

Cyber Talk



2021 BUYER'S GUIDE TO  
**CYBER SECURITY**

Sponsored by Cyber Talk

# Navigating a Post-Pandemic Era Requires a Deep Understanding of Preventing Advanced Threats

## Introduction

For the world's security professionals, the 2020 COVID-19 outbreak amplified what many already knew about cyber threats — they've reached pandemic stage. Targeted Advanced Persistent Threats (APTs) have grown in sophistication and in their ability to accelerate data loss and damage on-premise and cloud infrastructures. Shifting remote workforces safely surfaced as a serious security challenge. Vast numbers of employees were suddenly confined to home offices with the ability to access corporate networks and cloud applications from anywhere and everywhere. Microsoft has reported an almost 775 percent increase in the usage of cloud services due to the pandemic.<sup>1</sup>

It is also important to realize that organizations operate in a hybrid way with full-functioning physical and cloud data centers, and the advent of expanded remote access, presenting huge management challenges.

Even before the pandemic lockdown, the zero trust architecture model and its ability to grant least privileges for application access surfaced as a guidepost. In 2020, zero trust took on even greater importance for security professionals to boost cyber security protections.

It's clear to security professionals that stronger preventative security is needed, and essential as organizations revise their strategies to protect anything and everything everywhere.

This is the new cyber security normal that organizations will face in 2021 and beyond.

---

<sup>1</sup> "Why Security Misconfiguration Are Higher During COVID-19," by FireMon, Security Blvd., May 11, 2020  
<https://securityboulevard.com/2020/05/why-security-misconfiguration-are-higher-during-covid-19/>



# SolarWinds Supply Chain Attack

In December of 2020, organizations were shaken by the SolarWinds supply chain attack, a major international cyber attack. Shockingly, it was determined that the threat didn't materialize overnight, but it had been lurking in systems for nearly a year and a half.

The organized cybercrime group responsible for the hack demonstrated a sophisticated knowledge of software idiosyncrasies and the software development lifecycle. Their level of understanding enabled them to evade detection. The hackers also deliberately impersonated employees who were working remotely, and operated in the same city as employees in order to disguise their initiatives.<sup>2</sup>

The attackers exploited a software supply chain, ultimately affecting more than 18,000 organizations worldwide.<sup>3</sup> Affected groups included both US federal agencies and private sector organizations.



---

<sup>2</sup> <https://www.cybertalk.org/your-solarwinds-and-supply-chain-attack-questions-answered/>

<sup>3</sup> <https://www.cybertalk.org/2021/02/15/solarwinds-it-isnt-over-yet-and-these-details-are-disconcerting/>

# Attack on Microsoft Exchange Servers

In March of 2021, Microsoft announced updates on behalf of four different zero-day vulnerabilities. Although researchers first discovered the vulnerabilities in early January of 2021, hackers may have known about these vulnerabilities for years. As a result, cyber criminals devised expansive schemes to cash in on the zero-days.

As media reports emerged, the magnitude of the hackers' endeavors grew readily apparent. As many as 250,000 may incur damage or disruption due to attacks on Microsoft Exchange Servers.<sup>4</sup>

When organizations identify attack opportunities early, they can often save themselves and their clients from serious subterfuge and sabotage. It's evident that such calculated cybercrimes are being executed by well-funded, often state-backed hacker groups, and that the attacks are more sophisticated and elusive than standard malware or ransomware attacks.

In addition to the proliferation of APTs, the multi-vector attacks and polymorphic nature of modern cyber attacks also differentiates them from those of years past.

## A QUICK HISTORY LESSON

- Cyber threats first developed in the 1980s, with the mass availability of personal computers.
- These were followed by attacks in the 1990's that precipitated the development of the network firewall.
- In the early 2000s, we saw attackers leveraging a wider array of vulnerabilities, and by the early 2010s hackers had developed sophisticated maneuvers, such as APTs, and the proliferation of targeted ransomware attacks.

---

<sup>4</sup> <https://www.cybertalk.org/2021/03/12/hacks-doubling-every-two-hours-microsoft-exchange-servers-still-under-attack/>

# Securing Vulnerable Organizations Against Advanced and Sophisticated Threats

In 2021, advanced cyber attacks occurred across public and private sectors; from manufacturing to telecommunications to healthcare to the financial sector. The public sector, in order to keep operating daily, has had to continually play defense against cyber attackers. Some private enterprises have had to shutter their doors after experiencing a cyber attack. This has been yet one more reason adding to a socially and financially devastating year. Much like a COVID-19 vaccine has introduced a preventative defense against contagion, so does the cyber world require such solutions.

