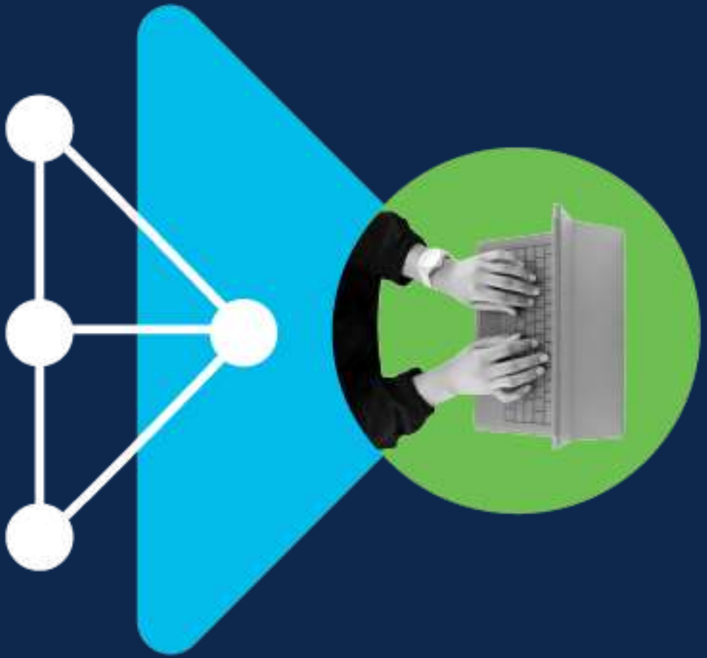
CISCO
SECURE

The bridge to possible

Cisco Secure Endpoint

Bezpečnost od koncových zařízení až po cloud



Milan Habrcetl, Cisco Cybersecurity Specialist
Jiří Tesař, Cisco Technical Security Architect
TechClub webinar, 5.10.2021

Securing your endpoints can be a challenge

57%	Time to detect is the key KPI for security teams
74%	Cybersecurity skills shortage impacted organization
68%	Increase in the frequency of attacks against endpoints

Challenge: Time

“I don’t have enough time to go after every new threat, alert, patch and compromised devices accessing critical apps.”

Challenge: Expertise

“My team can’t be experts on every new threat**,** threat hunting, and all compliance **and** privacy mandates.”

Challenge: Evidence

“We can’t always get to the root cause of every attack, stolen credentials, or find the best security/productivity balance.”

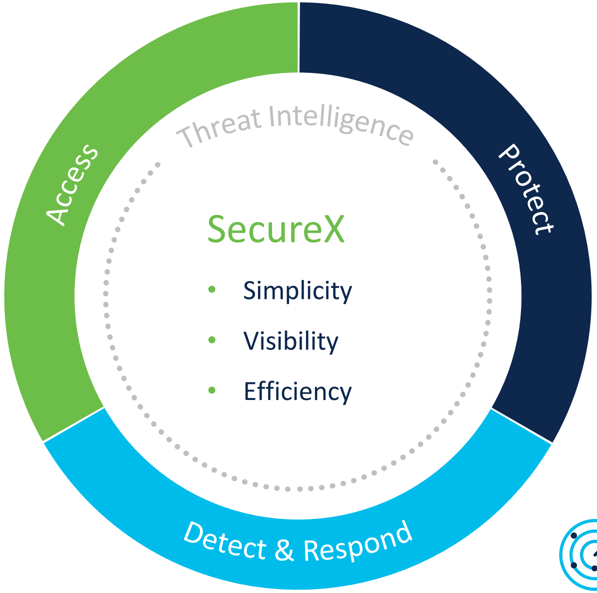
It’s time to reimagine endpoint security

Multi-factor Authentication

Risk-based Access Control

Posture

Virtual Private Network



Access

Protect

Detect & Respond

Threat Intelligence

SecureX

- Simplicity
- Visibility
- Efficiency

Machine Learning

Next Gen Antivirus

Fileless Malware I Ransomware Protection

Internet Protection

Broadest XDR

Advanced EDR

Threat Hunting

Attack Surface Reduction

Stop threats. Before compromise.

