Cyber Talk

SECURING IoT BLIND SPOTS WITH NANOTECH

Introduction

The digital transformation's march to new technologies has ushered in the next tipping point. Connected device usage is exploding. IoT devices in use are projected to reach 31 billion in 2020.[1] Sensors are being deployed in smart buildings and cities and smart systems for corporate conferencing, security alarms, heating and ventilation, medical devices, among others. All these devices collect data, making them potentially vulnerable to cyberattacks.

IoT devices in many industries have inherent security weaknesses, creating security blind spots. Vulnerable IoT devices are offering cybercriminals yet another attack vector to breach data on your connected network.

Likewise, virtualization and cloud technologies have diversified from virtual machines into containers, serverless applications, and Function as a Service (FaaS). New technology adoption opens the door to unknown attacks that outpace standard security relying on a traditional patchwork of firewalls, antivirus, and intrusion protection.

In this whitepaper, we'll explore how advanced sixth generation cyber security technology can help you defend against multi-vector cyberattacks and advanced persistent threats (APT), safeguarding your complex information assets.

To help you see where security is headed, let's briefly review the arc of previous generations of cyber security controls.

[1] Nick G. How Many IoT Devices Are There In 2020? More Than Ever!, TechJury, February 19, 2019

Cyber Generations

Gen Zero 1960s. If an enterprise had a computer, it was a mainframe or microcomputer. A small number of system administrators oversaw computing operations. Attacking computers hadn't been invented yet.

Gen 1 1980's. Standalone personal computers (PCs) entered the workplace. For curiosity and sport, amateur hackers put malware on floppy discs to infect PCs. To counter this, vendors invented antivirus software.

Gen 2 1990s. Local area networks (LANs) connected PCs with servers inside the enterprise and to the Internet. For-profit criminals joined amateurs in using the Internet to access organizations' computers to steal sensitive data and disrupt operations. This was the start of using firewalls to separate local networks from the Internet.

Gen 3 2000's. Cybercrime became a global business. Criminals monetized attacks on web servers, applications, and email servers by stealing sensitive data such as banking credentials from individuals and organizations. Intrusion Prevention technology joined firewalls and antivirus for cyber security.

Gen 4 Early 2010's. Governments sponsored cyber espionage with attacks like Red October, Flame, DNC hacks, and Black Energy sabotage malware attack on the Ukraine power grid. Threat actors introduced polymorphic malware that self-adjusts its identifiable features in order to evade detection and automated malware editing to create large volumes of new unknown malware evading signature-based security controls. Sandboxes and anti-bot security technologies responded to these threats.

Gen 5 Late 2010's. Threat actors unleashed multi-vector cyberattacks that leveraged attack tools stolen from government intelligence agencies. These attacks such as NotPetya, WannaCry, SamSam, and BadRabbit traveled across networks connecting business partners. They rapidly infected and shut down tens of thousands of organizations globally. In addition, attacks against smartphones to steal account credentials and attacks against cloud deployments became commonplace.

To counter unknown multi-vector threats, engineers developed consolidated-security architecture that protected all environments. Advanced threat prevention was created to prevent unknown threats from entering IT assets and impacting network, cloud, SaaS, and mobile environments.

Gen 6 2020. The maturity of IoT devices and the integration of industrial operating technologies with Internet technology as well as cloud technologies diversifying into virtual machines, containers, serverless apps, Function as a Service (FaaS) and microservices[2] brings us to today's 6th generation of technical complexity. The massive increase in unprotected threat surfaces means organizations must now protect 50 or more types of real and virtual assets against 60 or more kinds of attacks generated by state-sponsored advanced persistent threat (APT) groups and highly organized gangs of cyber criminals.[3]

[2] Jean-Christophe Huc, What are serverless app?, Quora April 3, 2017 https://www.quora.com/What-are-serverless-app?share=1