As organizations of all kinds deploy IoT (Internet of things) technologies, and stay connected via smartphones, the dangers only multiply. These days, an attack that begins within a smartphone can go through an organization's cloud, and can end up shutting down the data center. The cloud, autonomous cars, and millions of connected IoT devices require a scalable and well-rounded approach to security.

Security experts advise organizations, especially the most vulnerable ones, to think about cyber breaches not in terms of 'if', but in terms of 'when'.

To that effect, understanding the core elements required for top-tier cyber security is a must. Applying innovative digital defense is mission-critical for the survival of any modern organization. Dig into the Cyber Talk Buyer's Guide to scope out key considerations when it comes to improving your cyber security architecture.

This buyer's guide provides in-depth strategies that can help you realize new goals and that can assist in enhancing your organization's security posture.

## DID YOU KNOW?

- **More than 90% of organizations are using outdated cyber security tools.<sup>5</sup>**
- **77% of security professionals anticipate a significant breach in the near future.<sup>6</sup>**
- **By 2021, cyber damages will total more than \$6 trillion, worldwide.<sup>7</sup>**
- **Through 2022, 95% of breaches will likely occur as a result of customer misconfigurations, or other human errors.**
- **42% of storage objects evaluated with recorded data loss prevention incidents were misconfigured.<sup>8</sup>**

<sup>5</sup> InfoSec Newsflash, Cyber Security Statistics for 2019, Cyber Defense Magazine, March 21, 2019  
<https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019>

<sup>6</sup> Jaikumar Vijayan, 31 cybersecurity stats that matter, TechBeacon, September 30, 2019  
<https://techbeacon.com/security/31-cybersecurity-stats-matter>

<sup>7</sup> Matt Powell, 11 Eye Opening Cyber Security Statistics for 2019, CPO Magazine, June 25, 2019  
<https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019>

<sup>8</sup> Charlie Osborne for Zero Day, 99 percent of all misconfigurations in the public cloud go unreported, ZD Net, September 24, 2019  
<https://www.zdnet.com/article/99-percent-of-all-misconfiguration-in-the-public-cloud-go-unreported>

# 10 Most Important Considerations in Choosing Your Cyber Security



1 REAL-TIME PREVENTION



2 IDENTIFICATION



3 INSPECTION WITHIN SSL/TLS



4 GOING BEYOND SIGNATURE-BASED DEFENSES



5 PROTECTION FROM EVERY DIRECTION



6 A ZERO TRUST APPROACH



7 SHARED THREAT INTELLIGENCE



8 CONTROL THE CLOUD



9 UNIFIED MANAGEMENT CONFIGURATION



10 SECURITY FROM THE START

Read on for an in-depth discussion of each component.  
To get started, we'll take a look at a few key concepts.

## UNIFIED AND EFFICIENT SECURITY



Having unified management control across all networks, clouds, mobile, and endpoint environments increases operational efficiency and reduces complexity. Unified security can cut operations time by as much as 80%. It scales easily, and also offers the highest caliber of prevention. Unified management is an important feature as you build your next-generation security architecture.

## NETWORK



When thinking about network security, you'll want to know which applications your users are running within your network, and then you'll want comprehensive visibility, combined with flexible enforcement points around applications. Gaining insights into and taking control of what your users are doing can help you secure your network.



## SHARED INTELLIGENCE

Threat intelligence is known as one of the most proactive and effective security solutions available. Threat intelligence products that gather information from expert feeds, enriched by research from expansive security research teams, enable automated remediation processes, reducing manual operations for your team. The reliable real-time data can also help you make the right decisions in the face of threats. In this buyer's guide, learn why embedded threat intelligence is an important feature of your security architecture.



## MOBILE

Nearly every enterprise allows employees to bring their mobile devices (BYOD) and to use them in conjunction with company resources. As a result, organizations deploy safeguards that protect business data, provide secure mobile access to business documents, and that keep mobile devices safe from threats. Obtaining security that can protect a wide range of mobile devices is essential.