Dynamic multifaceted prevention

- Behavioral analytics, machine learning, signatures and more

Attack surface reduction

- Securing remote work with Duo, AnyConnect, Umbrella, AMP for Endpoints and Cloud

Posture and IT Operations assessment

- Endpoint policy compliance and zero-day attack prevention

Remediate faster. Completely.

Extensive EDR and XDR capabilities

- Advanced and cross-control detection and response
- Endpoint isolation and other attack surface reduction capabilities

Accelerated threat response

- Automated playbooks, hundreds of preloaded queries
- Human-driven hunts for threats with in-depth mapping to MITRE ATT&CK framework

Dynamic Malware Analysis

- Identify attacks in real time to drive faster threat detection and response

Maximize operations. Efficiently.

Never losing context: SecureX ribbon

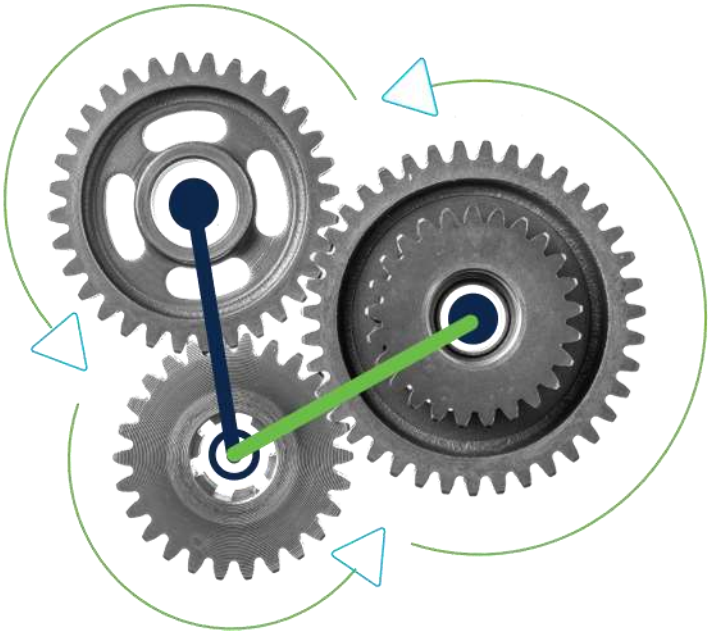
- Pivot and investigate faster with relevant information that you take with you

Simplified incident management

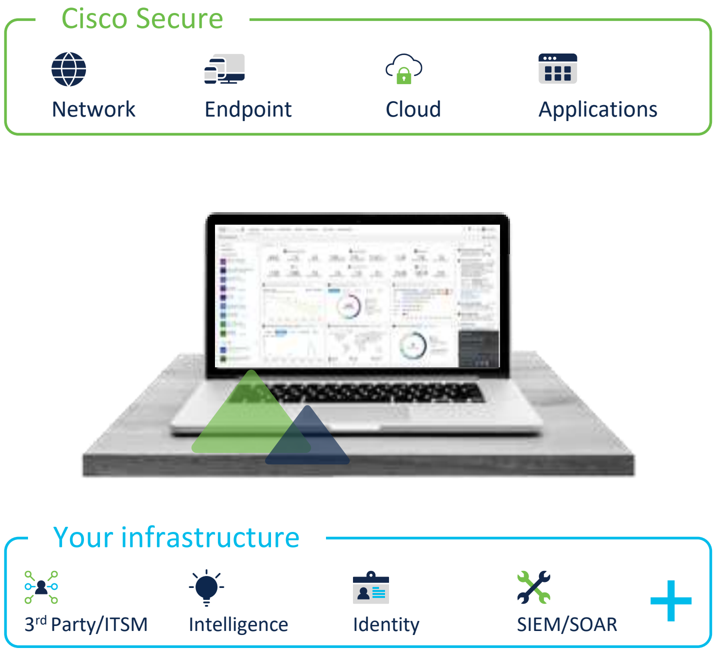
- Pre-built or build your own investigation workflows
- Built-in approval actions, malware analysis, live queries, threat response and third-party integrations

