



ActiveEDR Wächter und Jäger in einer Person

Warum Endpoint Security nicht an einer Stelle aufhören kann.

CYBERSECURITY

IT'S KIND OF A BIG DEAL

NIST

Cybersecurity Framework

National Institute of Standards and Technology (NIST)

Cybersecurity Framework



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

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

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

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

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

NIST

Cybersecurity Framework

Traditional Approach

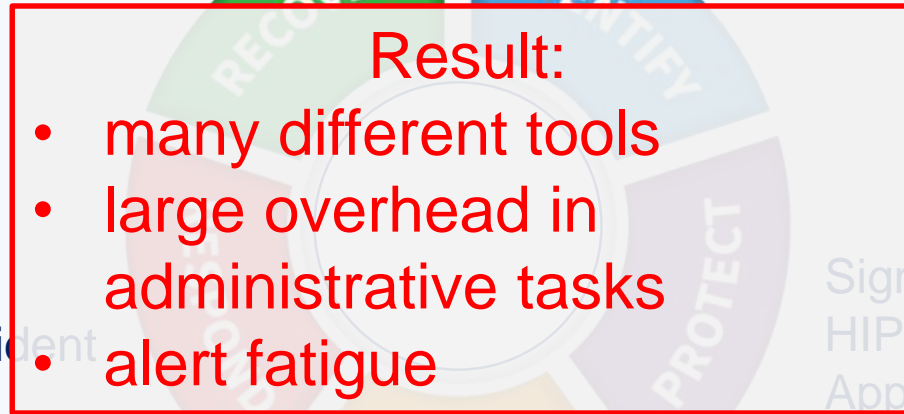