---

By keeping all of these concepts in mind, you'll develop a robust security architecture to defend against today's threats, and tomorrow's.

---



## CLOUD

The cloud has become an integral piece of architecture within many organizations. When it comes to cloud security, the shared responsibility model means that the onus falls on the administrator to secure the data, not the public cloud vendors (contrary to some perceptions). This can present a major challenge for organizations, and some try to skimp on cloud security measures. However, robust cloud security can assist in reducing costs, and enhancing reliability. This guide can show you the additional advantages of investing in more comprehensive cloud security.



## ENDPOINT

You'll want endpoint security that can be managed centrally using a single management console, as this allows for simple and flexible administration, and increased security. In addition, non-traditional endpoints mean that you need security that can keep up. The buyer's guide can help you identify the right endpoint security for your organization.

---

Check Point responds 10X faster to vulnerabilities than Palo Alto Networks.

---

## 1 Prevent in Real-Time

A cyber attack can shake the foundations of an organization, negatively impacting the entire business. Avoid attacks before they can take root. Get security that's designed to prevent, not just to detect.

Your prevention platform should include cutting-edge technologies, like behavioral detection and machine learning algorithms that can identify and block exploits on networks, cloud, and endpoint, before they execute and infiltrate your network. The ability to prevent patient-zero, so to speak, is critical. Get a real-time prevention platform with rapid responses to new vulnerabilities and a high malware catch-rate. As a starting point in developing a shortlist of vendors to work with, look for vendors with NSS Labs recommendations.

The payoffs of investing in prevention are profound. Applying cyber security prevention can streamline protections across your system (networks, cloud, endpoint, mobile, and IoT), improve efficiency and reduce your costs.

Prepare your organization for the new normal post-coronavirus. Be bold. Think prevention first.

Here are the top three areas to pay attention to when it comes to prevention:

### PREVENT THREATS IN YOUR REMOTE ECOSYSTEM: SECURE REMOTE ACCESS:

In the era of hyper-distributed working environments, ensure that your remote ecosystem is secure. Organizations commonly expect employees, contractors, business partners and vendors to rely on technologies to perform work remotely. All parties are liable to use both organization-owned and bring your own device (BYOD) access points. Security concerns include the lack of physical security controls, reliance on unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.<sup>9</sup> You'll want to take a comprehensive approach to securing users and their access. You need to accurately gauge user permissions so they are not excessive, such as with cloud applications. This offers protection should a user be compromised and with the least amount of privileged access, the spread of a breach can be minimized. To protect all users, and to protect the heart of a business, organizations should opt for the highest security levels possible when it comes to the distributed workforce.

---

Fact: Check Point offers better real-time prevention than Palo Alto Networks.

---

<sup>9</sup> <https://www.checkpoint.com/cyber-hub/network-security/what-is-remote-secure-access-vpn/covid-19-and-secure-remote-access-best-practices/>



## PREVENT THREATS IN THE CLOUD:

A prevention-focused security approach should also offer comprehensive protection for cloud environments. Research shows that organizations depend on an average of 3.4 public clouds and 3.9 private clouds.

Cloud workloads are critical. Disruption to their operations can lead to widespread organizational fallout. Agile protections for the cloud are must-haves. Unlike in a previous era, cloud posture management, serverless security and firewalls powered by contextual AI can now be deployed easily and efficiently. Don't compromise on cloud security.

## PREVENT THREATS TO THE PERIMETER AND THE DATACENTER:

Prevent known and unknown attacks. In obtaining resilient enterprise network security, opt for streamlined management that can provide IoT nano-security to terabit super networks. In other words, obtain the highest levels of performance and security possible for your environments. Doing so will help you prevent fifth generation cyber attacks. It's time to step up your security. Eliminate patchwork infrastructures with high TCO. Turn to comprehensive architecture.

---

Proven: Check Point offers 2.5X better security with risky apps than Palo Alto Networks.

---

2



## Identifying Users, Applications, and Devices From All Sources

You need a solution that gives you full visibility into who's on your system, what they're doing and where they're going, no matter whether the activity is on your networks, cloud, mobile, endpoints, or IoT devices.

Receive accurate, real-time information about who's browsing through your resources. An IP address isn't good enough. Find out the precise identity of each user who's accessing your organization's assets.

