SentinelOne

ActiveEDR
Wächter und Jäger in einer Person

Warum Endpoint Security nicht an einer Stelle aufhören kann.

Source: https://slidr.io/arthurakay/cybersecurity-it-s-kind-of-a-big-deal-ccc-2017#1

NIST

Cybersecurity Framework

National Institute of Standards and Technology (NIST)

Cybersecurity Framework

Source: https://www.nist.gov/cyberframework/online-learning/five-functions

SentinelOne

NIST

Cybersecurity Framework

IDENTIFY

Identifying physical and software assets within the organization to establish the basis of an Asset Management program

Identifying asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basis for the organizations Risk Assessment

Source: https://www.nist.gov/cyberframework/online-learning/five-functions

NIST

Cybersecurity Framework

PROTECT

Establishing Data Security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

Managing Protective Technology to ensure the security and resilience of systems and assists are consistent with organizational policies, procedures, and agreements

Source: https://www.nist.gov/cyberframework/online-learning/five-functions

NIST

Cybersecurity Framework

DETECT

Ensuring Anomalies and Events are detected, and their potential impact is understood

Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities

Maintaining Detection Processes to provide awareness of anomalous events

Source: https://www.nist.gov/cyberframework/online-learning/five-functions

SentinelOne

NIST

Cybersecurity Framework

RESPOND

Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents

Mitigation activities are performed to prevent expansion of an event and to resolve the incident

The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities

Source: https://www.nist.gov/cyberframework/online-learning/five-functions

NIST

Cybersecurity Framework

RECOVER

Ensuring the organization implements Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents

Implementing Improvements based on lessons learned and reviews of existing strategies

Source: https://www.nist.gov/cyberframework/online-learning/five-functions

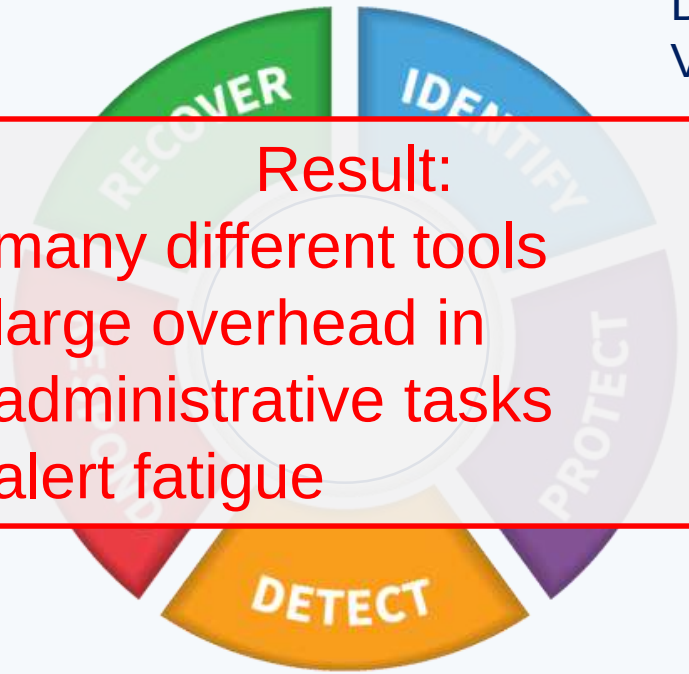
NIST

Cybersecurity Framework

Traditional Approach

Rebuild systems
Reimaging devices

Device Asset Management
Vulnerability Scanner



Result:

- many different tools
- large overhead in administrative tasks
- alert fatigue

EDR – manual incident response

Signaturebased AV
HIPS
Application Whitelisting

Exploit Detection/Protection
EDR – Data Recording

Quelle: https://www.nist.gov/cyberframework/online-learning/five-functions

SentinelOne

NIST

Cybersecurity Framework

SentinelOnes Approach

Machinespeed Recovery
patented remediation
& rollback technology
USPTO Patent No. 10,102,374