Rebuild systems
Reimaging devices

Device Asset Management
Vulnerability Scanner

EDR – manual incident
response

Signaturebased AV
HIPS
Application Whitelisting

Exploit Detection/Protection
EDR – Data Recording



NIST

Cybersecurity Framework

SentinelOne Approach

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

Realtime Response

- Autonomous Mitigation
- RemoteShell
- Network isolation

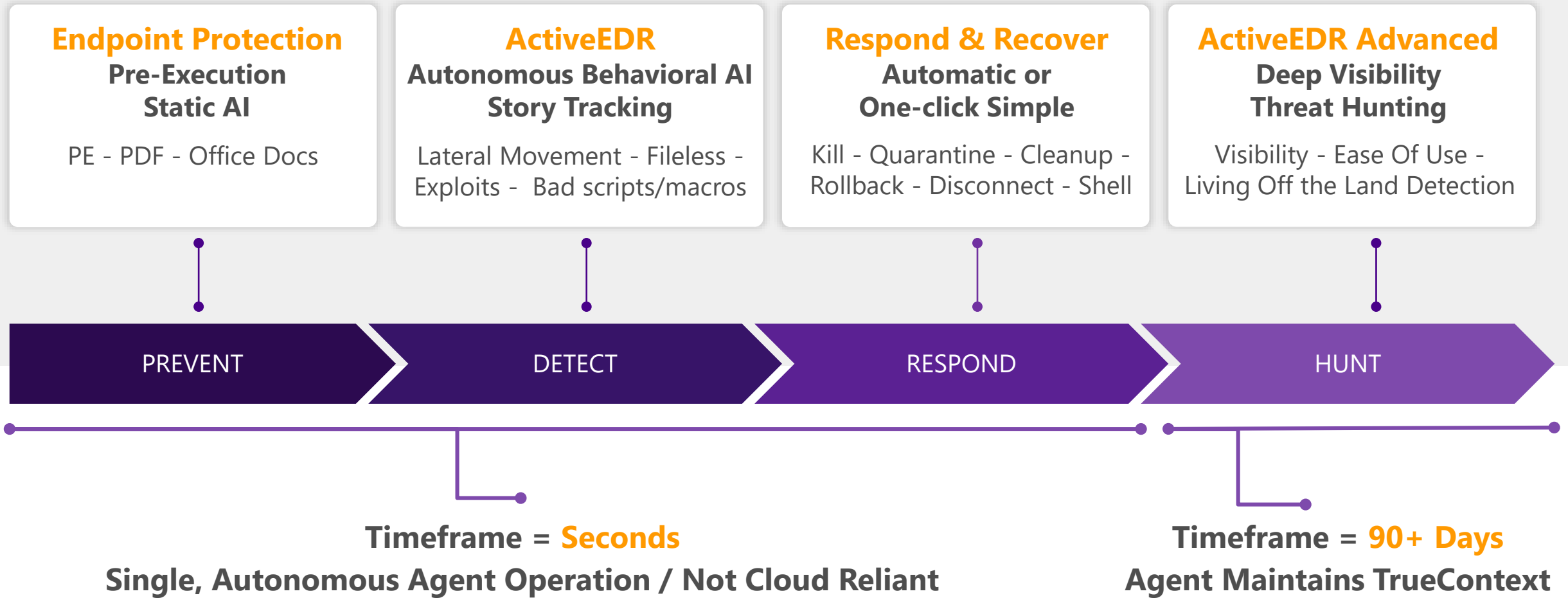


Device Assessment
(Ranger)
Vulnerability Assessment

Static AI
Behavioural AI
ActiveEDR

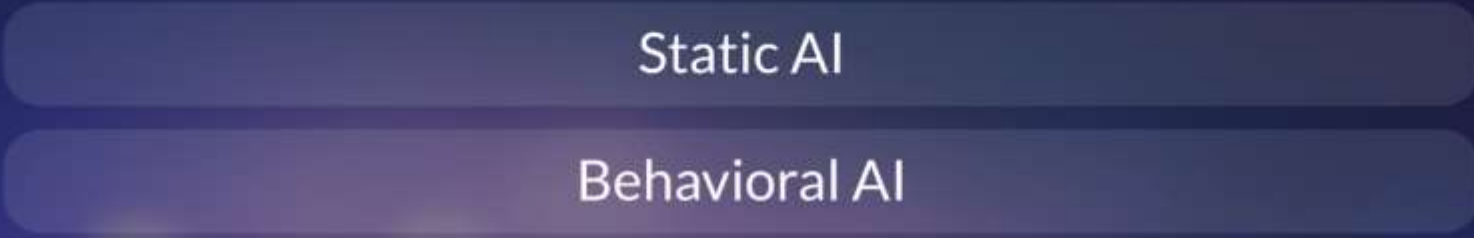
Advanced EDR
Threathunting