Obtain up-to-the-minute information about what's on your system. Your mission-critical applications (and data) are perpetually at risk. An alarming 37 percent of security risks occur within the application layer, with SQL injections (SQLI) and cross-site scripting (XSS), comprising more than 15 percent of these events.<sup>10</sup> The race to build and deploy quickly can mean that application layer vulnerabilities go unnoticed. And within the applications and data sets, where is the information going?

Get a security solution that offers comprehensive visibility and granular insights so that you can act quickly, and protect your critical infrastructure.

---

<sup>10</sup> Hamsa Srinivasan, What's the Best Strategy to Manage Application Security Risk, Security Intelligence, July 6, 2018  
<https://securityintelligence.com/whats-the-best-strategy-to-manage-application-security-risk>

## 3 Uncover Attacks Hiding Within Encrypted Traffic (Inspect Within SSL/TLS)

Organizations that apply SSL/TLS, ensure that a third-party cannot sit between the server and the browser to read or manipulate electronically transmitted information. Any bad actors will only see a garbled mess of alphanumeric text.

Research indicates that only 3.5% of organizations decrypt their network traffic in order to fully inspect it.<sup>11</sup> Reluctance to inspect often comes from concerns about reduced firewall performance, loss of privacy, and creating a sub-par end-user experience, among other factors.<sup>12</sup> In addition, if SSL/TLS interception is executed poorly, the initiative can do more harm than good.<sup>13</sup> However, when executed well, SSL/TLS inspection can significantly improve security.

From 2016 through the present, the percentage of websites protected with the SSL/TLS protocol, as executed through HTTPS, has increased from 40% to over 80%.<sup>14</sup> HTTPS can protect users against man-in-the-middle (MitM) attacks, malicious content, and more. It stops credit card and identity theft. Without it, you're blind to a large portion of your company's traffic.

Google now uses HTTPS as a search ranking signal. This means that investing in SSL/TLS will not only improve your security, it will also improve your organization's SEO, making you more competitive within your marketplace.<sup>15</sup> These days, browser makers are doing all but demanding that websites apply HTTPS before displaying pages to web-users, and pressure from the general public is also mounting.

A lock icon on your site may be tiny, but the protection that it affords and trust that it generates could be huge.

## 4 Threats Can Get Past Signature-Based Defenses: Here's What to Do

Signature-based defenses have been an organizational go-to since the early 2000s.

However, the strength of a security system can no longer be measured by the number of malware signatures included in a vendors' library of threats. Anti-virus and intrusion prevention products are only updated with "known" attacks, and fail to protect organizations from threats that exploit signature-based defenses by new variants and/or zero day attacks.

---

<sup>11, 12</sup> Zeljka Zorz, What is flowing through your enterprise network, Help Net Security, February 20, 2020  
<https://www.helpnetsecurity.com/2020/02/20/firewall-tls-inspection>

<sup>13</sup> Lucian Constantin from IDG News Service, It's time to turn on HTTPS: The benefits are well worth the effort, Computer World, March 14, 2017  
<https://www.computerworld.com/article/3180690/its-time-to-turn-on-https-the-benefits-are-well-worth-the-effort.html>

<sup>14</sup> Nicole Casal Moore, How Let's Encrypt doubled the internet's percentage of secure websites in four years, Michigan News, November 13, 2019  
<https://news.umich.edu/how-lets-encrypt-doubled-the-internets-percentage-of-secure-websites-in-four-years>

<sup>15</sup> Lucian Constantin from IDG News Service, It's time to turn on HTTPS: The benefits are well worth the effort, Computer World, March 14, 2017  
<https://www.computerworld.com/article/3180690/its-time-to-turn-on-https-the-benefits-are-well-worth-the-effort.html>

Organizations must step up to the plate with measures to protect themselves from unknown threats. Cyber security platforms that can protect all vectors, including cloud, mobile, network, and IoT, are your best bet. Invest in a platform that offers:



Sandboxing (static, dynamic, and behavioral analysis)



CDR (content disarm and reconstruction), hence, sanitizing documents



Artificial intelligence/  
machine learning



Threat cloud

---

All of these components can help you stay ahead of the hackers.

