Check Point®
SOFTWARE TECHNOLOGIES LTD

IT'S TIME TO RETHINK SECURITY MANAGEMENT

A Resource for the Security Professional

ONE
STEP
AHEAD

TABLE OF CONTENTS

IT'S TIME TO RETHINK SECURITY MANAGEMENT

03 **INTRODUCTION**

05 **START SOLVING REAL PROBLEMS**

- 06 THE DANGERS OF SILOS
- 06 THE QUEST TO MANAGE SECURITY COMPLEXITY
- 06 DYNAMIC CLOUD ENVIRONMENTS
- 07 OPERATIONAL DEFICITS
- 07 INADEQUATE SECURITY MONITORING

08 **THE SECRET TO STRONG SECURITY MANAGEMENT**

- 09 CONQUER WITH CONSOLIDATION
- 09 UNIFIED POLICY MANAGEMENT
- 09 INTEGRATED THREAT MANAGEMENT
- 10 AUTOMATED OPERATIONS

11 **CONCLUSION**

01 INTRODUCTION

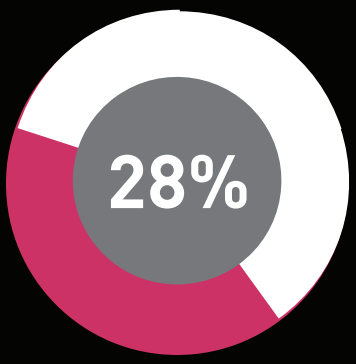
This is an amazing time in history. The advancements in technology, the proliferation of inter-connected devices and an interdependent digital global economy have fueled countless improvements. New developments in technology, processes, and connected machines are changing everything – from how we work, how we bank, how we communicate, how we live and how we secure our environments. These advancements, while giving us many opportunities, have pushed the cybersecurity industry through rapid transformation. The very emergence of this new cyber realm, as much innovation as it has given us, has also evolved into a place to house dangerous unknowns. The unfortunate reality is that the industry hasn't managed to keep pace. As many of us continue to witness, the attack surface is complex and growing, and the threat vectors and defenses are proving difficult to manage.

To be as effective as possible, threat defenses need to be observed and managed in real-time to give as much time to respond as possible. Robust security management is a solution that includes the installation of high-tech systems designed to protect an organization's data, networks and devices, while providing real-time visibility into security risk. This includes the development, documentation, and implementation of policies and procedures for protecting these assets.

Unfortunately, the response to potential threats tends to be point product solutions or the reactive construction of new policies and rules, which only serve as a Band-Aid, at best. This is largely because a unified security program – based on integrated technology – is often not being used.

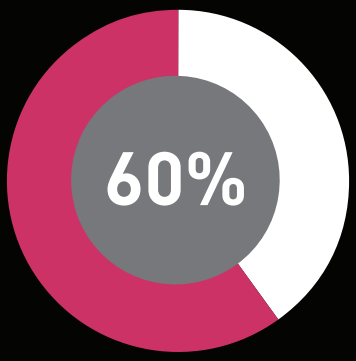
This paper invites you to rethink your current security posture, and enable strong protections for the organization. Everything from technology, people, policy, operations and management must be considered in a new light, with a fresh mindset.

Your security is only as strong as your ability to manage it.



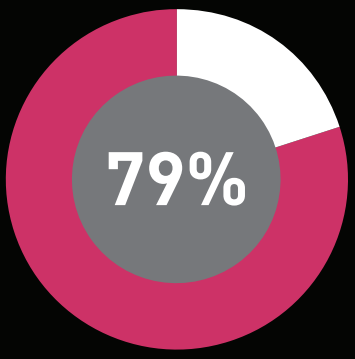
28% of organizations say they are challenged by too many overlapping controls, and processes tend to cause trouble.

- ESG



By 2017, 60% of enterprise private cloud deployments will automate the provisioning of information security controls.

- Gartner



79% of information security professionals working at enterprise organizations believe network security has become more difficult over the past two years.