Do more with less

- Automated and collaborative tools that supercharge security analyst productivity
- Address the ongoing talent shortage and burnout



Integrated XDR with Cisco SecureX



Cisco Secure

Network

Endpoint

Cloud

Applications

Your infrastructure

3rd Party/ITSM

Intelligence

Identity

SIEM/SOAR

+

We’ve done the hard work to simplify your experience, accelerate your success and secure your future

- Get fuller visibility to threats beyond the endpoints
- Simplify investigations with built-in threat response
- Run automated playbooks, automate actions and access operational metrics directly from SecureX
- Enable better, faster decisions and pivots with relevant context and analytics from SecureX

Save time with the threat response feature of Cisco SecureX

Without Threat Response

1. IOC / Alert

2. Investigate incidents in multiple consoles

3. Action/Remediate

32 minutes

With Threat Response

1. IOC / Alert / Browser Plugin

2. Investigate and remediate incidents from multiple security tools in a single console

5 minutes

Integral part of the Cisco Secure Remote Worker solution

Cisco Identity Services Engine

Verify the identity of all users before granting access to company-approved applications

Cisco AnyConnect

Enable secure access to your network for any user, from any device, at any time, in any location

Cisco Umbrella

Hold the first line of defense against threats on the internet wherever users go

Secure Endpoint

Maintain the last line of defense through Secure Endpoint

Fueled by superior threat intelligence from Talos

Visibility across all vectors from a best in class portfolio

TALOS

Automated Analysis

Specialized Tools

Telemetry

- Domain
- File
- IP
- URL
- Network
- Flow

Why customers love Cisco Secure Endpoint?

Reduces workload, time and resources

- Robust prevention, detection & response
- Scalable and integrated architecture
- Powered by global threat intelligence

Istanbul Grand Airport

"Using AMP [Secure Endpoint] Everywhere, we gain visibility, unified information sharing, and a faster **time** to detect and respond to threats."

Read More Here

CISCO SECURE

"Cisco AMP will stop infection/exploit from spreading to other devices."

IT Professional, Medium Enterprise Consumer Company

"It doesn't impact the devices. It's just a rock-solid solution."

Dan Turner, CIO at Per Mar Security Service

"Integrating AMP with SecureX gives a lot of visibility to your endpoints."

IT Manager, $500M+ Manufacturing

"Within the first 4 months of integrating AMP it successfully blocked ransomware 6 times!"

Shon Olson, Network Admin, Smart-Fill Management Group

"AMP simplified SecOps and integration with Threat Response helped speed up investigations."

Security Mgr, Metals & Mining Company

"Cisco AMP has taken our time to remediate from hours to minutes."

Neal Gravatt Sr Network Engineer at a Real Estate/Law

"We significantly reduced our time for detection & remediation, enabling a focus on other Security areas."

Amit Mathur, IT Specialist, Convergent Corporation

"Cisco AMP has made breach defense reach all-time highs. It helps me sleep better at night!"

Ryan Paul, IT Specialist, Thunder Bay Regional HSC

"Cisco Secure Endpoint is 21st century endpoint protection."

Wouter Hindriks, Technical Team Lead at Missing Piece BV

Gartner peer insights. LEADER IT Central Station TechValidate by SurveyMonkey

"It has decreased time to detection by 95% and a 97% reduction in time to remediate."

Cole Two-Bears, Systems Architect NHS Management

"AMP has increased the confidence in our detection ability. It co-exists perfectly with our other solutions."

Ludovic Varet, Chief Security Officer, Gecina

"Productivity increased. Automated email alerts improved security ops."

Chief Security Officer, Small Business Healthcare Company

"With every incident, at least six to 10 man-hours are saved."

Wouter Hindriks, Technical Team Lead at Missing Piece BV

"AMP Gives The Visibility, Detection and Remediation Organizations Need."

Security Admin, $50M+ Healthcare

"We had two ransomware attacks before AMP. We haven't had another one since. Great Software!"