---

## 5 Threats Can Come From All Directions: Protect Everywhere

Locking down everything is critical. The only way to ensure that your network is secure is by ensuring that everything connected to it is secure. Secure your individual computers, phones, tablets, and other extensions of your network.

An ever-growing number of hackers are capitalizing on these vulnerabilities because organizations often lack sophisticated tools to protect against advanced threats.

Whether your organizations' data is at rest or in motion via the cloud or on mobile devices, be sure that you have proactive protection designed for everywhere; from traditional data centers to the hyper-distributed environment.

Comprehensive protection is critical. In its absence, points of failure can go unnoticed, leading to major breaches.

For example, in briefly returning to the aforementioned Sunburst supply chain event, SolarWinds lacked security safeguards across developer build environments. As a result, the company represented a prime target for hackers. This security oversight could potentially have been avoided through the implementation of comprehensive security architecture.

To reduce the cost and complexity associated with adoption of a comprehensive, consolidated security solution, consider Security Access at the Service Edge (SASE) solutions. While SASE just began to take off in early 2020, it gained additional significance with COVID-19 with the need to protect users and applications, mobile devices, and endpoints from any location. By 2024, adoption rates for SASE solutions may well surpass forty percent.<sup>16</sup> SASE is unified security that can complement your organization's computing culture.

---

<sup>16</sup> "Emerging Technology Analysis: SASE Poised to Cause Evolution of Network Security," By Nat Smith et. Al. Gartner, October 22, 2019 <https://www.gartner.com/en/documents/3970571/emerging-technology-analysis-sase-poised-to-cause-evolut>

Proven: Check Point offers 12X fewer vulnerabilities when compared with competitors.

## NSA Top 25 Vulnerabilities

In October of 2020, the US National Security Agency released a cyber security advisory concerning specific nation-state sponsored activities. The advisory describes 25 unique, publicly known vulnerabilities that have been operationalized in cybercriminal exploits. Cyber security researchers found that these CVEs were 7x more likely to be exploited than any other vulnerabilities in 2020. The cyber criminals behind the attacks have targeted victims across 161 countries and across a variety of industries.

The impact of such attacks has been severe. For example, depending on the precise vulnerability exploited, the cyber criminals can potentially take control of a business network. When this occurs, the criminals can manipulate users' emails and network traffic, disable services and harvest users' credentials. They can also potentially delete files or manipulate sensitive data.

In seeking a security provider, see to it that the selected vendor has the capacity to protect your organization from the exploitation of all 25 reported vulnerabilities. Check Point's capabilities have scored highest in this arena when compared to other vendors.

Fact: Check Point protects against more of NSA's Top Vulnerabilities than Cisco Security.

### DID YOU KNOW?

- More than 90% of organizations rely on outdated cyber security tools.<sup>17</sup>
- In 2020, more than 155 million people were affected by a data breach and lost personal information.<sup>18</sup>
- For a business in the US, the average cost of cyber attack could be as much as \$8.64 million.<sup>19</sup>
- By 2025, cybercrime may cost the world over \$10 trillion annually.<sup>20</sup>

<sup>17</sup> <https://www.cybertalk.org/2020/12/03/2021-cyber-security-the-data-loss-that-you-can-prevent/>

<sup>18</sup> <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

<sup>19</sup> <https://www.thesslstore.com/blog/password-security-what-your-organization-needs-to-know/>

