Check Point
SOFTWARE TECHNOLOGIES LTD

SECURE YOUR EVERYTHING™

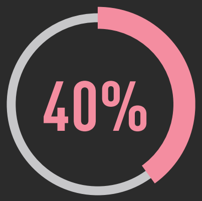
SIX REASONS FOR CHOOSING CHECK POINT TO PROTECT YOUR ENDPOINT DEVICES

Introduction

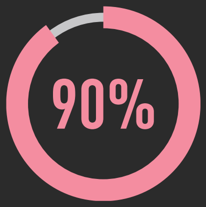
The Covid-19 has accelerated changes in workplace. Companies gained experience working remotely and more employees will have the opportunity to work away from the office, at least part-time. Hackers around the world are taking advantage of those changes. Endpoint Protection solutions play the critical role in protecting against today's threats.

With millions of types of unknown malware using sophisticated evasion techniques, stopping today's most dangerous attacks requires a deep level of data traffic inspection to and from corporate endpoints. Traditional products do not provide this level of inspection for potential threats. They use traditional detection methods based on signatures or rules — and while these are valuable techniques for detecting established, known threats, they cannot detect new, sophisticated, unknown malware and phishing attacks.

According to research conducted in March 2020 by Dimensional Research:



of security professionals are not confident in the resilience of their current Endpoint Protection solution against advanced cyber-attacks.



of security professionals agree that in the past 3 years the sophistication of cyber-attacks has increased.

As such, it is essential that organizations examine whether their existing Endpoint Protection solutions are protecting them from today's most complex, damaging attacks. They should evaluate whether they have to replace them with an advanced, comprehensive solution which can identify and block even new, unknown malware threats.

Check Point's SandBlast Suite is providing an advanced Threat Prevention consolidated solution, with the highest catch rate in the market, by using a multi-layered advanced technology. The SandBlast Suite includes SandBlast Network, SandBlast Agent and SandBlast Mobile. The solution is part of Check Point Infinity, which provides full protection for the entire organization's network.

In this paper we will review six important reasons for choosing Check Point to protect your Endpoint devices: prevention, a multi-layered technology, consolidated architecture, cloud management, remediation and industry validation.

1 Prevention, not detection

It is much less costly to prevent an attack, than to detect and remediate it after it has breached the network and caused damage. Cyber Security research showed that the average cost of malware attacks rose by 11% over 2018, to $2.6 million.[1] Therefore, when choosing a security solution for endpoint devices, it's important to make sure that the solution is actively preventing attacks. This is why Check Point has invested heavily in various prevention technologies, including:

1 **Zero-Phishing** — Phishing attacks use fraudulent emails, messages, and social applications to trick end users into passing on sensitive data such as application login credentials and credit card information. Check Point's Zero-Phishing engine provides the broadest phishing protection in the market. It performs a full scan of websites and forms, followed by a deep heuristic analysis. The analysis includes reputation, similarity algorithms (such as visual similarity and textual similarity), detection of image-only websites, lookalike favicons, and more. Check Point's Zero-Phishing solution also includes a password reuse capability, which alerts users when using their corporate password on non-corporate domains.

2 **Files sanitization (CDR)** — In many cases, malware infection starts with a document. SandBlast Agent's Threat Extraction solution proactively prevents known and unknown attacks by removing exploitable or suspicious content from documents. The solution facilitates true zero-day prevention, while delivering files to users quickly so work is not interrupted, ensuring productivity.

3 **Exploits Prevention** — Most successful attacks don't need sophisticated tools that exploit zero-day vulnerabilities — they simply exploit known vulnerabilities that have been left unpatched.The SandBlast Suite identifies critical applications and OS vulnerabilities and prevents their exploitation.

