mondoo

Building a Stronger Security Posture with Extensible Security Posture Management (xSPM)

Introduction

Ransomware attacks are a significant threat to organizations of all sizes, causing significant financial and reputational damage. Extensible Security Posture Management (xSPM) is a set of practices and open source tools that help organizations ensure the security and compliance of their complete infrastructure (e.g. on-prem, Cloud, SaaS). xSPM is an essential component of an organization's cybersecurity strategy. It plays a key role in helping prevent ransomware attacks and is a crucial tool for ensuring security and compliance across the different layers of infrastructure (e.g., Cloud, Kubernetes, Containers, SaaS, Linux, Windows, On-Prem, and VMware).

xSPM can help organizations optimize their IT infrastructure and reduce operational costs through streamlined processes and better resource utilization. Implementing xSPM leads to cost savings by consolidating and simplifying security tools and processes. It also helps organizations reduce the need for external resources and consultants, leading to cost savings in the long term. By ensuring compliance with industry regulations and standards, xSPM helps organizations avoid costly fines and penalties.

In this whitepaper, we will discuss the importance of xSPM and how it can help organizations protect their infrastructure from security threats and meet regulatory compliance.

TABLE OF CONTENTS

What is the procedure of a ransomware attack?

The threat of ransomware attacks grows as attackers become more experienced and strategic. A recent, independent survey of 1100 global IT and cyber security professionals found that:

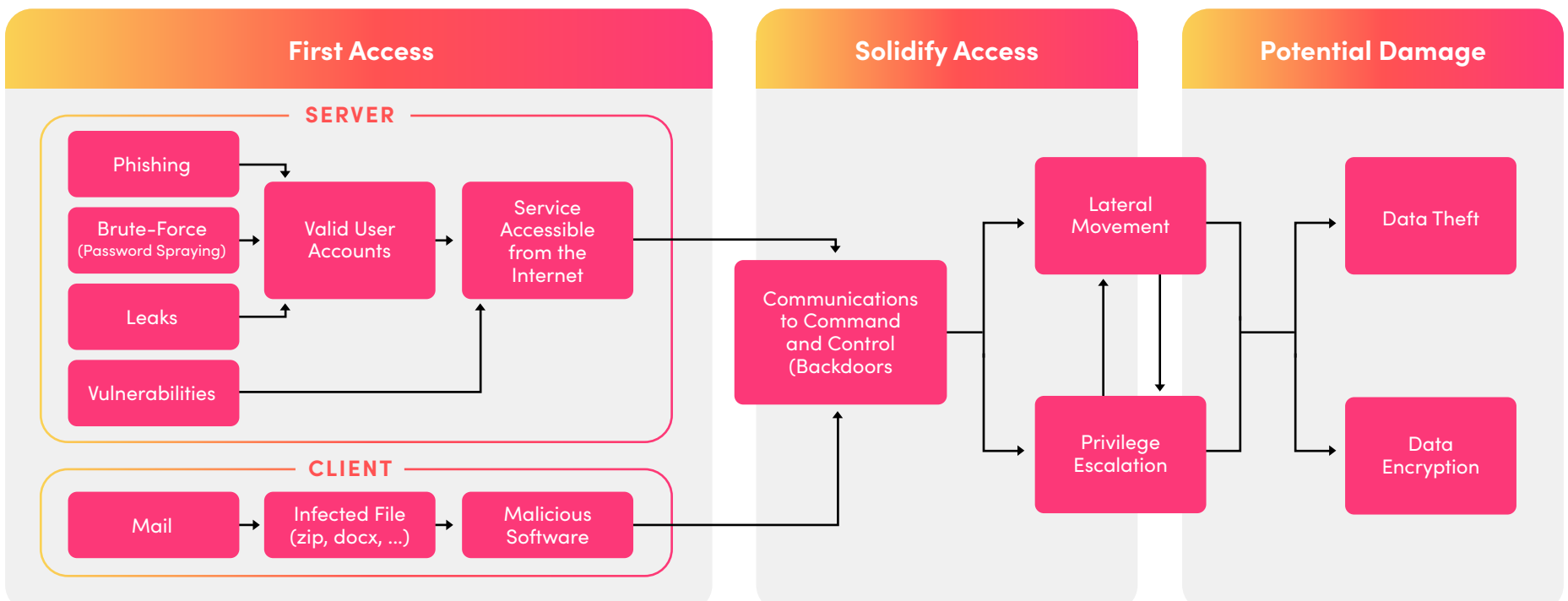
80%
were victims of ransomware attacks in 2022

MORE THAN 60%
of victims paid the ransom

(Forbes)

Across the globe, attackers are increasingly successful at penetrating IT environments and shutting down operations. This means your organization can not work, machines can not produce goods, and products or services cannot be delivered to your customers. Shielding your infrastructure from these sophisticated criminals requires understanding how they work. Fortunately, most ransomware attackers follow similar patterns. By studying these attacks, organizations are able better to protect themselves from their devastating and costly consequences.

