How Security Consolidation helps Small Cybersecurity Teams

Consolidating cybersecurity solutions helps small teams monitor, manage and protect their internal environment

Introduction

Small security teams are in a constant race to keep up. They have to keep up with daily tasks, manage monitoring, alerts and operations, and that is besides what they have to do when encountering real incidents.

The dynamic nature of cybersecurity, the changes in the threat landscape and the expansion of the attack surface, leads organizations to add more security solutions, from different vendors, creating a layered security infrastructure that introduces new challenges to any team, with a much bigger impact on small ones.

In this white paper, we look at the concept of consolidation of security solutions and discuss why it is becoming the go-to security approach of many CISOs with small teams.

It's a Jungle Out There

While the layered security approach obviously improves a company's security posture, it has also brought a level of chaos into security organizations. With each new solution or vendor comes new deployments and integrations, more cumbersome and time-consuming maintenance, and new skillsets required for smooth operations.

Yet, sophisticated attacks continue to bypass these advanced security layers while FOMO (fear of missing out) compels security teams to evaluate every new solution that comes out. The surge in remote working during 2020 created new opportunities for malicious actors, which only intensified the quest for additional and more advanced security tools. The security environment has become so complex, security gaps are almost unavoidable. Each new solution requires new budget discussions and a re-evaluation of the fragile balance between security and business needs.

This problem is intensified for small security teams with scarce resources. So why do CISOs add more and more security solutions when we already know the abundance of tools creates so many challenges?

Consolidation

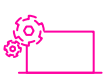
Deploying a single solution that replaces multiple security tools frees up much of your small team's time and reduces your organization's overall workload. Consolidation also better addresses your budget and resources constraints. From facilitating operations and management, through reducing costs to better decision-making and faster time-to-remediation, consolidation done-right is your ultimate choice. However, there are things you cannot compromise on when consolidating cybersecurity tools:

Comprehensive Visibility

The digitization of almost everything has created an attack surface that keeps growing. Visibility is one of the main pillars of cybersecurity. It brings control and peace of mind, but only under certain circumstances.

The security solutions that build your layered security infrastructure may provide visibility to parts of your internal environment, yet often this visibility is fragmented, lacks context and misses the big picture.

To ensure you always have complete visibility of your internal attack surface, consider adopting a solution that consolidates multiple common tools for securing the internal environment. Such a solution will provide the required visibility across all primary prevention and detection components and add context-based inputs to even stealthy attacks are detected.



Technological Capabilities

Looking at how organizations protect their internal environment reveals a multitude of tools, each providing a different capability to keep assets secure. In some cases, you have overlapping capabilities, which means you are wasting resources.

A single solution that consolidates multiple capabilities that are currently provided by various tools from different vendors enables you to optimize your resources.

To provide your small team with the best consolidated security solution for protecting your internal environment, look for all of the following technological capabilities in a single platform:

NGAV

(Next Generation AntiVirus) for basic endpoint malware prevention.

EDR

(Endpoint Detection and Response) for more advanced endpoint threat prevention, detection and response.

NTA/NDR

(Network Traffic Analysis/Network Detection and Response) for detection of malicious activity, such as lateral movement, on your network.

UEBA

(User and Entity Behavior Analytics) for detecting anomalous or malicious user behaviors.

Deception Technology

for exposing attackers that have bypassed your security controls by making them access fake assets.

The Essentials For Consolidating Your Internal Environment Security

When exploring consolidated solutions for protecting your internal environment, whether you are looking to replace existing solutions or building out your infrastructure, be sure they include the following “must-haves.”

IR inside

Once you discover a threat, shortening the time to respond should be one of your main goals. A consolidated solution that uncovers, prioritizes and lets you respond to all threats in a single pane of glass will greatly improve your small team’s efficiency and time to response.

Automation of investigation and remidation processes

A consolidated solution can bring all your threat alerts to a single platform and automatically prioritize them based on the risk they pose to your critical assets. Automating as many policies and investigation workflows as possible will facilitate the response and remove much of the manual work from your analysts’ workload.

Extensive coverage for enhanced resilience

To ensure successful, efficient and timely incident response, you need to ensure your remediation covers your entire internal environment and includes remediation actions for each entity type, including file, host, network and user. Only a solution that extends the response across the environment will enhance your overall cybersecurity resilience.

Out-of-the-box remediation tools and playbooks

Pre-built remediation tools and playbooks enable your small team to do more with less, accelerate the remediation process, and shorten the time to response. A consolidated solution that includes out-of-the-box automated tools and playbooks, including customized ones, will augment your team’s capabilities and reduce their manual efforts.

Automation and simplicity

When combining multiple capabilities into a single solution, automation and simplicity are key for successful implementation and operation. From prevention actions, through accurate detection and prioritization of threats, to investigation workflows and remediation, everything should be automated. This will not only save time and resources, but also leverage your team’s existing skills and facilitate adhering to compliance requirements.

In addition, pay attention to the simplicity of the solution as your team will truly benefit from a consolidated solution that enables them to manage, monitor, investigate and act from a single pane of glass, to fully protect your internal environment.

MDR inclusive

Having access to a Managed Detection and Response (MDR) team’s domain expertise and deep understanding of the threat actor landscape, and high-end research tools and capabilities, brings your small team to the forefront of cybersecurity. The most important things to look for from an MDR provider include:

- 24X7 proactive monitoring of the organization’s environment
- Real-time augmentation of detection mechanisms
- Management of events, alerts, customers inquiries and incidents
- Alert analysis and correlation to other alerts in the system
- Proactive outreach for response collaboration
- Proactive threat intelligence and threat hunting
- File analysis and attack investigation
- Remediation guidance and customized playbooks
- Domain expert support for ongoing inquiries and assistance
- Research reports

Note that the costs can substantially vary from one MDR service provider to another and in some cases, the technology solution provider will provide these services for a small fee or with no additional charge at all.

Summary

Finding a single solution that consolidates all the essentials mentioned above in order to keep your internal environment secure should always cover more than one aspect of your security needs. It should also facilitate your team's operational needs, leverage their skills and optimize their resource allocation.

About Cynet

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.

Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.

LEARN MORE