Jeremy Johnson, Network Admin, Perry-Spencer Communications

"In combination with Cisco Umbrella we see a reduced impact on the business."

Tim Crosweller, IT Manager, Security Consulting

"It's given us visibility that we otherwise didn't have by 80%."

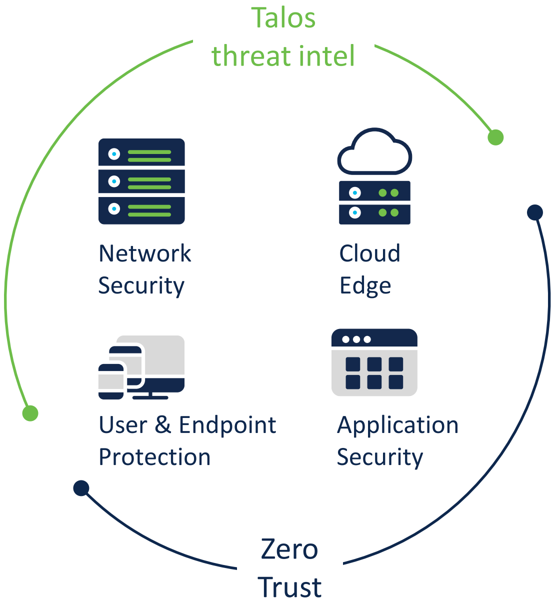
Mark Bonnamy, Technical Director at Ridgewall Ltd

cisco SECURE

Cisco Secure portfolio: simpler to buy and use

Security Choice Enterprise Agreement

- Great discounts on 2+ security products with support included
- Buy what you need now and add more in the future
- Single coterminous agreement managed in one portal
- Built-in 20% growth allowance with true forward terms
- Pay annually with 0% financing