UNDERLYING TECHNOLOGY FLOW



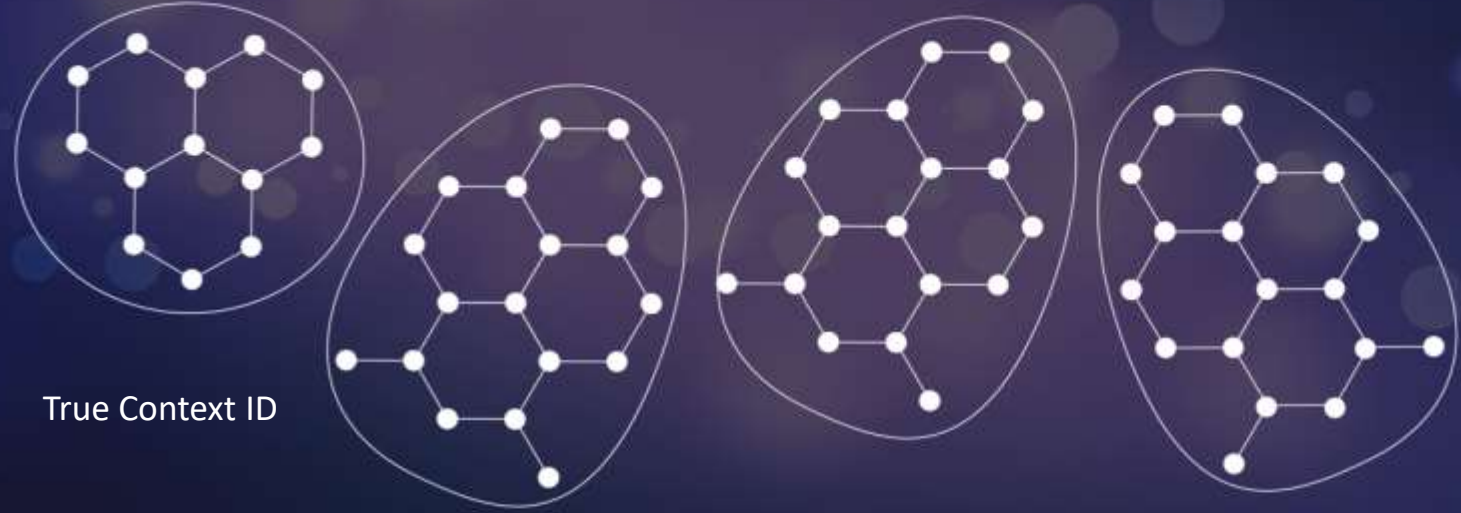
SentinelOne Autonomous EDR

EPP



EDR

Benign Events



Cloud



Endpoint



REAL TIME RESPONSE & RECOVERY

Purpose

Take a Protective Action

How

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

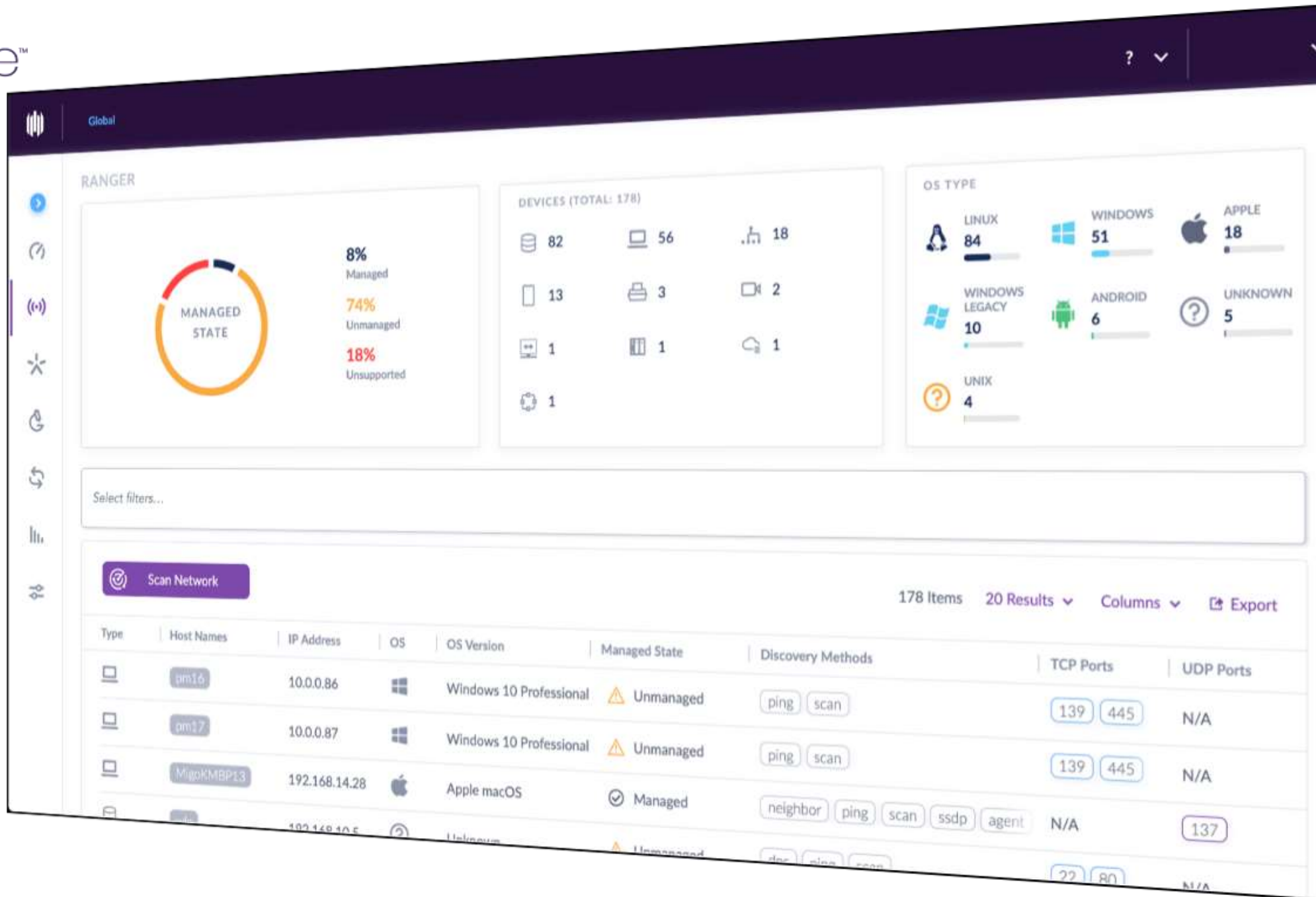


Remote Shell

Complete Powershell / Bash remote shells for deeper IR analysis

Ranger

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



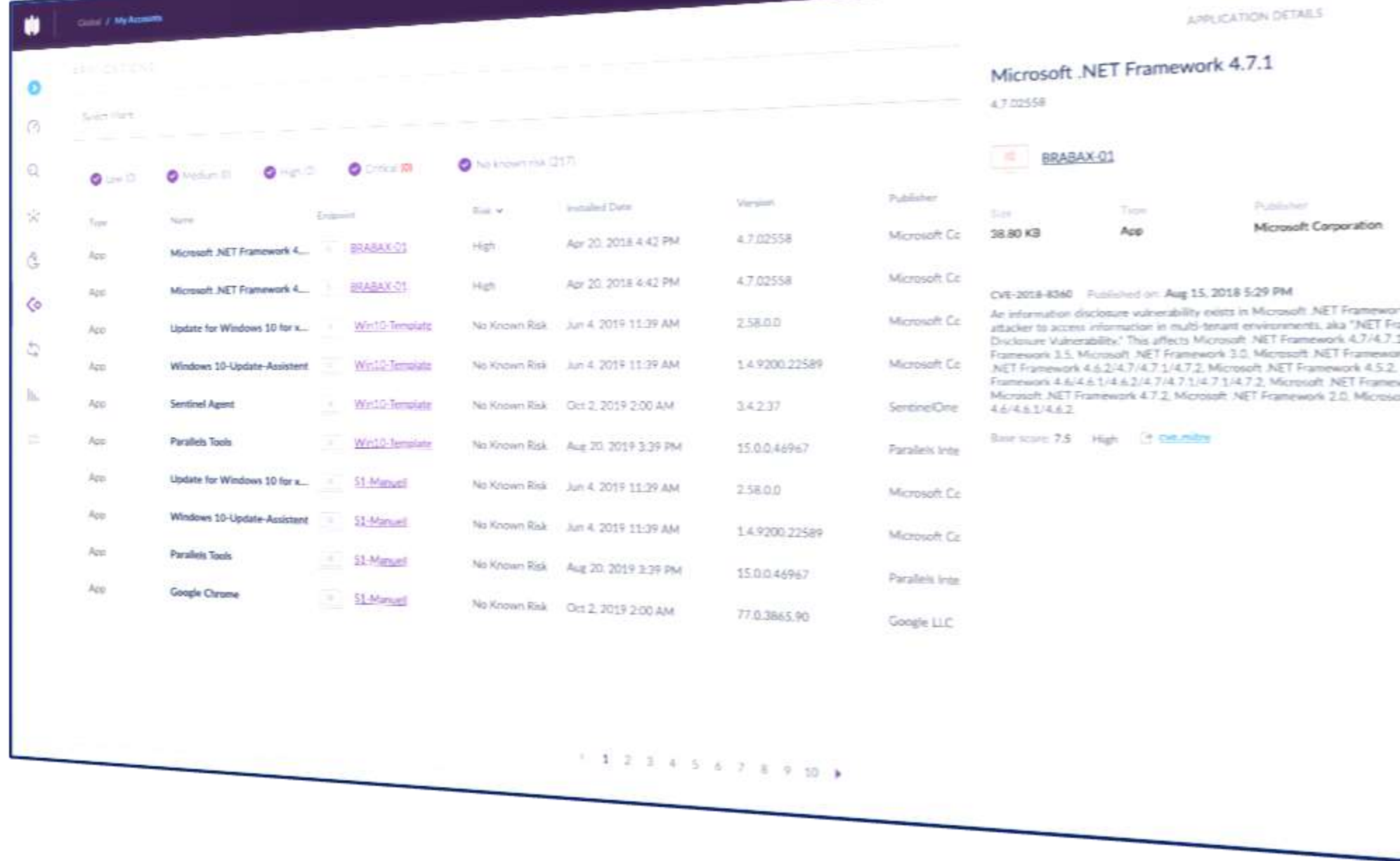
The screenshot displays the Ranger interface with the following components:

- Global** header with a search icon and dropdown menu.
- RANGER** section containing:
 - MANAGED STATE** donut chart: 8% Managed, 74% Unmanaged, 18% Unsupported.
 - DEVICES (TOTAL: 178)** summary: 82 Servers, 56 Laptops, 18 Servers, 13 Mobile, 3 Printers, 2 Cameras, 1 IoT, 1 Storage, 1 Cloud, 1 Misc.
 - OS TYPE** breakdown: LINUX (84), WINDOWS (51), APPLE (18), WINDOWS LEGACY (10), ANDROID (6), UNKNOWN (5), UNIX (4).
- Select filters...** input field.
- Scan Network** button.
- 178 Items | 20 Results** with column and export options.
- Table** with columns: Type, Host Names, IP Address, OS, OS Version, Managed State, Discovery Methods, TCP Ports, UDP Ports.