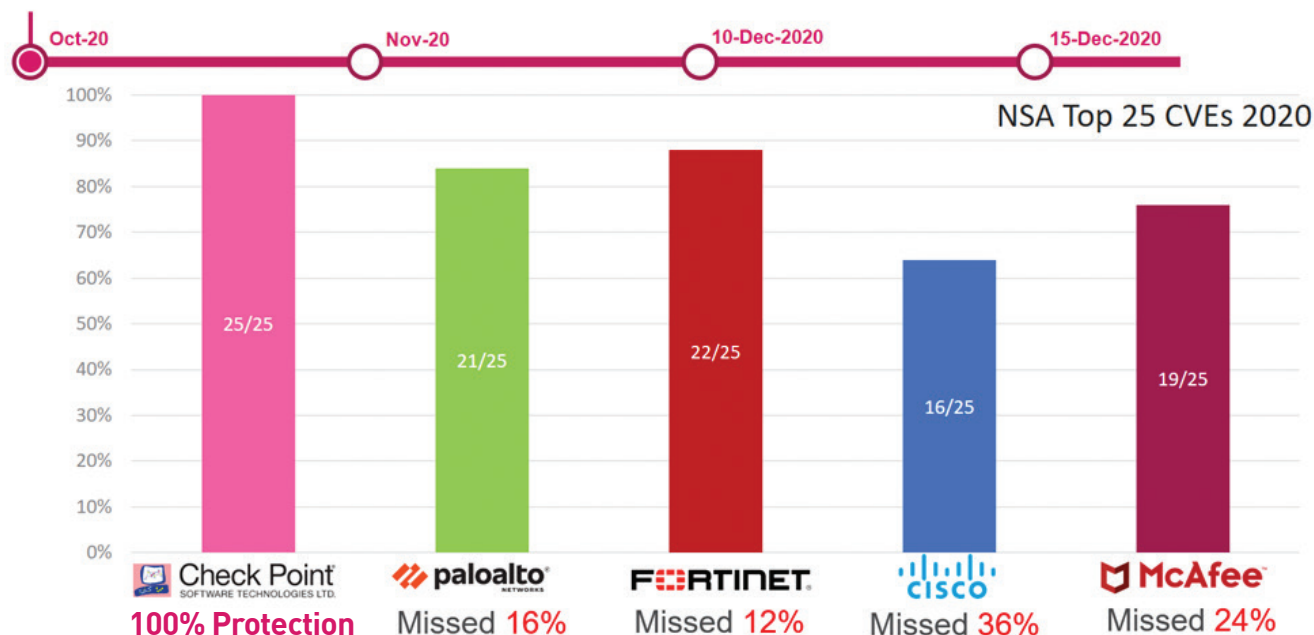
<sup>20</sup> <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>



## 1<sup>st</sup> to Secure Your Everything



NSA issued **an alert for on-going abuse** of 25 high-profile vulnerabilities in the wild. **Check Point customers were 100% covered at this initial announcement.**



Validation date—Nov 2<sup>nd</sup>, 2020 [CP Blog](#)

6



## Guard Against Insider Threats With Zero Trust

Protecting the security perimeter from cyber threats used to be enough. Once a user, application or device was inside, it could be trusted. Now, the business environment has expanded and the perimeter is everywhere.

The key to overcoming the challenge of "perimeter everywhere" is a Zero Trust architecture. Zero Trust is the way to handle the increased propensity for connecting everything to the network. The surest bet is not to trust anything, and to move trust down to the user/device, forcing each user/device earn trust before syncing with the network. With least-privileged access, datacenter elements are never exposed to the user. Instead, users are granted granular access and only gain visibility into authorized applications.

Within the Zero Trust space, you can also go beyond access control and can obtain integrated threat prevention. This includes advanced IPS and WAF, which can protect applications.

Modern Zero Trust models also provide DDoS protection. Your application connector will conceal the data center from attackers. Zero Trust can also offer application-level reverse proxies in the cloud. This allows for granular visibility and enforcement: user actions, key management and SSO.

Chances are high that many of your employees use work devices during non-working hours. This may be the case on account of a limited number of devices shared by a large family, higher quality work technologies than personally owned devices, or due to bring your own device policies (BYOD). Regardless of the context, ensure the integrity of your systems.

Future-proof your enterprise. No matter the user of the technology connected to your system, you can limit your cyber security risk. Zero trust network access can help safeguard software and hardware on every device, anywhere, anytime.

7



## Shared Intelligence Means Better Security With Less Work

To have the greatest quantity of threat intelligence at your disposal, purchase a solution with shared threat intelligence. Receiving intelligence from multiple streams, supplemented by research directly from incident response teams can help you see around blind spots. Shared threat intelligence enables you to see which threats are affecting your geographical locale, or your industry, specifically. When shopping for solutions with built-in threat intelligence, look for platforms that are:

- Accurate
- Aligned with your intelligence requirements
- Integrated
- Predictive
- Relevant
- Tailored
- Timely

Top-tier solutions can connect the dots for you, enabling you to quickly respond to threats, or to remediate where necessary. With comprehensive, shared threat intelligence, you can see the whole picture in full-focus, rather than a partial, blurry scene.

