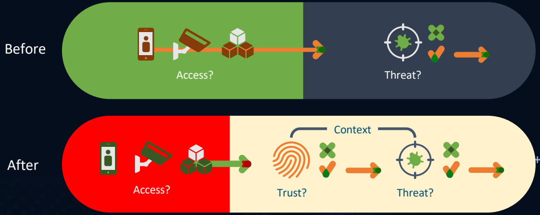
情境

信任？

威胁?

Enforce appropriate trust and threat levels based on the access risk

FIT 2019


Before

Access?

Threat?

After

Access?

Context

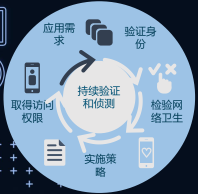
Trust?

Threat?

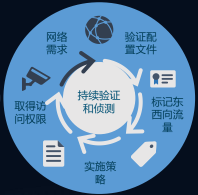
思科可信访问体系可满足三大需求

FIT 2019

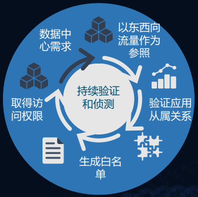
可信用户设备访问


应用需求
验证身份
检验网络卫生
实施策略
取得访问权限
持续验证和侦测

可信IoT访问


网络需求
验证配置文件
标记东西向流量
实施策略
取得访问权限
持续验证和侦测

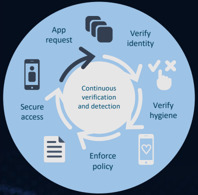
可信工作负载访问


数据中心需求
以东西向流量作为参照
验证应用从属关系
生成白名单
取得访问权限
持续验证和侦测

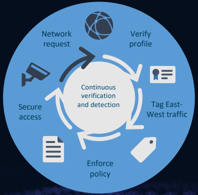
Cisco Trusted Access solves three primary needs

FIT 2019

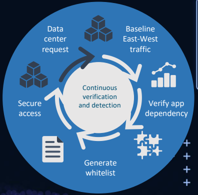
Trusted User-Device Access


App request
Verify identity
Verify hygiene
Enforce policy
Secure access
Continuous verification and detection

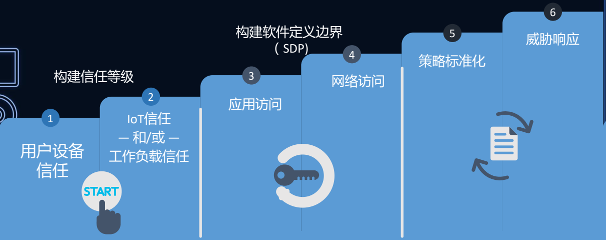
Trusted IoT Access


Network request
Verify profile
Tag East-West traffic
Enforce policy
Secure access
Continuous verification and detection

Trusted Workload Access


Data center request
Baseline East-West traffic
Verify app dependency
Generate whitelist
Secure access
Continuous verification and detection

可信访问体系



构建信任等级

1 用户设备信任

START

2 IoT信任 — 和/或 — 工作负载信任

构建软件定义边界 (SDP)

3 应用访问

4 网络访问

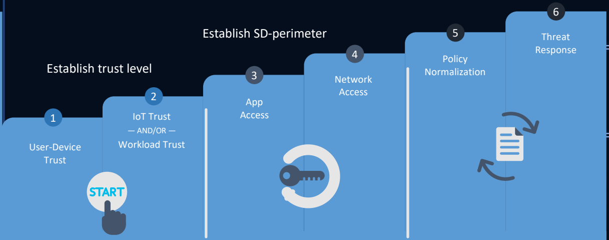
自动化自适应策略

5 策略标准化

6 威胁响应

采取实用的零信任体系确保网络安全

Trusted Access Approach



Establish trust level

1 User-Device Trust

START

2 IoT Trust — AND/OR — Workload Trust

Establish SD-perimeter

3 App Access

4 Network Access

Automate adaptive policy

5 Policy Normalization

6 Threat Response

Using a practical Zero Trust approach to security

可信访问策略进化

FIT 2019

网络访问 应用访问

软件定义访问
(SD-Access)

Duo Security is now part of Cisco.

CISCO

可信访问在部署混合型IT设施企业中的应用

IoT访问解决方案		应用/服务	
		本地 ↔	云
Head-less设备	本地	软件定义访问	软件定义访问

移动和BYOD访问解决方案		应用/服务		
		本地 ↔	云	
用户设备	↕ 本地	软件定义访问	软件定义访问或Duo**	Duo MFA
	本地	软件定义访问[†] 或 Duo**	Duo	

[†]集成到AnyConnect
*Duo Beyond网关 (i.e. 反向代理) **适用于BYOD的Duo Access

Trusted Access Policy Evolution

FIT 2019

Network Access Application Access

Software-Defined Access
(SD-Access)

Duo Security is now part of Cisco.