- ESG

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete"

- R. BUCKMINSTER FULLER

02

START SOLVING REAL PROBLEMS

The security industry does not need more point products to duct-tape solutions together and hope for the best. Companies need real solutions – ones that can integrate their system and give them visibility into the security risk of the environment. A powerful security platform gives your company a strategic and tactical advantage by enabling the management of potential threats, without inhibiting business innovation.

THE DANGER OF SILOS

Some security vendors have multiple management platforms and consoles that are complicated and difficult to maintain and manage. Those kinds of solutions are usually operating with different platforms and multiple consoles, each one with different policies and configurations. In addition to the overlapping and redundant tasks for security administrators, multiple management platforms multiply the effort needed to protect the business - and can also put the organization at higher risk.

Security solutions are often not fully integrated within change management processes. This leads to outages and unnecessary complexity. According to the Ponemon Institute's 2015 Global Cost of Data Breach Study, "malicious attacks can take an average of 256 days to identify, while data breaches caused by human error take an average of 158 days to identify." This is directly related to the lack of integration. If your company has several different security platforms in use at the same time, that most likely are not built to integrate with each other, then finding a potential breach becomes that much more difficult. This is the primary reason why it can take months to find the source of a data breach.

MANAGING SECURITY COMPLEXITY

The basics of network security have evolved. It wasn't that long ago that network security consisted of a handful of autonomous components that performed basic and completely separate tasks. Network architects had to be careful not to over-secure networks as device design often had to compensate for single points of failure and bottlenecks.

Fast forward to now; security has evolved to include several moving parts. Everything from different types of traffic, log events from multiple devices, partner and vendor ecosystems, segmented networks and multiple branches, to centralized security alerts and compliance, are all part of the ongoing environment of security. It's not only vast, but also complex.

DYNAMIC CLOUD ENVIRONMENTS

According to Gartner, by 2017 (just one year away), *60% of enterprise private cloud deployments will automate the provisioning of information security controls.* With dynamic clouds, there is virtually no physical barrier for a business to scale its cloud-based business to meet customer needs as fast as the market demands.

Dynamic clouds allow for software and services to grow with your business. They enable extreme agility. Typically that includes automatically adjusting itself to correct for changes in demand or workloads. Servers are able to exist only for hours or minutes, as they can be automatically provisioned, configured and de-commissioned without human interaction. Cloud computing also allows anyone with network access and credentials to manage the entire infrastructure, including platforms and applications.

While this may be an enormous opportunity for businesses, it also brings tremendous risk. Typically, security that is installed on the perimeter, or that requires human checks, simply cannot keep up. Lack of proper segmentation makes it easier for malicious actors to access systems via lateral movement in the environment, and this has played a role in several high-profile security breaches.

As most organizations have heterogeneous environments, security management should centrally manage both physical and virtual networks. It's imperative that security be automated and embedded into the cloud infrastructure.

OPERATIONAL DEFICITS

With the dearth in experienced security professionals, throwing more people at the problem is not an option. Even if that were an option, security processes that are mostly manual in nature and labor-intensive will result in an increase in configuration errors as systems become more dynamic. A dynamic, fast-growing environment also creates blind spots that impact security effectiveness.

Security managers can evaluate tasks and workflows to identify those tasks that would most impact a team's ability to respond quickly to a security event to prevent an attack. These tasks, which could include security architecture planning, threat impact analysis and breach investigation, should be priorities for the security team. If not, they end up reactively dealing with routine tasks such as patch management, asset inventory, ticketing and resolving issues, and access rights management. These tasks are extremely time-consuming, so an assessment of workflow bottlenecks and process efficiencies would be helpful in identifying the tasks that can be either automated or delegated.

INADEQUATE SECURITY MONITORING

ESG reported that "roughly 40% of enterprise organizations claim their security staff is so busy dealing with emergency responses that they have little time for cybersecurity training, planning or strategy". This is an unfortunate reality in many organizations, and this is exactly the reason why a robust security management platform can help.