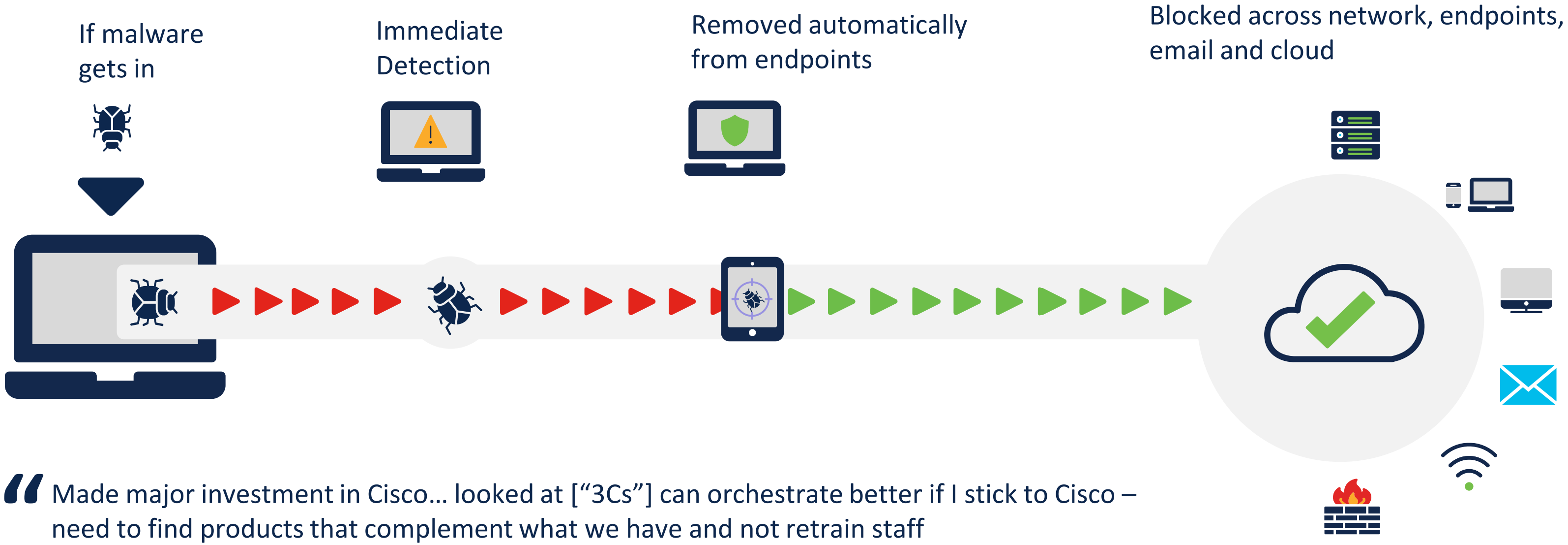
SECURE X

- Cloud-native, built-in platform experience including XDR capabilities and beyond
- Integrated and open for simplicity with true turnkey interoperability
- Unified in one location for visibility that accelerates your time to detect and investigate
- Maximized operational efficiency that accelerates your time to remediate

Protect

Save time and block more with security that works together

See once, block everywhere



If malware gets in

Immediate Detection

Removed automatically from endpoints

Blocked across network, endpoints, email and cloud

> “Made major investment in Cisco… looked at [“3Cs”] can orchestrate better if I stick to Cisco – need to find products that complement what we have and not retrain staff
> – Security Director

Higher security efficacy with the least false alarm

Validated by 3rd party tests: AV Comparatives, Miercom, and NSS Labs

Recognized for accuracy, reliability and consistency

Strong prevention – multiple engines and blocking tools

	Protection Rate	False Alarms
Malware Protection Test	100%	0
Real World Protection Test	99.3%	1

False Alarm Test

“Very High” FP has as many as 100-150 false positives

AV comparatives APPROVED Business Security DEC 2019

	FP rate on non-business Software
Acronis, Avast, Bitdefender, Cisco, ESET, Fortinet, G Data, Kaspersky, Sophos	Very Low
Cybereason, FireEye, SparkCognition, Microsoft	Low
Elastic, Viopre, Vmware,	Medium
K7, Panda	High
CrowdStrike	Very high

Factsheet Business Test (March-April 2020), go to: https://www.av-comparatives.org/tests/business-security-test-march-april-2020-factsheet/

Detect & Respond

Know everything about the endpoint and respond with

Advanced Endpoint Detection and Response (EDR)

Detection

- Continuous activity monitoring
- Advanced endpoint search
- Sandboxing
- Cloud IOCs
- Threat hunting
- Vulnerable and low prevalence software identification
- Unmanaged endpoint discovery

Response

- Custom block/allow lists for files and network traffic
- Application control and allow list
- Endpoint isolation
- Accelerate threat response with an integrated security platform

Improve security & IT Ops alignment and simplify threat hunting with

Orbital Advanced Search

Key capabilities:

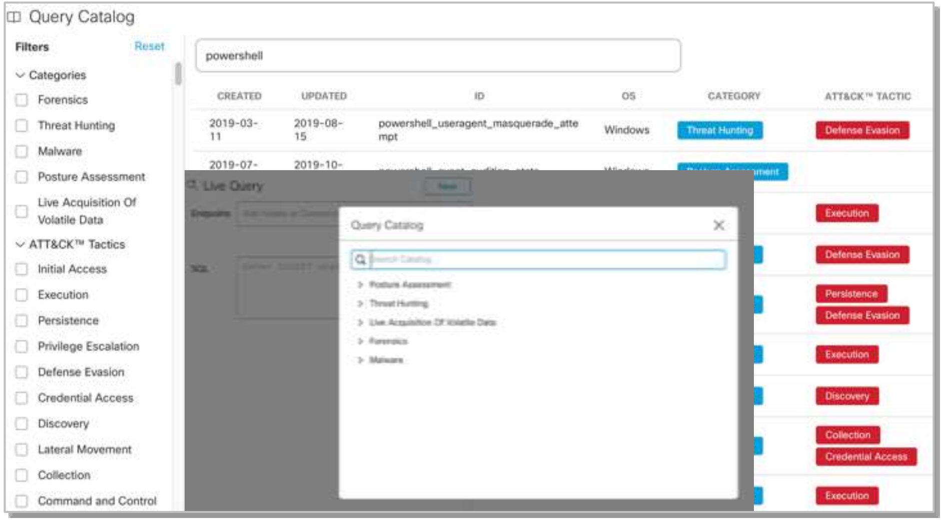
Advanced search; pre-defined, customizable queries; forensics snapshot