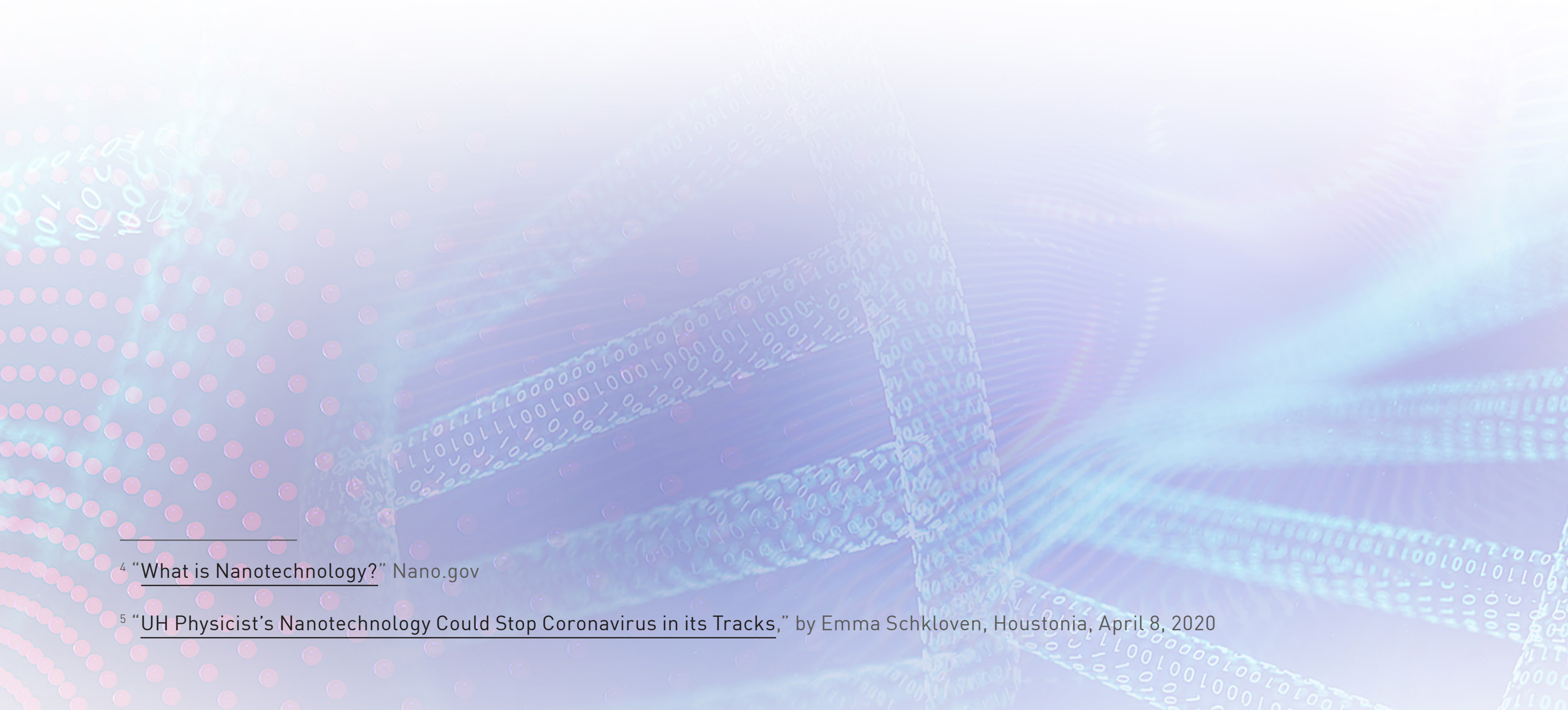
[3] Gil Shwed, CPX 360 2020 Cyber Talk: Cyber Security for 2020, Feb 12, 2020, https://www.youtube.com/watch?v=YUmwsvvXcJk

The challenges that C-level and security executives face for protecting their organization's unique blend of complex 6th generation technology are fourfold:

- Covering of all real and virtual IT assets with preventative cyber security
- Provisioning sixty or more diverse security controls for many types of devices
- Handling the rising costs of security operations
- Recruiting sufficient cyber security staff

> "Nanotechnology is science, engineering, and technology conducted at the nanoscale, which is about 1 to 100 nanometers. Nanoscience and nanotechnology are the study and application of extremely small things and can be used across all the other science fields, such as chemistry, biology, physics, materials science, and engineering."[4]

Nanotechnology can have unintended but life-saving implications. It's reported that Seamus Curran, a University of Houston physics professor and nanotechnologist developed a hydrophobic coating in 2011.[5] It's possible the coating can be applied to many surfaces, including masks that can be water-proofed so the COVID-19 coronavirus can't stick to its surface. Curran is also CEO of Integricote, a nano-coatings company.



[4] "What is Nanotechnology?" Nano.gov

[5] "UH Physicist's Nanotechnology Could Stop Coronavirus in its Tracks," by Emma Schkloven, Houstonia, April 8, 2020

Moving to Gen 6 Security

The path forward for handling these challenges lies in a new type of 6th generation security architecture. It begins by embedding lightweight (measured in Mbs) Nano security agents in every real and virtual device to provide complete security coverage in all environments. Their small size makes them suitable to embed in smart conferencing units, security alarms, wearable medical devices and other IoT and IIoT (Industrial IoT) devices and smartphones. In addition, Nano agents can be applied in real and virtual IT infrastructure elements and services. including containers and serverless applications.

To provide the needed types of security controls, each Nano agent calls on the threat intelligence capabilities of Check Point ThreatCloud™, giving a large and formidable arsenal of the latest cloud-based security engines to the connected device. The agent/cloud-engine portion of the architecture is able to deliver true preventative security for every asset and with minimal latency.

To reduce the cost and burden of operating this mass of technology, the new architecture uses advanced central management for all security engines and security agents. This gives security professionals total visibility of all environments through one user interface and simplifies the creation and management of security and access policies for network, cloud, SaaS, mobile devices, endpoints, and IoT devices. This consolidated management greatly reduces the number of staff hours needed for monitoring, administration, and management, while preventative security greatly reduces the need for time-intensive attack remediation.

In addition, being able to deploy hundreds of kinds of agents and security engines on demand greatly simplifies procurement as compared to sourcing security from dozens of independent vendors.

Strategies for Upgrading to Gen 6 Security

If you are in the enviable position of planning a forklift upgrade of your entire security operation, deploying the central management system and swarm of security agents is fairly straightforward after you have identified the vulnerable devices that need security and assessed your security requirements.

On the other hand, if you plan to roll out 6th generation security gradually, you can benefit most by deploying the central management system and populating it with only the security engines and agents you need immediately to plug your most egregious security gaps such as smartphones and IoT devices. To complete your Gen 6 roll out, you can replace legacy point solutions such as firewalls, web application security, email security and the rest as their service contracts expire.

Conclusion

Today's technology has become monstrously complex and costly to protect against today's sophisticated threats. Gen 6 security architecture based on agents, cloud security engines and consolidated management is the silver bullet today's organizations need to slay beastly security complexity and costs.

To learn how Check Point is reducing exposure to IoT cyber risk and proactively tackling IoT-related threats and vulnerabilities, visit https://www.checkpoint.com/products/iot-security/ or contact your local Check Point representative.

GEN VI
STEP UP TO THE 6TH GENERATION
OF CYBER SECURITY

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