THE CASE FOR A PREVENTION-FIRST APPROACH

Sponsored by Cyber Talk

Will 2023 be another year of continuous data breaches? In 2022, global organizations contended with a ransomware attack every 11 seconds.[1] In the third quarter of the year alone, 15 million data records were compromised due to cyber security incidents. The average cost of information loss is $5.9 million, and worldwide cyber crime costs are projected to exceed 10 trillion annually by 2025.[2] [3]

"The past 12 months presents one of the most turbulent and disruptive periods on record, at least as far as security is concerned," says Check Point's Chief Product Officer and board member, Dorit Dor. Unless we take drastic action now, the next 12 months may not prove much different, and a confluence of factors could actually render the new year significantly worse.

Cyber security incidents cannot become a new norm. They reduce organizational integrity, and place critical services and individual lives at-risk. How is your organization going to help flatten the security incident curve and cultivate a stronger resilience profile?

The Prevention-First Approach

Put cyber security prevention at the center of your strategy. In stopping frequent and costly cyber attacks, in-depth analyses show that implementing a prevention-first cyber security framework is easier, more effective and more cost-efficient than continued reliance on detection methodologies alone. A detection-based set-up means that you're allowing the cyber criminals within arm's reach of your valuable assets. If your organization is not yet leading with a prevention-first strategy, here's what you need to know in order to secure every facet of your enterprise…

Prevention-First is Easier

As organizations like yours accommodate growing digital footprints and store ever-increasing quantities of data, cyber security must scale. Cyber security must keep up with increasing risk levels. If using a detection-focused approach, the approach may not lend itself to the sprawling complexity associated with digital growth. A detection-focused approach may lead to operational overwhelm.

[1] Cybercrime to Cost the World $10.5 Trillion Annually by 2025, Steve Morgan, Cyber Security Ventures, November 13, 2020.
[2] The State of Cybersecurity Resilience 2021, Accenture, November 3, 2021
[3] Cybercrime to Cost the World $10.5 Trillion Annually by 2025, Steve Morgan, Cyber Security Ventures, November 13, 2020.

An overwhelmed security operations team, deluged by dozens of simultaneous alerts (some of them false), may miss or have trouble coping with fast-moving threats, leading to acutely negative security outcomes.

A prevention-first cyber security program orientation reduces the complexity of the workload for the security operations team. It can also help prevent burnout. This is especially beneficial amidst the continued shortage of skilled cyber security professionals, which places hefty burdens on the shoulders of existing staff members.

A prevention-first framework also enables staff members to focus on higher-value tasks, meaning that security ops can measurably improve the larger security picture as a whole.

> "Prevention is so much better because you can sleep at night" – CISO Pete Nicoletti, Check Point

Prevention-First is More Effective

As noted previously, detection means allowing the hackers in and flirting with the possibility of a fiasco. In contrast, a prevention-first cyber security framework allows organizations to stop attacks before they can filter through systems.

In more technical terms, prevention starts with the neutralization of malware prior to a kill-chain's exploitation stage. If malware cannot operate as intended, the downstream consequences, and the subsequent need to track, contain and remediate the damage are negligible.

Prevention-First is More Efficient

A prevention-first framework is more efficient than a detection-based approach from both the time and cost perspectives.

Time

Organizations that implement a prevention-first approach and that reduce threats capable of accessing systems can eliminate post-breach wheel spinning, which encumbers the security operations center team, and consumes an extensive quantity of time.

For instance, in the event that an adversary has accessed systems, a security operations center (SOC) team must assess whether or not the intruder has deposited an artifact or a dropper within the network, which would allow them to access systems at a later date.

This work requires more time than needed in this day in age, given the protection afforded by a prevention-first framework.

Cost

The cost of cyber attack recovery often far-and-away exceeds the cost of implementing prevention-focused security technologies. The average cost of a cyber attack itself is $5.9 million. By way of comparison, the average cost of cyber security for a large business might be between $2 and $5 million, according to estimates.[4]

Detection Alone: Not Enough

On their own, detection-based tools cannot offer the level of security required to keep a modern organization sufficiently secure.