A successful ransomware attack can be divided into three phases. The following picture shows a typical attack path.



1. **FIRST ACCESS PHASE:** Attackers gain initial access to the corporate network (e.g., On-Prem, Cloud, SaaS).

2. **SOLIDIFY ACCESS PHASE:** Attackers spread throughout the corporate network. They install multiple backdoors to gain many different ways to access the corporate network at any time.

3. **POTENTIAL DAMAGE PHASE:** Attackers steal data and encrypt the entire corporate network at different levels. (For example, they might encrypt on the Windows and hypervisor levels.) They also destroy backups so that organizations have no choice but to negotiate a ransom for their data and systems.

If you carefully analyze the behavior and the tools used during these attack phases, you can identify two main reasons why attackers are successful in compromising organizations:

- **Infrastructure components are not up to date with the latest patches**, e.g., operating system patches, packages, and libraries.
- **Infrastructure components do not have secure configurations,** e.g., operating system services, cloud services, SaaS, and Kubernetes.

The same root causes are also corroborated in the Cyber Signals Report by Microsoft that revealed 80% of attacks can be attributed to outdated software and misconfiguration.

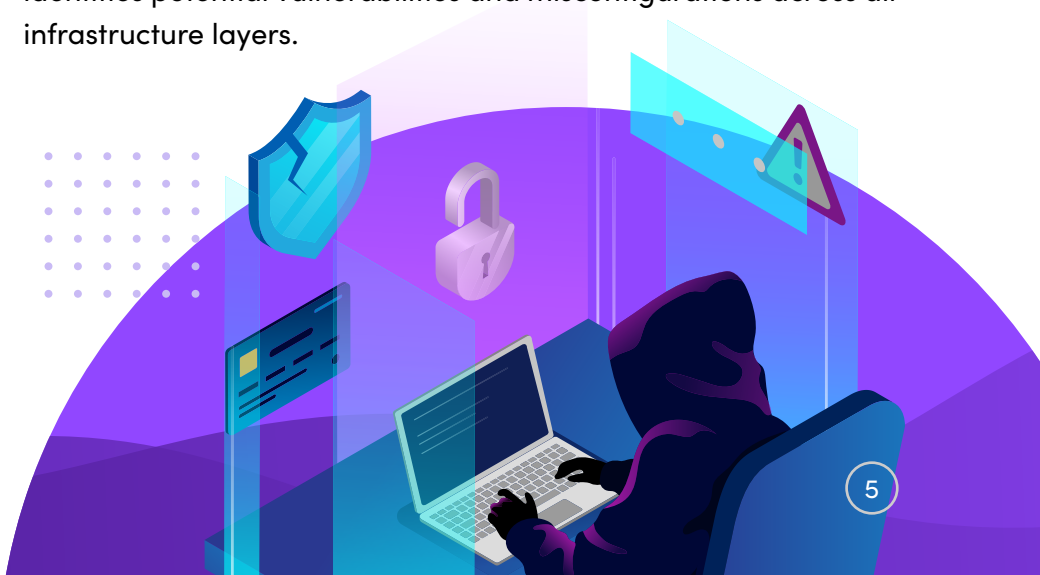
Most organizations are not aware of how vulnerable they are. Time and time again, when we see companies become victims due to one or both of these risks, it's because the vulnerable versions and misconfigurations are not visible across their entire infrastructure.

Without a complete understanding of their technical issues across their fleet, companies can't perform an appropriate risk assessment and countermeasures. In order to implement the above points effectively and efficiently, organizations need extensible security posture management.

What is security posture management?

Security posture management (SPM) is the process of assessing, improving, and maintaining the security posture of an organization and its infrastructure. It involves identifying potential risks and vulnerabilities, implementing controls to mitigate those risks, and continuously monitoring and reviewing the effectiveness of those controls.