Primary use cases:

Threat hunting; IT operations enablement, and vulnerability and compliance tracking

Benefits:

Faster investigation and quicker response, seamless investigation and remediation



Query Catalog

Filters Reset

powershell

Categories

- □ Forensics
- □ Threat Hunting
- □ Malware
- □ Posture Assessment
- □ Live Acquisition Of Volatile Data

ATT&CK™ Tactics

- □ Initial Access
- □ Execution
- □ Persistence
- □ Privilege Escalation
- □ Defense Evasion
- □ Credential Access
- □ Discovery
- □ Lateral Movement
- □ Collection
- □ Command and Control

CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC
2019-03-11	2019-08-15	powershell_useragent_masquerade_attempt	Windows	Threat Hunting	Defense Evasion
2019-07-	2019-10-	[illegible]	[illegible]	Posture Assessment	
					Execution
					Defense Evasion
					Persistence Defense Evasion
					Execution
					Discovery
					Collection Credential Access
					Execution

Live Query

Query Catalog

Search Catalog

- Posture Assessment
- Threat Hunting
- Live Acquisition Of Volatile Data
- Forensics
- Malware

Orbital Advanced search

Use cases

Threat Hunting

Search for malicious artifacts in near real-time to accelerate your hunt for threats.

Incident Investigation

Get to the root cause of the incident fast, to speed up remediation.

Vulnerability and Compliance

Check system status (OS versions, patches etc.), ensuring hosts comply with policies.

IT Operations

Track disk space, memory, and other IT operations artifacts quickly.

Threat Hunting

Uncover hidden threats faster across your attack surface

Using MITRE ATTACK and other industry best practices

Continuous hunting by elite threat hunters

Human-driven hunts based on playbooks producing high fidelity alerts

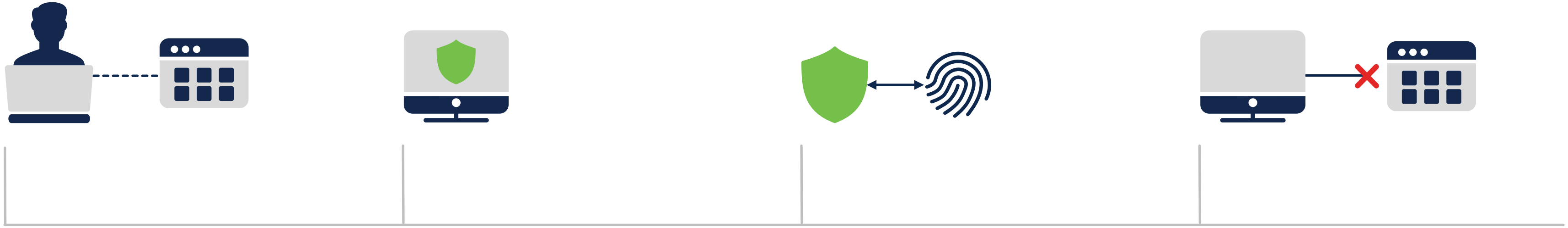
Systematic playbook development

Execute on new and historical data, pushing the frontier of unknown threats

Access

Protect applications from infected devices with the industry’s first “Zero Trust on the Endpoint” approach

Block malicious devices from accessing applications.



Users use their devices to access application.

Cisco Secure Endpoint running on the device detected malware.

It notifies the MFA about the infected device.

MFA blocks that device from accessing apps.