## 8 Control the Cloud

Organizations need the ability to easily manage security and compliance for cloud environments. The development of the public cloud allows organizations to scale, and to conduct business more efficiently, but the lack of borders also demands an entirely new level of security. As a result, we're seeing more cloud challenges than in the past. We'll describe why you should take control over your cloud security, and show you how to do so.

- Cloud hijacking is a growing concern. A variety of measures should be taken to protect against compromised credentials and identity theft, including the encryption of sensitive information before it's placed in the cloud, MFA and more. As an added layer of security, consider a solution with just-in-time privilege elevation with out-of-band authorization for IAM actions. Limit access, but also retain the capacity to modulate controls.
- In controlling your cloud, you'll also want to be able to easily visualize and assess your security posture, quickly detect misconfigurations, actively enforce best practices, and mitigate risk through simple remediation. With a consolidated cyber security solution, you can accomplish all of these things through a single management console, bringing agility to the security and compliance lifecycle.
- Hassle-free cloud compliance and governance are critical. Security teams are often beyond busy, and the magnitude of this endeavor frequently exceeds employees' capacities. Look for security with comprehensive compliance management, including automated, continuous compliance that can help assess and enforce best practices.

## 9 Managing a Unified Configuration

Synchronize your security. Centralized security management reduces complexity, strengthens security, improves workflow, and reduces human errors.

Buying one security management console that can offer forensics for cloud, mobile, networks, and endpoints dissolves the complexity that comes from managing different consoles, policies and logs.

When you invest in a single security management console, you not only reduce complexity and improve security, you also improve workflow. Multiple consoles means toggling back and forth across 10 or more different systems, leaving some systems unattended while you examine others. As a result, you and your team may see threats belatedly, giving them ample time to cause preventable system damage. A single management solution presents all of the insights upfront, cutting down on management time, and allowing you to rapidly triage any outstanding challenges.

Lastly, owning multiple solutions that are not interoperable requires security professionals to manually enter data into different platforms. Not only does this create the monotonous task of rekeying information, it also exposes organizations to data entry errors. With an integrated solution, data only needs to be entered once, cutting down on the risk of employee errors and strengthening your cyber security posture.

For any of a number of reasons, is not always possible for a given organization to adopt a fully consolidated approach. In this case, organizations can adopt a modular approach to security, gradually deploying individual security components over time in order to build a complete security posture. Depending on your budget, your labor force, or other constraints, this could be the best option for your organization.

10



## The Security Vendor's Architecture Must Be Secure

Those who build security products are well versed in terms of how to build securely. Nonetheless, the occasional security vulnerability gets baked into an application. If this occurs, you'll want to be working with a company that reacts swiftly, and that can quickly provide patches (or alternatives) to customers.

In 2019, previously unknown vulnerabilities within a security vendor's system were exploited by a state-backed hacking group. Unfortunately, it took a long time for these vulnerabilities to be patched, and to this day, there are still customers running vulnerable versions of those solutions. This incident highlights the importance of choosing a vendor that has your back, and that's ready to take every action necessary to efficiently provide quality security.

Working with a mature, well-known security firm can mean the difference between consistent security, and rapid responses, vs. compromised systems.

Check Point's Infinity architecture encompasses more than 60 security services and provides services for more than 50 types of assets. Experts can respond to requests in real-time or in under 24 hours.

---

Fact: Check Point provides 9X less menu complexity over all competition.

---







## Comparing the Competition

Decide on which vendor to work with by taking the ten key components of effective, advanced security and benchmarking them against actual vendors. To make things easy, we've taken the heavy lifting out of the equation for you, providing you with a brief analysis of who's who within the market space. Discover which vendors have security products that most closely align with the recommendations in this buyer's guide.

### KEY PLAYERS IN CYBER SECURITY MARKETSPACE

#### 10 Most Important Considerations in Choosing Your Cyber Security

	 Check Point SOFTWARE TECHNOLOGIES LTD	 CISCO	 paloalto NETWORKS	 FORTINET
Real-Time Prevention	✓	×	×	×
Identification	✓	✓	✓	✓
Inspection within SSL/TLS	✓	✓	✓	✓
Going Beyond Signature-Based Defenses	✓	✓	✓	✓
Protection from Every Direction	✓	Partial	Partial	Partial
Zero Trust Approach	✓	Complicated	✓	✓
Shared Threat Intelligence	✓	✓	✓	✓
Control the Cloud	✓	×	✓	Partial
Unified Management Configuration	7 Menus	35 Menus for Same Tasks	32 Menus for Same Tasks	19 Menus for Same Tasks
Security from the Start	✓	×	×	×

Check Point is 60% easier to manage in day-to-day tasks as compared to competitors.

