SentinelOne White Paper

SentinelOne

noetic

Extended Detection and Response & Cyber Asset Attack Surface Management

to Achieve Greater Security Coverage

Table of Contents

The Challenges of Cyber Asset Management	3
What is Extended Detection and Response?	5
What is Cyber Asset Attack Surface Management?	6
Benefits of an XDR and CAASM Integration	7
XDR and CAASM Solution Use Cases	8
Conclusion	9
References	10
Ready for a Demo?	10



01

The Challenges of Cyber Asset Management

As organizations digitally transform due to remote workforce growth and migration to cloud environments, the size of their possible attack surfaces has also drastically increased. Gartner predicts that enterprise attack surfaces are expanding with associated risks from the use of emerging cyber-physical systems, such as cloud-based applications, open-source code, social media, and more.[1]

The specific needs and insights for different assets remain fragmented and siloed from one another. Security analysts have an overwhelming number of vectors to manually manage, in addition to the heightened complexity of internal and external cyber threats for each attack surface. The lack of asset visibility, security coverage gaps, and asset vulnerabilities pose a cybersecurity problem for companies.

1. Asset Visibility

One significant challenge for companies is a comprehensive view of all their cyber assets. Lack of asset visibility is a pitfall because malicious actors can hide their activities behind the guise of regular network traffic. This makes it difficult to determine which assets are at risk as an entry point for attackers. Lack of asset visibility also makes it difficult for security teams to prioritize and focus resources on the business's most critical assets.

Security teams may also not be aware of new and risky assets within the company's network. As departments grow larger with progressing needs, they may bring in line of business (LOB) applications, shadow IT, and other third-party systems without the IT department's knowledge. These latest assets will become new entry points for attackers if they do not have the proper security controls installed.

2. Security Coverage Gaps

Security coverage gaps also pose another critical risk to a company's security posture. Assets missing a crucial layer of protection lead to security coverage gaps. For example, security teams must shuffle among different point-specific tools and technologies to defend against evolving adversaries. The combination of disparate tools and the need for a centralized solution to manage an expanded cyber ecosystem causes oversight of the proper installation and deployment of the correct security tools.

1 Gartner, Top Security and Risk Management Trends for 2022 (2022).

3. Asset Vulnerability

Modern adversaries constantly explore new, advanced, and automated techniques to exploit vulnerabilities and gain further access to an organization's network. Security teams are tirelessly working to patch these vulnerabilities but cannot instantly resolve them. Without prior identification and understanding of each vulnerability, security teams cannot correctly prioritize the most critical ones and efficiently organize their workloads.

4. Addressing Cyber Asset Management

Many security teams currently have to manually identify their assets and ensure the appropriate security controls are in place. This laborious process takes away valuable time from other priorities. It also gives attackers a chance to discover weak points quickly and put businesses in jeopardy.



Security teams can take the following steps to improve upon their cyber asset management system and secure themselves from the cyber threat landscape:

- Retain an up-to-date security asset inventory for the entire organization
- Regularly correlate internal data to ensure accurate and efficient reporting
- Deploy a Cyber Asset Attack Surface Management (CAASM) solution

Enterprises must have an extensive view of their security estate across in one single consolidated view. They need an innovative and modern approach to integrate visibility and automated response actions throughout their organization. The integration of Extended Detection and Response (XDR) and Cyber Asset Attack Surface Management (CAASM) equip organizations with visibility, detection, and response capabilities to an extensive asset inventory.

02

What is XDR?

Extended Detection and Response (XDR) brings comprehensive prevention, detection, analytics, and automated response capabilities across multiple security layers. It is an evolution of Endpoint Detection and Response (EDR), which primarily focuses on endpoint functionality and protection. According to the IBM Cyber Resilient Organization Study from 2021, 30% of their respondents said their organizations deploy more than 50 tools and technologies for security. The growing utilization of security tools and technologies across the security estate marks a need for XDR and its scope to centralize visibility and response capabilities, and broaden to more surfaces: endpoints, servers, network security devices, cloud workloads, email, and beyond.

30%

of respondents said their organizations deploy **more than 50** tools and technologies for security.

Source: IBM Cyber Resilient Organization Study 2021

With correlated data and insight from the entire cybersecurity ecosystem, XDR solutions provide businesses with more effective detection and response.

XDR Solution Highlights

- Maximize detection visibility across multiple security levels without worrying about critical blind spots and data silos.
- Accelerate investigation and threat hunting with custom hunting and response rules.
- Automate response actions to quickly remediate threats across an entire connected ecosystem.

XDR Benefits

- Increase SOC efficiency and productivity with a single centralized dashboard to reduce context switches and juggling different platforms.
- Reduce mean time to detect, investigate, and respond with correlation across numerous data sources and fast automation.
- Streamline security workflows with various out-of-the-box integrations to achieve the maximum potential from all your security platforms.

03

What is CAASM?