CISCO

Trusted Access across Hybrid IT Enterprises

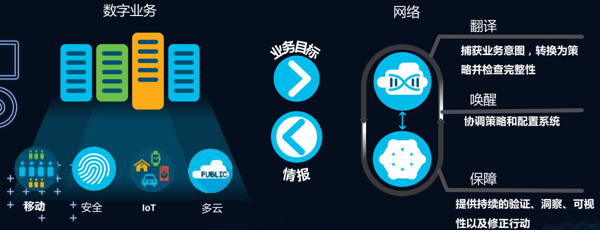
IoT Access Solution		App/Services	
		On-Prem ↔	Cloud
Head-less Device	On-Prem	SD-Access	SD-Access

Mobile and BYOD Access Solution		App/Services		
		On-Prem ↔	Cloud	
User-Device	↕ On-Prem	SD-Access	SD-Access or Duo**	Duo MFA
	Off-Prem	SD-Access[†] or Duo**	Duo	

[†] Integrated with AnyConnect
*Duo Beyond with Network Gateway (i.e. reverse proxy) **Duo Access for BYOD

基于意图的网络可加速可信访问流程

FIT 2019



翻译

捕获业务意图，转换为策略并检查完整性

唤醒

协调策略和配置系统

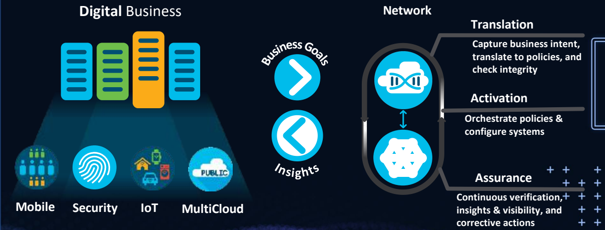
保障

提供持续的验证、洞察、可视性以及修正行动

意图驱动，情境感知

Intent-based Networking Accelerates Trusted Access

FIT 2019



Translation

Capture business intent, translate to policies, and check integrity

Activation

Orchestrate policies & configure systems

Assurance

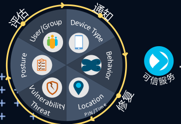
Continuous verification, insights & visibility, and corrective actions

Powered By Intent. Informed by Context.

软件定义访问

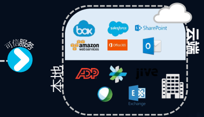
FIT 2019

持续的可视性和情境感知 → 基于意图的策略 → 适用于混合云和多云环境



基于群组的策略

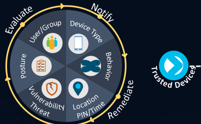
	Trusted Group	Partners	Cloud App A	Cloud App B	Server A	Server B
Trusted Asset	✓	⛔	✓	✓	✓	✓
Trusted Group	⛔	⛔	✓	✓	✓	⛔
Partners	⛔	⛔	✓	✓	⛔	⛔



Software-Defined Access

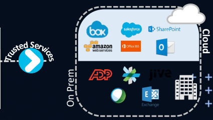
FIT 2019

Continuous Visibility & Context → Intent-based Policy → For Hybrid, Multi-cloud



Group–based Policy

	Trusted Group	Partners	Cloud App A	Cloud App B	Server A	Server B
Trusted Asset	✓	⛔	✓	✓	✓	✓
Trusted Group	⛔	⛔	✓	✓	✓	⛔
Partners	⛔	⛔	✓	✓	⛔	⛔



实用的方案帮助取得良好的结果

实现可降低风险的访问策略

防止任何受影响的用户、设备或工作负载访问应用程序和网络。

良好的用户愉悦度是培养安全文化的基础

思科自动化解决方案可帮助减少终端用户和IT部门之间的摩擦。

快速灵活地满足合规需求

使用软件定义边界方案确保对特定应用或网络中受监管数据的安全访问。

Practical approach to achieving results

Enable reduced-risk access decisions

Apps and network are no longer accessible to any compromised user, device or workload anywhere

Happier users foster a security culture

Shift automation to Cisco and some remediation to end-users to reduce friction for lean IT teams

Fast compliance right where it’s needed

Secure access to regulated data within specific apps or network segments using SD-perimeters

思科的优势在于消除产品短板

- 使用身份验证和动态情境感知
- 适用于内部部署和多云环境
- 简单、一致的访问准入支持，支持从任何位置上发起
- 全面涵盖企业下发和BYO设备
- 更高效的东西流量隔离

The Cisco difference is eliminating product silos

- Uses identity verification and dynamic context
- Works for on-premises and multicloud apps
- Simpler, more consistent access everywhere
- Covers corporate-issued and BYO devices
- More effective East-West segmentation

FREEBUF | FIT

THANKS