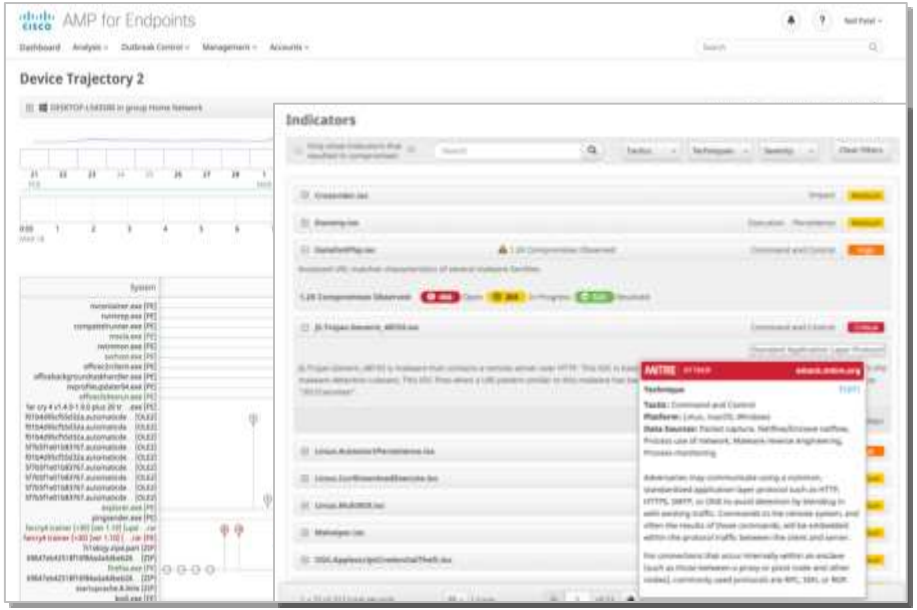
Secure endpoint access from anywhere on any device

Virtual Private Network

- Access from anywhere
- Greater visibility
- Comprehensive protection
- Ease of use and management

Eliminate blind spots with continuous monitoring and retrospective alerting

- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is it doing?
- How do we stop it?



https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html

Why Cisco?

Market Presence

6000+ endpoint security customers

15M+ protected endpoints

70k AMP Ecosystem customers

100M DNS security customers

Industry's first unified user access and device protection solution

See once, block everywhere

Strong Portfolio

- 200B DNS requests/day
- Broad OS/multi-platform support
- Strong third-party integration
- Visibility beyond managed endpoints
- EPP + EDR + XDR capabilities in single agent

Validation

- Deployed globally
- Leader in Zero Trust
- Third-party testing
- Fast ROI: 85% saw value in ~1 wk