[1] Ninth Annual Cost of Cybercrime Study, The Ponemon Institute LLC and jointly developed by Accenture https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf%23zoom=50

4. **Anti-Ransomware**—Check Point's Endpoint Protection Anti-Ransomware engine monitors the changes to files on user drives to identify ransomware behavior such as file encryption. Once a ransomware behavior is detected, SandBlast Agent blocks the attack and can even recover encrypted files automatically.
5. **Malware DNA**—Innovative model that classifies new forms of malware into known malware families based on code and behavioral similarity.
6. **Download Prevention**—Preventing the download of malicious applications and files blocks the attack at the earliest possible stage. The SandBlast Suite blocks malicious application and file downloads on windows desktop, iOS and Android mobile devices. This is achieved by using AI models that block the download immediately, also on https traffic.
7. **Anti-Bot**—SandBlast Agent and SandBlast Mobile monitor all the network traffic of the devices and block connections to malicious websites based on the dynamic security intelligence provided by the Check Point ThreatCloud™ reputation service.
8. **Man-in-the-Middle (MitM)**—These attacks involve a malicious intermediary between the victim and the entity they are trying to communicate with. Attackers may gain access to an unsecured network, take over a secured network or impose as a secured network. Then they can follow the transmitted data and steal credentials, corporate data, credit card information, and personal data. Check Point's SandBlast detects MitM attacks and automatically launches a secure connection.

For more information regarding the prevention technologies, please refer to the SandBlast Agent Solution Brief and SandBlast Mobile Solution Brief.

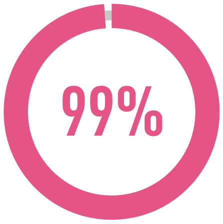
2 Multi-Layered Security

Achieving a high catch rate with today's sophisticated, ever-evolving attacks, requires a new approach. Traditional point products such as anti-virus, traditional sandboxing solutions, traditional endpoint security solutions, UEM solutions and even most mobile security solutions do not provide this level of inspection. They use traditional detection methods, such as signatures or rules, which can't detect complex, unknown malware and phishing attacks. The SandBlast Suite is designed to prevent those attacks by using a multi-layered technology that includes:

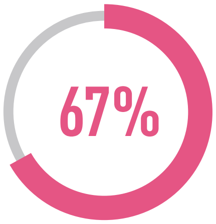
1. **Artificial Intelligence (AI)**—The velocity of malware evolution and the huge amount of data to process makes it impossible for human-created models to give comprehensive protection. To overcome this challenge, Check Point has developed dozens of AI engines and incorporated them in critical decision points. SandBlast Agent incorporates dozens of AI engines that perform static and dynamic analysis of files and executables, behavioral analysis, malware classification, signatures generation and more. SandBlast Mobile also incorporates many AI engines that perform behavioral analysis, static and dynamic analysis of applications and meta-data and malware classification.

2. **Cloud-based Reputation Engine** — The SandBlast Suite blocks access to malicious sites and drops malicious connections based on the risk score provided by Check Point's ThreatCloud™ reputation service. The SandBlast Suite collects indicators such as the domain, IP, and registrar, and sends them to the ThreatCloud™ reputation service. The reputation service calculates the risk based on advanced algorithms and sends the output back to the device for final verdict and prevention.
3. **Advanced Sandboxing** — Check Point's Threat Emulation engine provides the only sandboxing solution that combines the power of CPU-level and OS-level protection. The solution detects and blocks malware, and prevents infections from undiscovered exploits, zero-day, and targeted attacks. SandBlast Agent sends files and executables to the cloud-based Threat Emulation service and SandBlast Mobile sends applications to cloud-based mobile sandboxing. The cloud-based sandbox engines perform a deep analysis and provide a verdict that is used by SandBlast Agent and SandBlast Mobile to prevent attacks.
4. **Behavioral Analysis** — Check Point's behavioral engines provide predictive malware detection and classification. The engines collect behavioral indicators from the device, correlate them and apply behavioral heuristics, rules and machine learning engines in order to identify malware and classify it.

3 Consolidated Architecture



of security professionals claim that using solutions from multiple security vendors causes them challenges.