According to Gartner, cyber asset attack surface management (CAASM) is an 'emerging technology that enables security teams to solve persistent asset visibility and vulnerability challenges. CAASM solutions aggregate data from existing tools and data feeds to provide a continuous, multidimensional view of an organization's entire attack surface.'

CAASM solutions provide a new kind of visibility into an organization's security posture by unlocking asset data from already deployed tooling, such as XDR, as well as a business context from systems such as the Configuration Management Database (CMDB) and external threat and exploitability resources. These combined insights enable the security team to prioritize their workload effectively.



CAASM Solution Highlights

- Build on existing security and IT tools to create a multidimensional map of all assets in the organization, and the cyber relationships between them.
- Identify common cybersecurity posture challenges, such as security coverage gaps and non-compliant controls.
- Automate cyber hygiene remediation across the cloud and on-premises.



CAASM Benefits

- Reduce the attack surface by identifying coverage gaps, high-risk vulnerabilities, and common misconfigurations.
- Expedite the incident response process by leveraging asset intelligence to help the IR team focus on high-risk incidents.
- Drive a prioritized approach to vulnerability management by combining insights on asset criticality and exposure with vulnerability severity and exploitability.

04

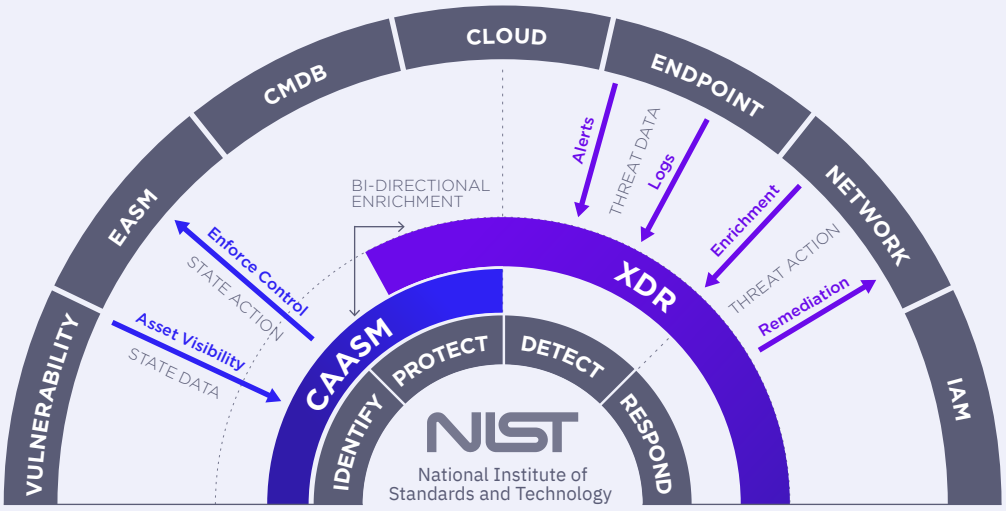
Benefits of an XDR and CAASM Integration

The combination of XDR and CAASM is an example of how complementary security technologies can extend their value. CAASM solutions rely on other security tools for asset intelligence and XDR is an excellent source of that data via native endpoint, identity, and cloud telemetry.

In return, CAASM solutions can provide XDR response workflows with enriched asset intelligence to provide great context and prioritization. This data might include information on asset exposure or criticality and the potential blast radius if it has been compromised.

XDR and CAASM Integration Benefits

- Automate the proactive deployment of XDR agents to unprotected endpoints to reduce coverage gaps
- Broadens the scope of XDR implementation to a broader asset inventory for better visibility, detection, and remediation
- Correlate XDR telemetry with other cyber assets in the business for maximum coverage, context, and insight



05

XDR and CAASM Solution Use Cases

1. Missing Agent Discovery & Remediation

Security teams must understand when virtual or physical machines are deployed without the necessary XDR agents. A CAASM solution builds its asset inventory across different tools and platforms, such as AWS, Microsoft Active Directory, ServiceNow, and more. For example, this correlated data allows security teams to identify 'negative space', where a machine exists in AWS, but not in the XDR management console.

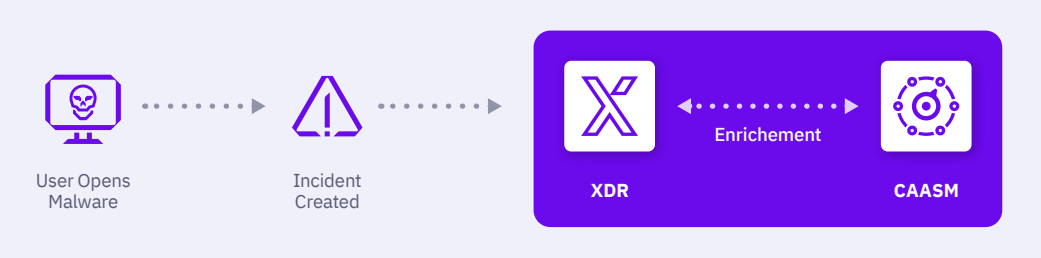
The CAASM solution triggers an automated workflow to enroll the machine, deploy the missing XDR agent, and start an initial scan for threats.