2.2

trillion artifacts analyzed daily more than any vendor

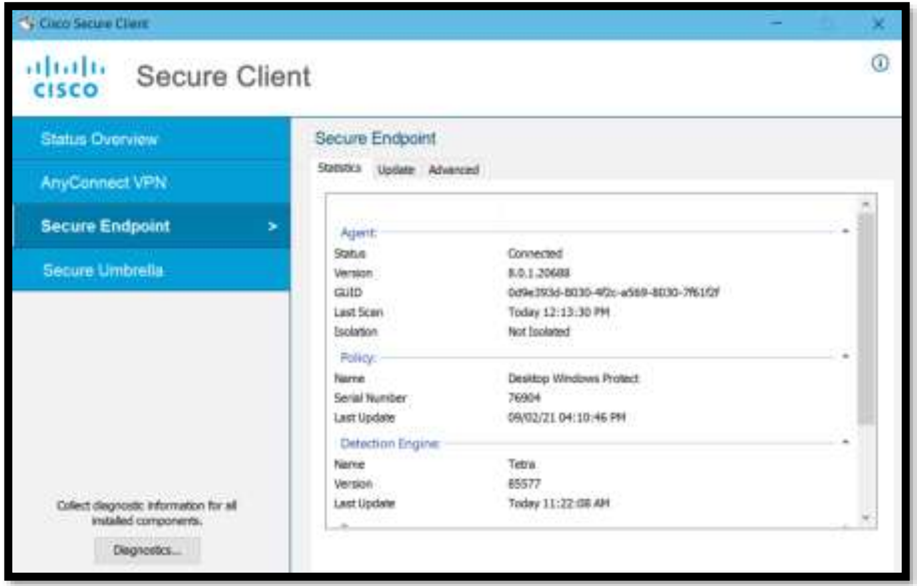
TALOS

Cisco Secure Client

Introducing Cisco Secure Client

Simplifies security with **ONE agent** across **SASE, XDR** and **Zero Trust**

- ONE agent driving operational efficiency
  - Unifies deployment, updates and management
- ONE agent radically reducing agent fatigue
  - Single agent for Secure Endpoint, Umbrella, AnyConnect
- ONE platform
  - Cloud-native, cloud-managed in our built-in SecureX platform
  - Unmatched customer value as it comes included with:
    - Device Insights for deep visibility of all your endpoints, apps and more
    - Indicator of device compromise for easy and fast disposition lookup
    - Fast response actions and remediation



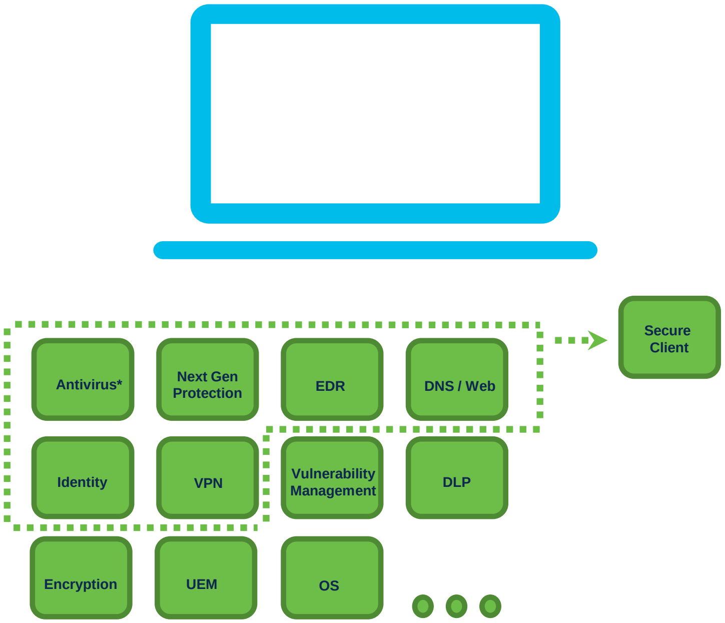
Secure Endpoint

Agent:	
Status	Connected
Version	8.0.1.20688
GUID	0d9e393d-8030-4f2c-a569-8030-7f61f2f
Last Scan	Today 12:13:30 PM
Isolation	Not Isolated
Policy:	
Name	Desktop Windows Protect
Serial Number	76904
Last Update	09/02/21 04:10:46 PM
Detection Engine:	
Name	Tetra
Version	85577
Last Update	Today 11:22:08 AM

Driving Endpoint Operational Efficiency

Better Endpoint Security with operational efficiency rooted in integration and agent consolidation

Unified, Single Agent View



ONE

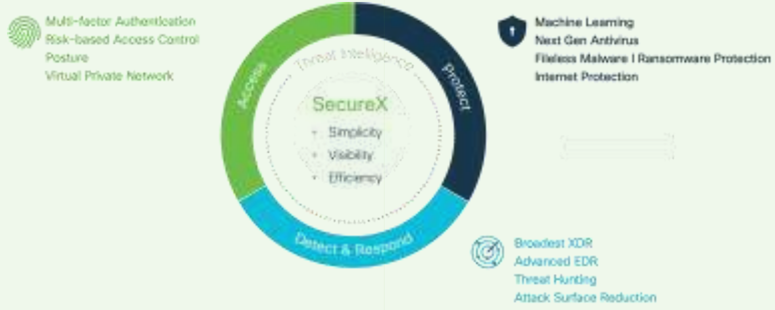
Agent

Consolidation Opportunity

Secure and Trusted Access
To let the good guys in

Block Threats Before Compromise
To keep the bad guys out

Relentless Breach Defense
To uncover the bad guys



CISCO SECURE

*Many customers still run legacy AV on systems (mostly from different vendor)

SecureX DEMO

CISCO SECURE