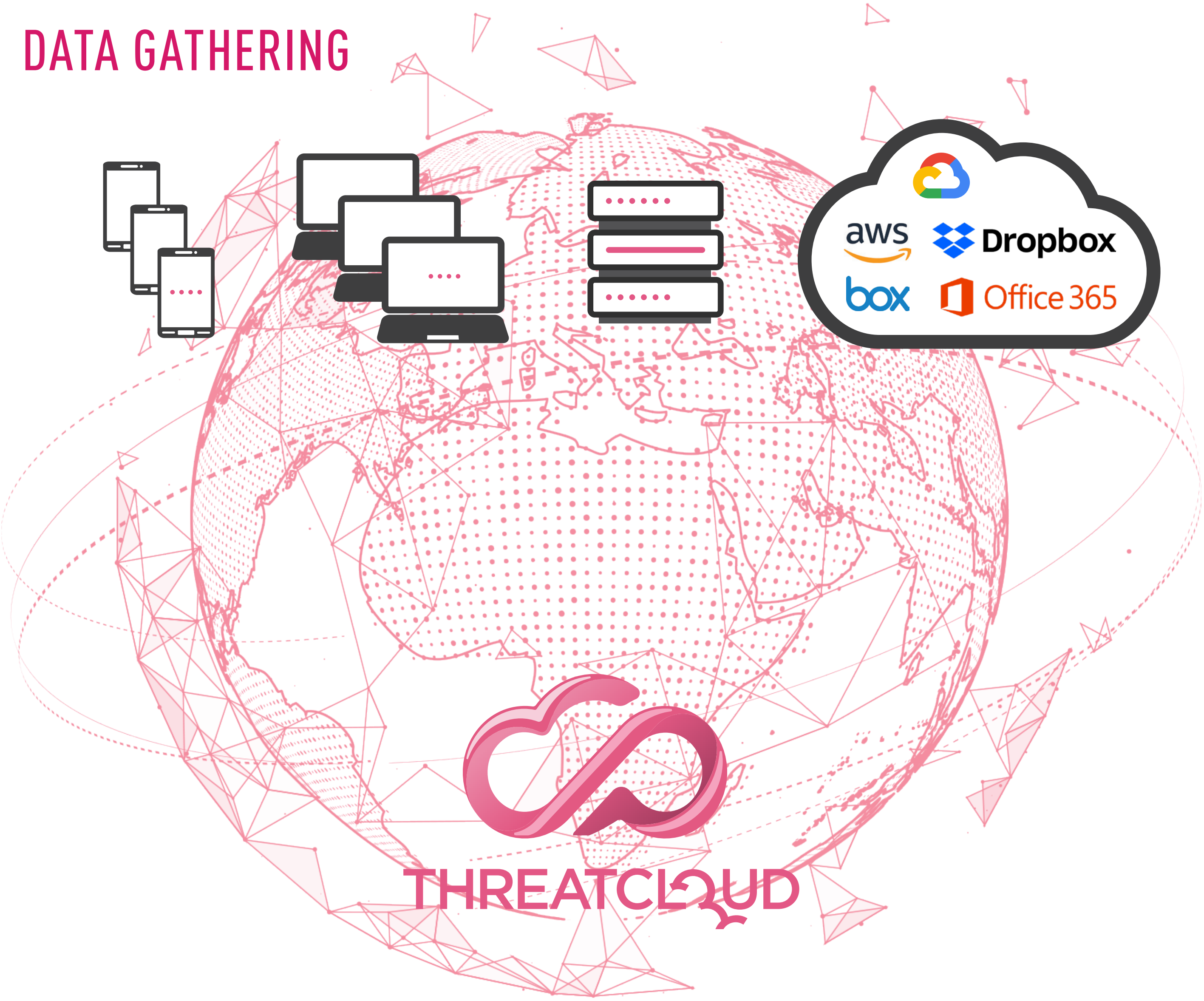


of security professionals agree that prioritizing consolidation to fewer security vendors would improve security

Check Point Infinity is the only fully consolidated cybersecurity architecture that protects businesses and IT infrastructures against mega cyber-attacks across networks, endpoint, cloud, mobile and IoT. The Infinity architecture delivers the highest threat prevention in the industry.

Infinity also provides SmartView: consolidated and web-based logs, reports and monitoring advanced tool. SmartView provides built-in and customized dashboards, views and reports.