Realtime Response
- Autonomous Mitigation
- RemoteShell
- Network isolation

Device Assessment
(Ranger)
Vulnerability Assessment

Static AI
Behavioural AI
ActiveEDR

Advanced EDR
Threathunting

Quelle: https://www.nist.gov/cyberframework/online-learning/five-functions

SentinelOne

UNDERLYING TECHNOLOGY FLOW

SentinelOne

Endpoint Protection
Pre-Execution
Static AI

PE - PDF - Office Docs

ActiveEDR
Autonomous Behavioral AI
Story Tracking

Lateral Movement - Fileless - Exploits - Bad scripts/macros

Respond & Recover
Automatic or
One-click Simple

Kill - Quarantine - Cleanup - Rollback - Disconnect - Shell

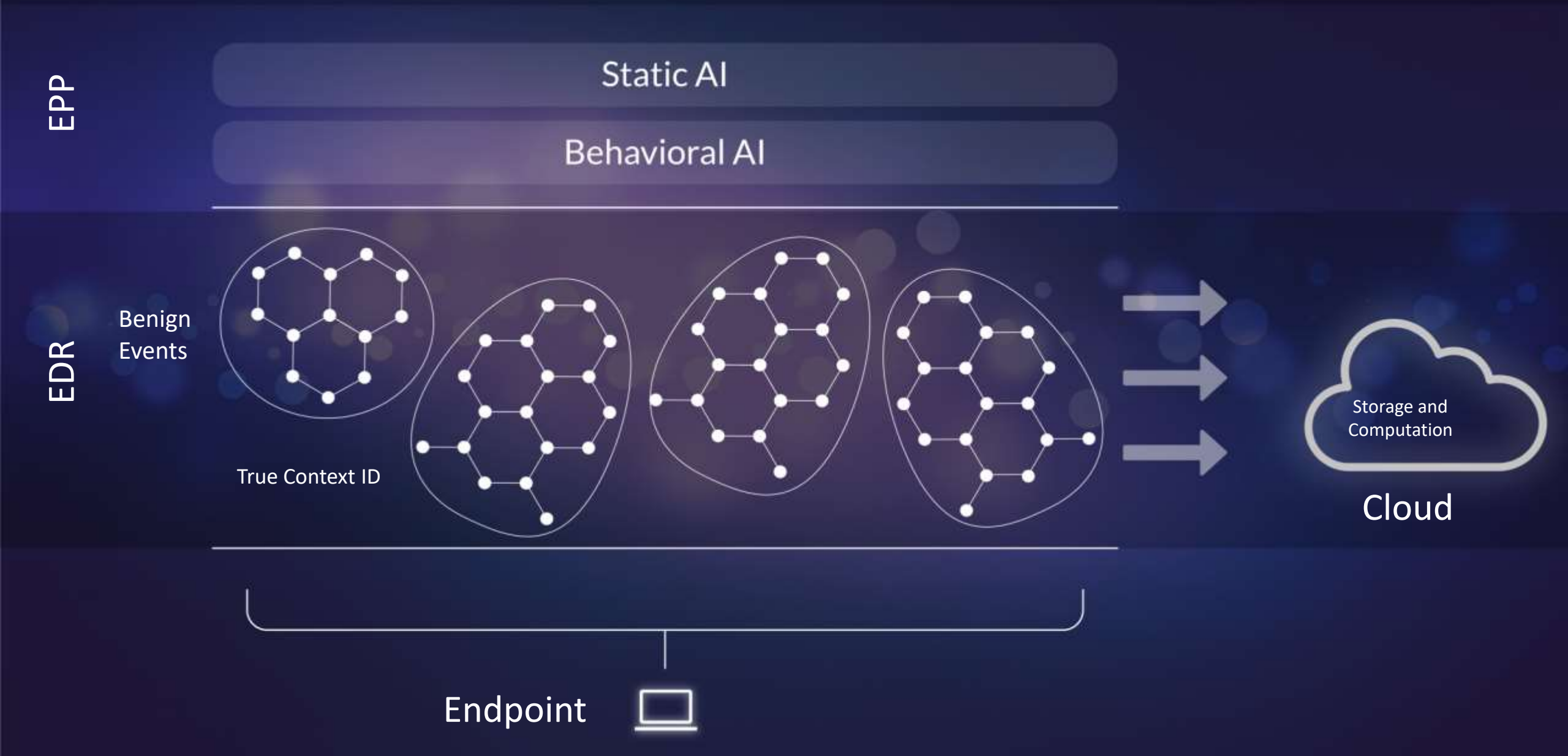
ActiveEDR Advanced
Deep Visibility
Threat Hunting

Visibility - Ease Of Use - Living Off the Land Detection

Timeframe = Seconds
Single, Autonomous Agent Operation / Not Cloud Reliant

Timeframe = 90+ Days
Agent Maintains TrueContext

SentinelOne Autonomous EDR



REAL TIME RESPONSE & RECOVERY

Purpose	How
Take a Protective Action	Automatic or manual agent actions based on policy