Knowing which activities and systems to monitor, and when, is key to filtering and locating the needle in the haystack of event data that could be the cause of a security breach. Being able to monitor and collect security events across disparate systems is just half the challenge. The ability to find connections between seemingly unrelated events is critical. In order to do this, correlation rules need to be built in order to monitor security status and identify traffic pattern anomalies.

Ideally, we want to address problems faster and more completely. A visual dashboard provides full visibility into security across the network, helping you monitor the status of your enforcement points and stay alert to potential threats. Fully customizable dashboards allow you to focus only on what matters to you. You receive a comprehensive view of your security posture, and can quickly drill down into incident or log details with a few clicks. Reports must be easily accessed and tailored for stakeholders and accessible from any web browser.

> *GARTNER SEES MANY ENTERPRISES THAT ADD SECURITY TOOLS BUT FAIL TO MONITOR AND MANAGE THE EVENTS THEY GENERATE. MANY ORGANIZATIONS CONSIDER SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) AS A SILVER BULLET, BUT SIEM OFTEN IS UNDERMANAGED AND/OR UNDERUTILIZED IN MANY ENTERPRISES.**

* *Avoid These "Dirty Dozen" Network Security Worst Practices. Published: January 8, 2015, Gartner, Inc.*

03

THE SECRET TO STRONG SECURITY

Perhaps one of the biggest challenges for leaders who manage cybersecurity initiatives is staying focused on the bigger picture, rather than the end result. Management must align the company's resources with the organization's security strategy to reduce risk and potential damage from attacks. This includes developing a culture where critical people are acutely aware of security policies and how to protect high-value company assets.

As awareness of data breaches continues to grow, the enterprise seeks proactive solutions to move ahead of hackers and cyber criminals. How can we address the cyber skills gap to ensure a more even battleground against increasingly sophisticated adversaries? Look at how to be proactive through consolidated security management, which lessens the probability of a breach.

CONQUER WITH CONSOLIDATION

In this case, rethinking security management means thinking beyond the current bounds of industry norms and seeing the challenges from a multi-dimensional point of view. Security complexity can be conquered through consolidation – bringing all security protections and functions under one umbrella. By consolidating security on a single platform, companies gain more control over their security, get better insight into their security posture, and can respond more quickly to shut down threats to their entire environment.

Simply put, security consolidation leads to stronger security. Having a unified security management platform for enterprises to consolidate all aspects of their security will help organizational efficiency and keep your teams adept at deploying strong protections across the company.

UNIFIED POLICY MANAGEMENT

Typically, security administrators must always consider what is already in place and see if there are current policies that need to evolve or be removed before you add on more layers or policies. Unified policies give your organization a different approach.

Ultimately, when policies are misconfigured, the organization is not able to protect and gain visibility into the increasing number of business segments. This puts the entire organization at risk. The key to a strong security architecture that can overcome the most difficult cyber security challenges can only be delivered by using a security management solution that delivers unparalleled operational efficiency.

Think of it like this:

In attempts to defend the network and critical assets from cyber threats, the industry has fallen into the trap of duct-taping policies together. We're partially to blame for the complexity we experience. Between point products, human errors and policy misconfigurations (among other problems), gaps in security visibility have increased substantially. It is absolutely critical to be able to view all security policies across all devices and vendors – from an integrated console - so you can understand where your vulnerabilities exist.

Having unified policy capabilities makes it possible to manage access control and threat prevention. With that said, you need to be able to easily segment policies to accommodate complex environments. For example, the Help Desk team can be empowered to add users, hosts and applications to be secured. Taken a step further, a direct integration of the security management platform with the ticketing system would streamline this process.

This ability to delegate routine tasks to non-security teams or security partners will free up the security team to focus on tasks that require more security expertise. Security would then become an enabler, and not an inhibitor, of business innovation.