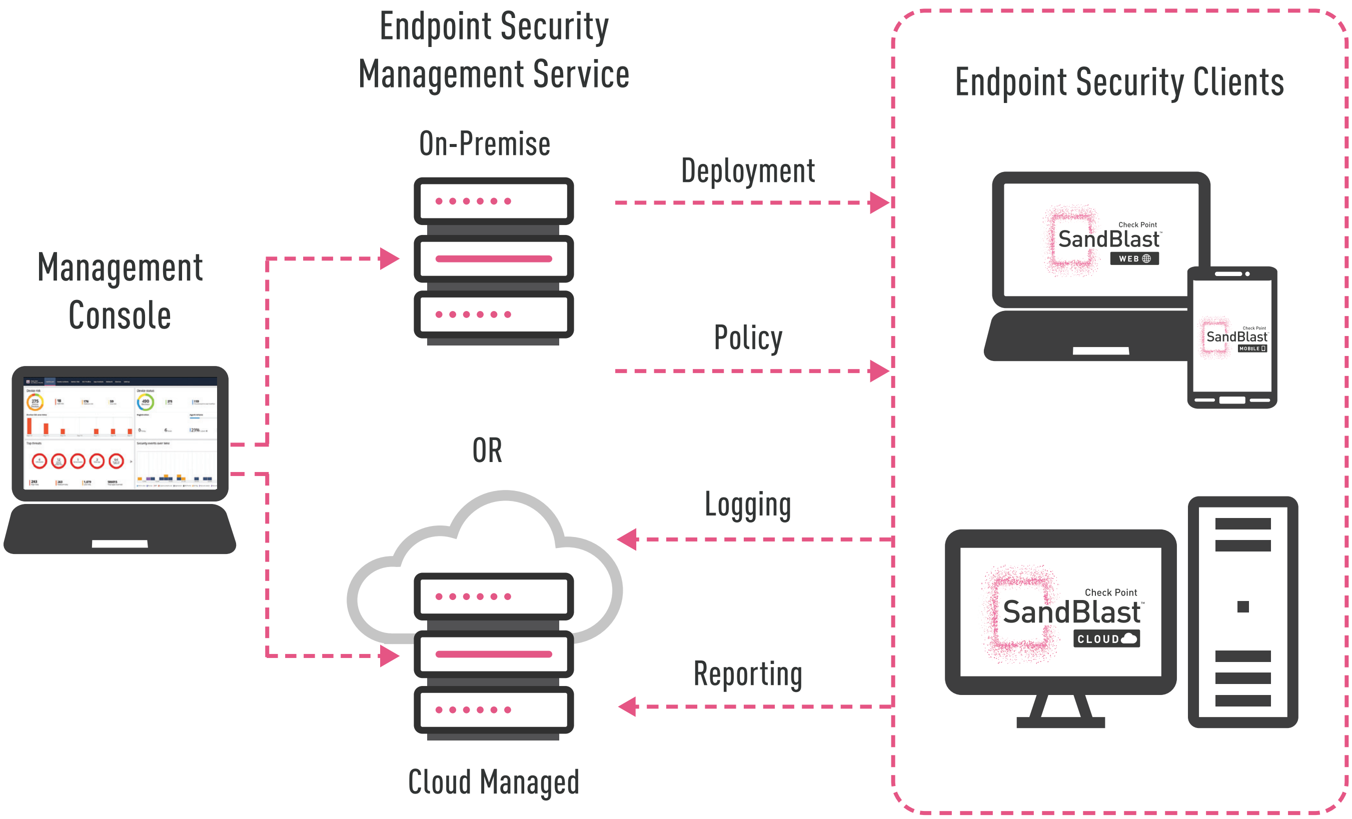
DATA GATHERING



ThreatCloud, the largest threat intelligence hub in the world, is part of Infinity. ThreatCloud is acollaborative knowledge base that delivers real-time dynamic security intelligence to Check Point's security solutions. ThreatCloud's knowledge base is dynamically updated using feeds from a vast network of global threat sensors, attack information from gateways around the world, and Check Point research labs. The resulting up-to-the-minute security intelligence is shared across the entire product line, including SandBlast Agent and SandBlast Mobile.