The goal of SPM is to ensure that an organization has strong security practices that can protect against potential threats and risks. This requires a proactive approach to security, where an organization continuously assesses its environment and identifies potential vulnerabilities and misconfigurations across all infrastructure layers.



Security posture management typically involves a range of activities, including:

- **Data collection:** Collecting the required data about the infrastructure.
- **Risk assessment:** Identifying and evaluating an organization's potential risks, vulnerabilities, and misconfiguration.
- **Control implementation:** Implementing controls and measures to mitigate identified risks, vulnerabilities, and misconfiguration, such as network security, access controls, hardening, and data security measures.
- **Monitoring and review:** Regularly reviewing and evaluating the effectiveness of security controls and measures and making any necessary adjustments to ensure that they remain effective.
- **Incident response:** Developing and implementing a plan to respond to security incidents, such as data breaches or unauthorized access to systems.

Effective SPM requires an organization to clearly understand its security goals and the resources and capabilities available to achieve those goals. It also involves the development of robust security infrastructure to ensure that they understand their role in maintaining the organization's security posture.

To implement SPM, traditionally, many different tools were used for the different infrastructure layers, like on-prem, cloud, and CI/CD. This resulted in a fragmented view of the infrastructure and made holistic risk assessment and countermeasures very difficult, as there was no single view of the infrastructure layers and their data.

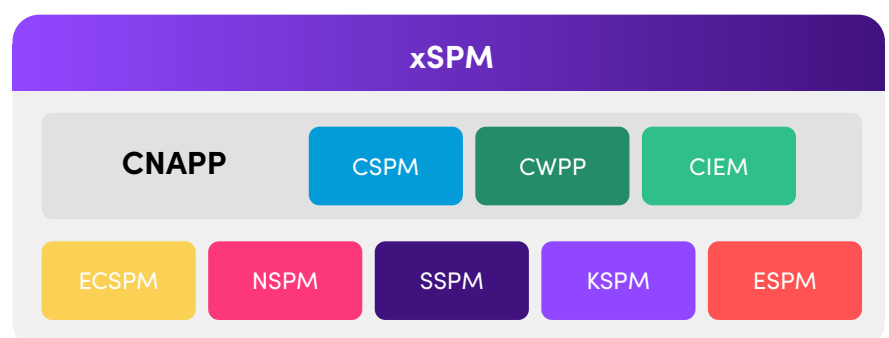
What is extensible security posture management?

Extensible security posture management (xSPM) is a set of practices and open source tools that help organizations ensure the security and compliance of their complete infrastructure (e.g. on-prem, Cloud, SaaS). xSPM typically involves:

- Automated and continuous monitoring
- Managing an organization's entire infrastructure and applications
- Data to identify and mitigate potential security threats, vulnerabilities, and misconfiguration across the infrastructure layers

Traditional security tools and approaches are designed to protect on-premises data centers and endpoints, not cloud-native applications or services. Cloud security tools are developed for modern cloud technologies and do not support on-premises applications and SaaS services. This results in a fragmented view of the infrastructure. With an xSPM solution, organizations can collect data and monitor the complete infrastructure stack for security and compliance.

An xSPM solution consists of the following parts:



Cloud-Native Application Protection (CNAPP)

An effective CNAPP helps security teams and administrators correlate information from various signals into a single view to identify and prioritize the organization's most significant risks by aggregating them. In doing so, CNAPP consists of CSPM, CWPP, and CIEM.

Cloud Security Posture Management (CSPM)

Cloud security posture management (CSPM) is an automated security solution that manages the monitoring, identification, alerting, and remediation of compliance risks and misconfigurations in cloud environments, such as AWS, Azure, and GCP. One of the key features is continuous monitoring for security policy enforcement gaps.

Furthermore, the solution includes agentless and agent-based vulnerability (CVE) and misconfiguration detection for operating systems, packages, and libraries on virtual machines, containers, serverless functions, appliances, and non-agent workloads.

For example, a common misconfiguration is accidentally granting public read permissions to s3 buckets.

Cloud Workload Protection Platforms (CWPP)

A cloud workload protection platform (CWPP) is a security solution that addresses the security needs of workloads in modern hybrid, multi-cloud, and data center environments. An effective CWPP can provide consistent control and visibility for physical machines, virtual machines, containers, and serverless workloads, wherever they reside.