INTEGRATED THREAT MANAGEMENT

The Oxford Dictionary defines visibility as ''the state of being able to see or be seen.'' If we apply this definition to cybersecurity, and security management in particular, we can define security visibility as the ability to deliver an unobstructed view into the operation of security controls, making the pertinent information easy to see and, therefore, manage.

When we talk about full-spectrum visibility, we're essentially talking about having a complete picture of your company's security posture. The most effective threat management will have an integrated, advanced visual dashboard, show how devices are configured, any attack in process or about to happen, noncompliance with policy and any other associated risk.

You cannot monitor or protect devices you don't know about. Security challenges are increased when there is a lack of proper visibility for incident detection and response. The most often cited challenges include the struggle to capture network behavior for incident detection (38%), monitoring network flows for anomalous behavior (35%), the ability to capture and analyze logs from network and security devices (29%), and the ability to establish a baseline of normal network behavior (27%).

This is precisely the reason why a single, visual dashboard is so important for event analysis, and threat monitoring and mitigation, to ensure full-spectrum visibility into threats across the entire perimeter and beyond. Risk managers must have technology in place that enables them to look at high-level alerts, drill down into the specifics and analyze correlated data from all security tools and sensors in the network.

AUTOMATED OPERATIONS

While it's true that security managers have toyed with automation in the past, with less than stellar results, today there is a better solution. Now there is much better control over the automation of workflows and tasks with the latest generation of security management platforms on the market. Lack of control presents a barrier to more automation and integration.

By automating operations, security teams have the confidence to integrate ticketing, network management or cloud orchestration systems, knowing that they can limit exactly what integrated systems have access to and what they are capable of doing. This capability to integrate securely is particularly relevant in cloud and outsourced environments. Security can be embedded into cloud orchestration platforms to automatically secure virtual machines as they are provisioned. On the flip side, if a virtual machine is infected, it can be quarantined immediately.

Cybersecurity is not only about stopping threats but about enabling a secure business process. Policy misconfiguration or inability to protect and gain visibility to the increasing number of business segments can put the entire organization at risk.

Therefore, a good security solution should be measured by its management capabilities. The key to a strong security architecture which can overcome today's cybersecurity challenges can be delivered using a manageable security solution which can deliver operational efficiency.

INTEGRATION IS KEY.

"WE ARE CALLED TO BE ARCHITECTS OF THE FUTURE, NOT ITS VICTIMS."

- R. BUCKMINSTER FULLER

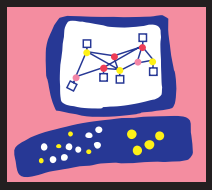
Reality has struck as CISOs manage expanding networks and increasing complexity, while being constantly vigilant in breached eras. Forward-thinking security executives balance technical and business requirements while battling continuously evolving and adapting adversaries. It's no longer an option to be purely defensive in protecting the environment; security executives must implement proactive measures and engage in collaborative efforts.

The bottom line is that you must provide strong protection efficiently without impeding business innovation. How do you accomplish this? You need intelligent technology that keeps up with the threat landscape – technology that can detect and block both known and unknown threats, as well as comply with regulations and give you complete visibility into the security operations of your company.

As evasion techniques evolve and get smarter, so must the technology to keep your business secure. A robust security management platform allows your company to be proactive in its approach to security, rather than reactive. When you are constantly reacting to problems after they occur, rather than preventing them, it wastes time, energy, and money that your company may not have to spend.

THE KEY IS TO OPTIMIZE SECURITY.

Our recommendation is to have a consolidated security management platform that provides a single view into all security configurations, and delivers comprehensive visibility into all network traffic, applications, events and threats. It's also important to be able to customize the security management for your specific needs. This can be achieved with a secure, trusted API architecture, allowing for web and command-line management. These features create a truly consolidated security management solution with high operational efficiency, risk visibility and delegated security.



Check Point®
SOFTWARE TECHNOLOGIES LTD

ONE STEP AHEAD

To learn more about Check Point's Solutions for Security Management, please visit www.checkpoint.com/management

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

March 2016