4 Cloud-Based Management and Simple Deployment

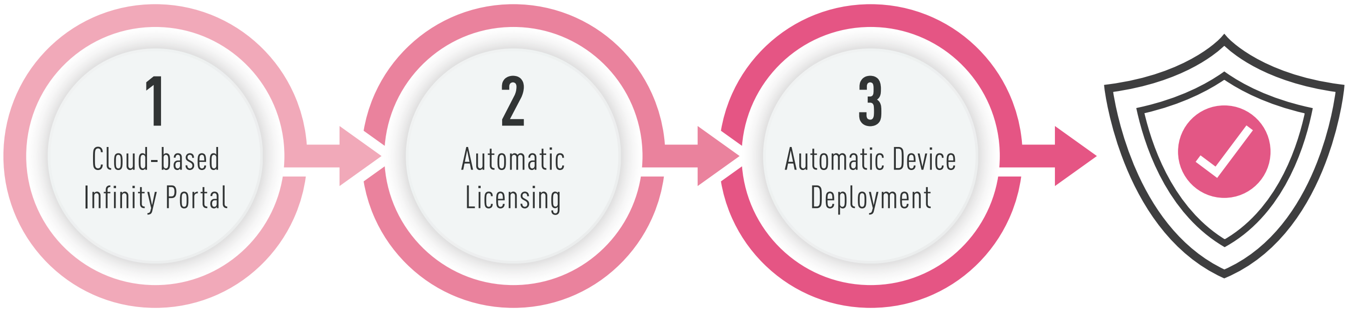
Even though cybersecurity employees are considered essential and were expected to continue working during the COVID-19 outbreak, many of them are required to do this from home. Therefore, a remote, expandable, fully redundant and easy-to-use management is important now more than ever. Infinity offers a unified cloud-based management solution that delivers these capabilities and enables provisioning and monitoring of devices and policies from the cloud, while keeping full redundancy and automatic backups.



Check Point SandBlast™

The SandBlast Suite can be deployed within minutes on all your Endpoint devices:

- Cloud-based deployment with Infinity Portal
- Centralized deployment
- Automated, seamless deployment
- Mobile device deployment using UEM sync
- Automatic Licensing



Further information regarding SandBlast Suite deployment can be found in the SandBlast Agent Cloud Management Administration Guide and in the SandBlast Mobile Dashboard Administrator Guide.

5 Post-Infection Remediation

Organizations today should assume that they will eventually be compromised at some point. Even if an organization is equipped with the most comprehensive, state-of-the-art security products, the risk of being breached cannot be completely eliminated. Therefore, strong attack containment and remediation capabilities are critical. The SandBlast Suite includes robust remediation capabilities:

1. **Quarantine** — Once malware has been detected by SandBlast Agent, the infected device can automatically be quarantined and the administrator will be notified. Once malware has been detected by SandBlast Mobile the access of the device to the corporate assets is automatically blocked until the threat is removed.
2. **Forensics** — SandBlast Agent Forensics automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report.
3. **Remediation** — SandBlast Agent is the only Endpoint Protection solution that automatically and completely remediates the entire cyber kill chain to shorten response time. SandBlast Agent is capable to perform fully automatic remediation thanks to its rich forensics data.
4. **Ransomware Recovery** — SandBlast's Anti-Ransomware engine recovers encrypted files regardless of the encryption used, by taking smart snapshots of the system.
5. **Incident Response** — The SandBlast Agent forensic analysis process starts automatically when a malware event occurs. Advanced algorithms and a deep analysis of the raw forensic data helps build a comprehensive incident summary with actionable attack information, including infected hosts, entry point, malicious events, damage scope and impact. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.

6 Industry Validation

Independent evaluation of security products, comparing the effectiveness, simplicity and performance of competitive solution is an important criterion when choosing security solutions. Check Point SandBlast Agent and SandBlast Mobile solutions are achieving the best prevention rates of both known and unknown attacks in various independent tests, such as NSS. Check Point achieves these excellent ratings by combining dozens of Artificial Intelligence engines, advanced sandboxing, dynamic threat intelligence, threat extraction (CDR) and zero-phishing prevention. As a result, the solutions are recommended by third-party, independent analysts including Forrester, Frost & Sullivan, Miercom, NSS and Gartner.

Summary

The SandBlast Suite is the industry's most comprehensive security solution for Endpoint Protection and Mobile Security, protecting users wherever they go. SandBlast Agent and SandBlast Mobile deliver the best prevention rate for even the most evasive and advanced zero-day and known attacks such as malware, zero phishing, ransomware, infected apps and Man-in-the-Middle attacks. This is achieved by applying a multi-layered, advanced technology.

The solution is part of Check Point Infinity, the only fully consolidated cybersecurity solution that protects against mega cyber attacks across the entire network. SandBlast Agent and SandBlast Mobile can be managed from any location using the cloud-based Infinity portal, with an intuitive interface, simple deployment, and easy configuration that allows for effective remediation techniques.

If you are new to Check Point, click here for a trial license of SandBlast Agent and here for a trial license for SandBlast Mobile. Existing Check Point customer can get the free trial though their User Center account.

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