Type	Host Names	IP Address	OS	OS Version	Managed State	Discovery Methods	TCP Ports	UDP Ports
laptop	pm16	10.0.0.86	Windows	Windows 10 Professional	Unmanaged	ping scan	139 445	N/A
laptop	pm17	10.0.0.87	Windows	Windows 10 Professional	Unmanaged	ping scan	139 445	N/A
laptop	MigokMBP13	192.168.14.28	Apple	Apple macOS	Managed	neighbor ping scan ssdp agent	N/A	137
server	...	192.168.10.5	Unknown	...	Unmanaged	...	22 80	N/A

Vulnerability Assessment

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



The screenshot displays the SentinelOne console interface. On the left, a navigation sidebar includes options like 'Home', 'My Assets', 'Applications', 'Vulnerabilities', 'Incidents', 'Alerts', 'Reports', and 'Settings'. The main area shows a list of installed applications with columns for Type, Name, Endpoint, Risk, Installed Date, Version, and Publisher. Two instances of 'Microsoft .NET Framework 4.7.1' are listed with a 'High' risk level and a 'BRABAX-01' vulnerability. The right-hand pane provides 'APPLICATION DETAILS' for this specific application, including its size (38.80 KB), type (App), publisher (Microsoft Corporation), and a detailed CVE-2018-8360 description. A base score of 7.5 is also shown.

Type	Name	Endpoint	Risk	Installed Date	Version	Publisher
App	Microsoft .NET Framework 4.7.1	BRABAX-01	High	Apr 20, 2018 4:42 PM	4.7.02558	Microsoft Co
App	Microsoft .NET Framework 4.7.1	BRABAX-01	High	Apr 20, 2018 4:42 PM	4.7.02558	Microsoft Co
App	Update for Windows 10 for x...	Win10-Template	No Known Risk	Jun 4, 2019 11:39 AM	2.58.0.0	Microsoft Co
App	Windows 10-Update-Assistent	Win10-Template	No Known Risk	Jun 4, 2019 11:39 AM	1.4.9200.22589	Microsoft Co
App	Sentinel Agent	Win10-Template	No Known Risk	Oct 2, 2019 2:00 AM	3.4.2.37	SentinelOne
App	Parallels Tools	Win10-Template	No Known Risk	Aug 20, 2019 3:39 PM	15.0.0.46967	Parallels Inte
App	Update for Windows 10 for x...	S1-Manual	No Known Risk	Jun 4, 2019 11:39 AM	2.58.0.0	Microsoft Co
App	Windows 10-Update-Assistent	S1-Manual	No Known Risk	Jun 4, 2019 11:39 AM	1.4.9200.22589	Microsoft Co
App	Parallels Tools	S1-Manual	No Known Risk	Aug 20, 2019 3:39 PM	15.0.0.46967	Parallels Inte
App	Google Chrome	S1-Manual	No Known Risk	Oct 2, 2019 2:00 AM	77.0.3865.90	Google LLC

APPLICATION DETAILS
Microsoft .NET Framework 4.7.1
 4.7.02558
 BRABAX-01
 Size: 38.80 KB | Type: App | Publisher: Microsoft Corporation
 CVE-2018-8360 | Published on: Aug 15, 2018 5:29 PM
 An information disclosure vulnerability exists in Microsoft .NET Framework attacker to access information in multi-tenant environments, aka "NET Framework Disclosure Vulnerability." This affects Microsoft .NET Framework 4.7/4.7.1 Framework 3.5, Microsoft .NET Framework 3.0, Microsoft .NET Framework .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2, Microsoft .NET Framework 4.7, Microsoft .NET Framework 4.7.2, Microsoft .NET Framework 2.0, Microsoft 4.6/4.6.1/4.6.2.
 Base score: 7.5 | High | [cve.mitre](#)

THE SOLUTION



ONE agent, ONE platform

Creating a SOC analyst on every endpoint



THE SOLUTION



ONE agent, ONE platform

Creating a SOC analyst on every endpoint



ONE AGENT | ONE PLATFORM

Any OS	Any Deployment	Any Connection	Any Integration	Any Person	Any Response
Windows	Cloud	Online	300+ APIs	Big team	Automated
Linux	MSSP	Offline		One person	Manual
macOS	On-prem			No team	Vigilance MDR
VDI	Hybrid				

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