For example, CWPP can find vulnerabilities and misconfigurations in all workloads, like virtual machines and containers.

Cloud Infrastructure Entitlements Management (CIEM)

Cloud infrastructure entitlement management (CIEM) is an automated cloud security solution that mitigates the risk of data breaches in public cloud environments. CIEM solutions prevent excessive entitlements by continuously monitoring human and non-human entities' permissions and activities to ensure they operate within appropriate access controls.

For example, CIEM creates a complete inventory of all accounts in your AWS Cloud and their permissions for the different resources.

Kubernetes Security Posture Management (KSPM)

Kubernetes security posture management (KSPM) uses security automation tools to detect and fix security and compliance issues in any Kubernetes component.

For example, KSPM can detect misconfigurations in a Kubernetes RBAC role definition that grants non-administrators permissions

they should not have, such as the ability to create new Pods. Also, KSPM can find vulnerabilities in all containers that are running in the Kubernetes cluster.

SaaS Security Posture Management (SSPM)

SaaS security posture management (SSPM) is automated and continuous monitoring for misconfigurations of cloud-based SaaS applications such as Slack, Atlassian, Microsoft 365, Google Workspace, GitHub, GitLab, and Okta. It helps organizations minimize risky configurations and detect configuration drifts, and it helps security and IT teams ensure compliance with specific standards.

For example, SSPM can ensure that all your user accounts in the Microsoft 365 SaaS service have multi-factor authentication enabled.

Endpoint Security Posture Management (ESPM)

Endpoint security posture management (ESPM) is an automated security solution that manages the monitoring, identification, alerting, and remediation of compliance risks and misconfigurations in on-premises environments. One of the essential features is continuous monitoring for security gaps on Windows, macOS and Linux clients.

Edge Computing Security Posture Management (ECSPM)

Edge computing security posture management (ECSPM) is an automated security solution that manages the monitoring, identification, alerting, and remediation of compliance risks and misconfigurations in on-premises environments. One of the essential features is continuous monitoring for security policy enforcement gaps for VMware (e.g., vSphere, vCenter, vCloud), Windows, Linux, etc.

Furthermore, the category includes agentless and agent-based vulnerability (CVE) and misconfiguration detection for operating systems, packages, and libraries on virtual machines, containers, serverless functions, appliances, and non-agent workloads.

Network Security Posture Management (NSPM)

Network security posture management (NSPM) is an automated security solution that manages the monitoring, identification, alerting, and remediation of compliance risks and misconfigurations.

Overall, xSPM solutions provide a range of capabilities, including:

- Continuous monitoring of the complete infrastructure stack (from local via CI/CD to production)
- Easy extensibility and customization (through open policy as code)
- Detection of security threats and vulnerabilities
- Detection of configuration drift
- Alerting and notification of security issues
- Remediation of security issues through automated or manual processes
- Compliance reporting and tracking

To achieve the above capabilities, the core of xSPM must be easily extensible with a community-driven approach to connect and collect data from the relevant infrastructure layers. The next step is performing a risk assessment and countermeasures with policy as code (PaC). PaC needs an extensive library of enterprise- and community-generated content that users can easily use and customize according to their needs.

Why is open source tooling necessary for xSPM?

Open source tools are essential to xSPM for different reasons:

- **ACCESSIBILITY:** Open source xSPM tooling is freely available to anyone who wants to use it to continuously monitor the complete infrastructure stack for security and compliance. This means that people worldwide have access to the same tools and technologies regardless of their financial resources. This level of accessibility is fundamental in developing countries, where access to proprietary xSPM tools may be limited or cost prohibitive.
- **COLLABORATION:** Open source xSPM tooling is developed and maintained by a community of volunteers who work together to improve and extend the xSPM core tools. This collaborative approach allows for rapid development and improvement as well as more integrations for the different infrastructure layers (on-prem, different Cloud providers, and new SaaS services), as people from diverse backgrounds can contribute their ideas and expertise.
- **TRANSPARENCY:** With open-source xSPM, the source code is available for anyone to view and inspect. This allows users to understand how the software works and ensure it is secure and reliable. It also allows users to customize and modify the software if they wish.
- **INNOVATION:** Open source xSPM encourages innovation by allowing users to build upon and improve xSPM core tools. This is particularly important in the tech industry, where new ideas and approaches are constantly emerging.
- **COST-EFFECTIVENESS:** Since open source xSPM is freely available, it can be a cost-effective alternative to proprietary software. This can be particularly beneficial for businesses and organizations that have limited budgets or need to use xSPM tools on a large scale.