USPTO Patent No. 10,102,374

S1 CORE

Kill

Kill offending processes

Quarantine

Isolate offending code

Contain

Isolate victim devices

Remediate

Recover system state with one click

Rollback

Recover ransomed files with one click

S1 COMPLETE

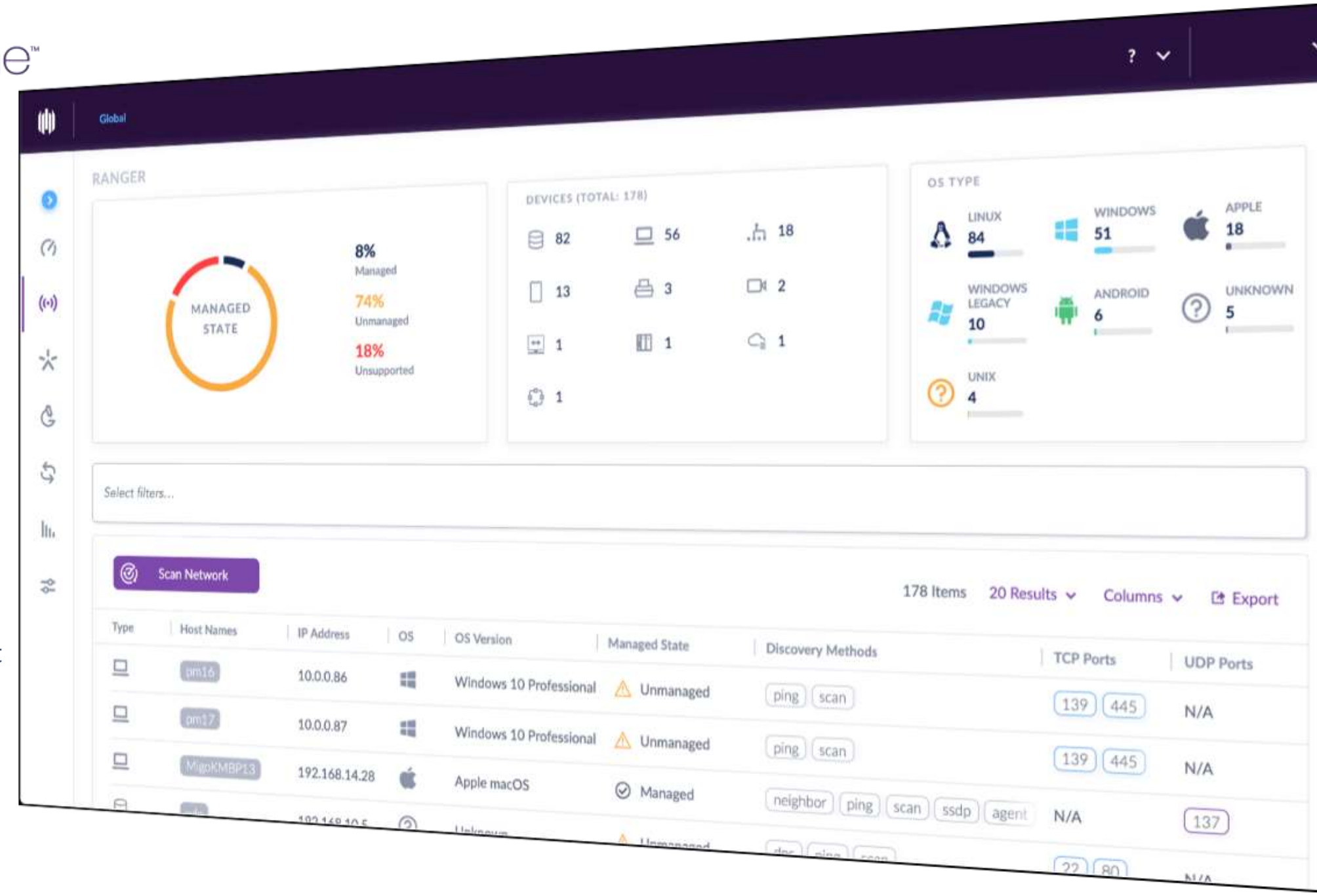
Remote Shell

Complete Powershell / Bash remote shells for deeper IR analysis

SentinelOne™

Ranger

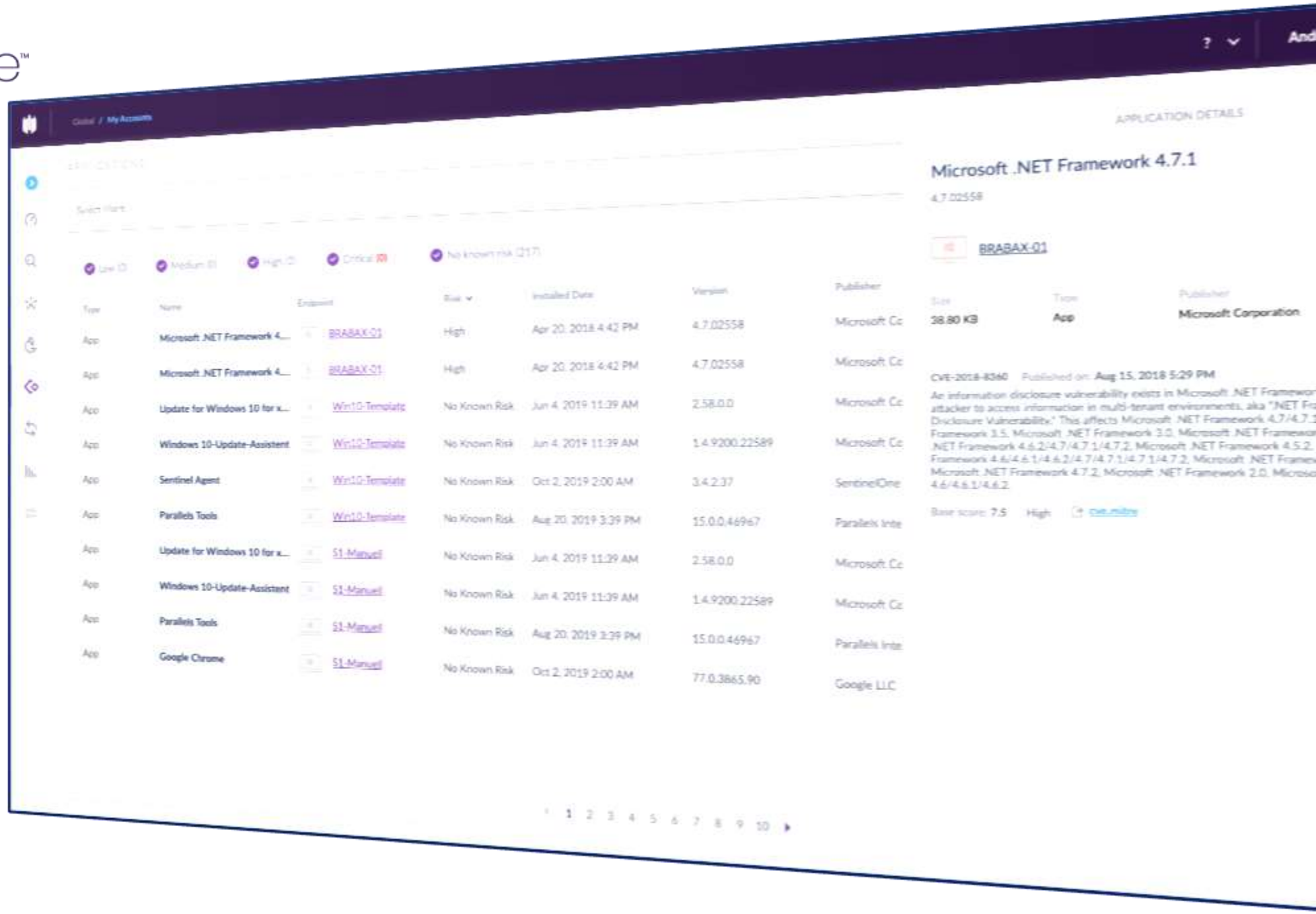
- **Unmanaged Device Discovery**
- **Hunt :** Managed & Unmanaged device communication
- **Identify, Locate, Assess Risk**
- **Mitigate:** Isolate from Network, Deploy Agent
- **Enrich** through Network integrations



SentinelOne™

Vulnerability Assessment

- **Identify vulnerable Applications**
- **CVE Mapping:** Map Application repository to known vulnerabilities
- **Identify, Locate, Assess Risk**
- **Mitigate:** Patch application to mitigate vulnerabilities



THE SOLUTION

SentinelOne

ONE agent, ONE platform

Creating a SOC analyst on every endpoint

THE SOLUTION

SentinelOne

ONE agent, ONE platform

Creating a SOC analyst on every endpoint

ONE AGENT | ONE PLATFORM

SentinelOne

Any OS

- Windows
- Linux
- macOS
- VDI

Any Deployment

- Cloud
- MSSP
- On-prem
- Hybrid

Any Connection

- Online
- Offline

Any Integration

300+ APIs

Any Person

- Big team
- One person
- No team

Any Response

- Automated
- Manual
- Vigilance MDR

Features

- USB Control
- Bluetooth Control
- Firewall Control
- Threat Hunting
- Full Remote Shell
- Vulnerability Reporting
- Advanced Remediation

Conclusion

A cybersecurity solution does not need to be complicated

You can combine multiple roles and do not lose focus

Get rid of multiple tools and administrative overhead

Get the most out of one agent and one platform

How does it look like?

A live demo – right over there!

SentinelOne
Endpoint Security - Completed

Thank you.

Q&A

SentinelOne
Endpoint Security - Completed