2. Vulnerability Prioritization

All companies have more vulnerabilities than they can patch. Modern XDR solutions play a crucial role in identifying and enumerating vulnerabilities across the systems they manage. By combining this information with the CAASM solution, we can generate a prioritized list of vulnerabilities to work on, combining threat insights from the XDR solution with asset and business content from the CAASM tool.

3. Incident Response (IR) Support

SecOps and IR teams rely on XDR for triaging threats and automating the appropriate response. However, the volume of incidents is still too high for many organizations. Integrating CAASM and XDR solutions can help SOC analysts to focus their cycles on the most significant risks to the business.

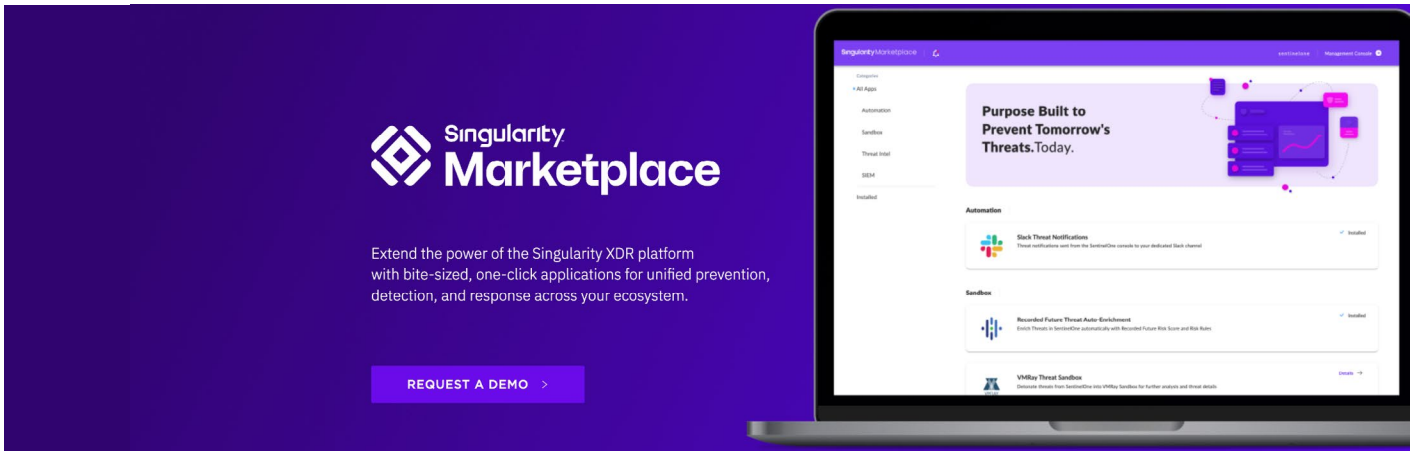


CAASM tools can provide automated enrichment and asset intelligence into XDR solutions with important information and context on indicators of compromise (IoC). If an analyst can understand whether a machine name or IP address is related to a business-critical application, or high-risk user, then they can prioritize their response accordingly.

06

Conclusion

SentinelOne and Noetic Cyber are ready to help your enterprise security team achieve unified prevention, detection, and response against known and emergent cyber threats. The Singularity XDR and CAASM integration is prepared to help you identify and extend protection to vulnerable assets. Read more about the XDR and CAASM integration from our SentinelOne and Noetic Cyber Joint Solution Brief.



About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

About Noetic Cyber

Noetic provides a proactive approach to cyber asset and controls management, empowering security teams to see, understand, fix and improve their security posture and enterprise ecosystem. Our goal is to improve security tools and control efficacy by breaking down existing siloes and improving the entire security ecosystem. Founded in 2019, Noetic is based in Boston and London. For more information, visit www.noeticcyber.com, or follow us on LinkedIn or Twitter.

Learn More About Singularity XDR and CAASM

- Integrated Cyber Asset Management and Remediation Webinar
- Reduce Risk with Unified XDR and Cyber Asset Management
- Begin Your XDR Journey with Frictionless One-Click Integrations
- SentinelOne Singularity XDR Solution Brief

07

References

- Gartner, Top Security and Risk Management Trends for 2022 (2022)
- IBM, Cyber Resilient Organization Study (2021)
- Gartner, Hype Cycle for Security Operations (2021)

Ready for a Demo?

Visit the SentinelOne website for more details,
or give us a call at +1-855-868-3733

sentinelone.com

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

Gartner peerinsights™ 4.9

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP

ISO 27001 CERTIFIED by schellman

TEVORA

PCI DSS Attestation
HIPAA Attestation

SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

S1_WP_015_XDR_CAASM_12122022

© SentinelOne 2022