Detection-based tools rely on signatures. This means that unknown threats can easily sleuth through traditional detection-based defenses. In 2022, cyber criminals launched over 400,000 new malicious files on a daily basis, rendering it somewhere between extremely difficult and nearly impossible for detection-based defenses to keep up.[5]

> "If your security devices are in detect mode it is like watching in a monitoring room when someone steals your goods, but no one is there to prevent it from happening." – Lari Luoma, Check Point Security Expert

[4] What is the Cost of Cybersecurity for a Business..., Bryan Badger, Integral Networks, Feb 13, 2022.
[5] Cybercriminals Use Over 400K Malicious Files to Attack Users Daily: Report, December 12, 2022.

Prevention-First Framework

In preventing a plurality of unknown and known threats, implement a prevention-first oriented cyber security framework. While there is not a one-size-fits all approach, the following guidelines are intended for any organization, regardless of industry or profile.

Step 1: Leverage a big data threat **intelligence platform**. These types of platforms provide security analysts with a real-time picture of pending threats in order to prevent threats. Intelligence platforms rely on hundreds of millions of sensors worldwide, and analyze millions of Indicators of Compromise (IoCs) every day. They can help professionals determine which tactics, techniques and procedures to prepare for. In essence, threat intelligence enables organizations to take a proactive approach to the prevention of advanced threats.

Step 2: Consolidation. Estimates suggest that the average cyber security team relies on 57 unique cyber security products.[6] On this account, teams often have extremely large quantities of data that needs analysis. However, the data is sufficiently disparate and disjointed that administrators cannot piece together the overall security risk nor see the larger picture. When implemented effectively, consolidation allows for strong cyber risk management through increased visibility and robust threat prevention.

Step 3: Artificial intelligence (AI) and automation. The implementation of artificial intelligence tools for purposes of automating processes renders your organization agile, adaptive and cyber-ready. Artificial intelligence uses behavioral models to analyze cyber threats, and deploys deep learning technologies to protect against the most sophisticated attacks, including zero-day phishing and domain name system exploits.

In addition, AI and automation are helping organizations increase the speed and accuracy of breach responses. Organizations that use artificial intelligence and automation have been found to experience a 74-day shorter breach life cycle than those without it. Further, organizations implementing AI show savings of $3 million more than their peer organizations. [7]

Step 4: Implement a suite of additional prevention-based **rules, processes and tools**. For instance, patch your servers and applications, use an Intrusion Prevention System, deploy multi-factor authentication for internal services, use anti-ransomware in users' endpoints, establish SOC and a user security operations platform that immediately identifies and isolates infected machines, and segment networks to prevent malware from east-west movements.

[6] "CISOs Struggling with %0+ Separate Security Tools, Infosecurity Magazine, Phil Muncaster, June 20, 2019.
[7] "How AI Cybersecurity Tools Tackle Today's Top Threats, Victor Dey, Venture Beat, December 15, 2022.

Prevention in-Action

If your organization is searching for best-in-class cyber security prevention tools that protect data from theft, corruption, loss and more, a sampling of Check Point's leading technology solutions are outlined below:

Meet **ThreatCloud**: Understanding the threats is the first step in preventing them. Check Point's real-time threat intelligence platform uses advanced predictive intelligence engines, data from hundreds of millions of sensors, and cutting-edge research from Check Point Research, along with external intelligence feeds to power its performance. Prevent threats 24x7 with this award-winning technology that provides global threat intelligence.

Meet Check Point **Infinity**: Check Point Infinity is the first modern, consolidated cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Check Point's entire portfolio of security solutions can be managed through a single pane of glass, and adheres to all five Zero Trust principles.

Meet Check Point's **automation tools**: Check Point offers EDR, XDR and NDR capabilities, which SOC staff can use to shut down potential threats automatically, thereby reducing work for security administrators. Check Point also integrates with Security Information and Event Management (SIEM) solutions, which detect and provide contextual information about security incidents, then automate responding to those incidents using Check Point APIs.

Meet Check Point **SandBlast**: Check Point SandBlast prevents unknown threats on firewalls, endpoints and mobile. On firewalls and endpoints, SandBlast includes sandboxing and Content Disarm & Reconstruction (CDR) protections. While files are "detonated" in a sandbox, CDR removes active content from files and gives the user safe content. This ensures users are safe and detects and prevents unknown zero day threats.

Regardless of the industry or size of your organization, it's time to switch to a prevention-first security operations approach.

In closing

While prevention represents merely one element within an effective cyber security strategy, it is the critical first-line of defense when it comes to reducing the probability of a breach. More insights here

Would you like to learn more about future-forward strategies in cyber security?
Learn more on CyberTalk.org

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