Open source xSPM plays a vital role in the tech industry and beyond. It promotes accessibility, collaboration, transparency, innovation, and cost-effectiveness, making it essential to the xSPM capabilities at a large scale.

Extensibility and policy as code

Policy as code (PaC) refers to the practice of writing and storing policies in the form of code, usually in a version control system. PaC can render any business logic in code and can be used to enforce architectural standards, corporate policies, regulatory requirements, and more. If organizations combine PaC with infrastructure automation (e.g., Terraform or Ansible), they can directly enforce policies with implicit compliance contracts.

PaC allows security and compliance teams to interface instantly with automation pipelines to ensure conformance. PaC delivers continuous documentation of policies and evidence that they are enforced. Furthermore, an open PaC approach includes that the language in which the policies are written is open source and can be easily extended and used.

There are several reasons why open PaC is vital for xSPM:

1. **AUTOMATION:** Open policy as code allows policies to be enforced automatically rather than relying on manual processes. This helps ensure that policies are consistently applied and reduces the risk of human error.

2. **TRANSPARENCY:** Storing policies in code allows them to be quickly reviewed and audited, which can help increase an organization's transparency and accountability.

3. **ORGANIZATIONS COLLABORATION:** Using version control systems to store policies allows multiple people to collaborate on policy development and review, which can help to ensure that policies are thorough and up to date.

4. **COMMUNITY COLLABORATION:** Sharing the latest security approaches and countermeasures requires cross-enterprise collaboration.

5. **INTEGRATION:** Policy as code can be integrated with other tools and processes, such as continuous integration/continuous delivery (CI/CD) pipelines, to automate policy enforcement at various stages of the development process.

Open policy as code helps organizations manage and enforce their policies more effectively, leading to better security and compliance and improving cost-effectiveness and risk management.

How can xSPM help your organization?

Open xSPM is critical for ensuring security and compliance across the infrastructure stack. By continuously monitoring and managing infrastructure (e.g., on-prem, cloud, Kubernetes) resources, including workloads and containers, xSPM helps organizations protect against security threats, meet regulatory requirements, improve efficiency, and ensure business continuity.

Protecting against security threats

One of the primary benefits of xSPM is the ability to continuously monitor and protect against security threats (including ransomware attacks and other types of malware) in the complete infrastructure. xSPM tools can identify potential security issues, such as vulnerabilities, misconfigurations, or unauthorized access, and alert organizations to take action. By proactively identifying and addressing security issues, organizations can reduce the risk of security breaches and attacks.

Ensure compliance

xSPM is essential for ensuring continuous compliance with relevant regulations and standards such as Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), SOC2, and ISO27001. To operate, many organizations must meet specific security and privacy standards, and xSPM helps ensure that an organization's infrastructure resources comply with these requirements. Furthermore, it can help organizations avoid fines and reputational damage due to non-compliance.

Improve efficiency

xSPM also enhances the efficiency of an organization's operations. By automating the monitoring and management of different resources across the infrastructure stack, open xSPM tools can help organizations save time and resources that would otherwise be spent on manual processes. Additionally, xSPM helps organizations identify and optimize underutilized resources, reducing costs and improving efficiency.

Ensure business continuity

xSPM also helps organizations ensure business continuity in the event of a security breach or other disruption. By continuously monitoring and managing infrastructure resources, open xSPM tools help organizations identify and respond to potential issues before they become significant problems. This can help organizations maintain business operations and minimize downtime.

Overall, xSPM is an essential component of an organization's cybersecurity strategy and is vital for protecting against cyber threats, ensuring compliance, protecting an organization's reputation and brand, and protecting its data and assets.

Learn more about the benefits of xSPM and how you can find vulnerabilities, lost assets, and policy violations in every part of your infrastructure at mondoo.com.

ABOUT MONDOO

Mondoo is a powerful security, compliance, and asset inventory tool that helps businesses identify vulnerabilities, track lost assets, and ensure policy compliance across their entire infrastructure. Our extensible security posture management (xSPM) platform is built on open source components like cnquery and cnspec, giving customers complete transparency and control over how their data is processed. With Mondoo, you can easily integrate security into your developer workflows and protect your organization's assets while minimizing the risk of security incidents.