## Agony Meter— Management efficiency scale

Whether managing a few sites with hundreds of rules or managing complex architectures that require auditing and compliance monitoring, you need the right tools and architecture. Are signal delays and multi-step processes in your security management console slowing you down?

If you could save five, ten or five hundred minutes per month in execution across security tasks, what would that mean for your productivity and overall enterprise security? You and your organization could benefit immensely. More effective and simple security management reduces chances errors that could lead to breaches. The greater the management complexity, the bigger the risks you face. Gartner has reported that 99 percent of all firewall breaches through the next several years will be caused by misconfigurations— not flaws.<sup>21</sup>

So, how can you determine which products will help you become more efficient, organized and effective in managing your security?

Cyber security researchers designed five day-to-day workplace security administration scenarios that parallel real-world in-the-office activities. The researches then lab tested their scenarios using security products from different vendors.

Out of those five scenarios, researchers distilled seven different measurements for security management work, as indicated by the table below:

FACTOR	TIME (SEC)	LEFT CLICK	RIGHT CLICK	DOUBLE-CLICK	KEYSTROKES	MENUS
Agony Value	5	1	1	1.5	0.2	25

For each measurement, an “agony score” or a numerical value indicative of task performance was created.













































































In conducting a comprehensive comparative analysis of security products from Fortinet, Cisco, Juniper, Palo Alto and Check Point, researchers determined that Check Point Security Management is the industry’s most integrated and robust platform for managing security across organizations at any scale. It’s also 60 percent easier to manage than other leading security platforms.

Keep your IT security simple, manageable and effective. Focus on robust, integrated security that saves time, saves on costs, and saves your organization from cyber threats.

<sup>21</sup> “Why Security Misconfiguration Are Higher During COVID-19,” by FireMon, Security Blvd., May 11, 2020  
<https://securityboulevard.com/2020/05/why-security-misconfiguration-are-higher-during-covid-19/>

# Summary

Based on the results of our analysis, Check Point security management is the industry's most integrated and robust platform for managing security at organizations large and small.

Agony Meter 2.0	 Check Point SOFTWARE TECHNOLOGIES LTD	 paloalto NETWORKS	 FORTINET	 CISCO
<b>Task 1</b> Application Control Granularity	 00:36  59  1	 01:22  70  9	 01:02  59  6	 01:50  70  7
<b>Task 2</b> IPS Exceptions based on Logs	 00:30  12  2	 01:42  44  8	 00:42  21  5	 02:34  45  9
<b>Task 3</b> Tag based Cloud Network Security	 00:38  46  1	 01:15  79  6	 01:42  100  5	 02:33  156  9 *
<b>Task 4</b> Finding the Needle in the Haystack	 00:13  10  1	 01:00  47  2	 00:44  37  1	 00:46  17  3
<b>Task 5</b> Simultaneous Security Tasks	 00:24  67  2	 01:34  82  10	 01:26  61  5	 01:20  97  10
<b>Totals:</b>	 02:21  175  7	 06:53  324  35	 05:36  281  22	 08:43  390  38
<b>Normalized Agony Score</b>	<b>1</b>	<b>3.21</b>	<b>2.45</b>	<b>3.99</b>

\* Cisco's results in task 3 reflect a 50% penalty since the lack of dynamic cloud objects make this task impossible to complete

The analysis above can help you distinguish the signal from the noise. Get better returns on your investment and get better outcomes with Check Point Security Management.

## Summary

In this guide, we've discussed each of the key elements that you need to consider as you strive to improve your cyber security. Choosing the right security product depends on understanding the technological functions that will protect your organization from the latest threats. Now that you know what's on the market and which tools can provide unyielding and robust digital defense, you can make the best cyber security decisions possible for your organization.

**Download a test plan for a next generation firewall.** To measure the effectiveness of your security management, go to the [Agony Meter](#). For additional cyber security resources, visit [Cyber Talk](#).