Eliminate most Corporate Cyber-risk with Micro-Perimeter Security Prevent & Protect

Whether it’s NSA (Nation State Attackers), APT groups (Adv. Persistent Threats), espionage, botnets, hacktivists or hackers for hire etc. – they all pose a significant cybersecurity concern for the modern-day enterprise. The magnitude of cybercrime impact is immense. The attack tactics, techniques and procedures have been the same for 40 years, constantly way ahead of the defense based security strategies. It’s time to change the game.

Don’t get lulled into a false sense of (cyber) security

Russian hackers can infiltrate your computer network in 18 minutes. *(Source: Crowdstrike)*

Russian hackers aren’t wasting any time when they put their minds to it. North Korean hackers need just under two and a half hours. Chinese hackers takes longer – about 4 hours.

The current perimeter defense methodology has been outmaneuvered by the cyber-criminals – the firewalls, various cyber-security point-based-solutions and the detection of malicious activity and behavior – are NOT able to do the job – just keep on reading.

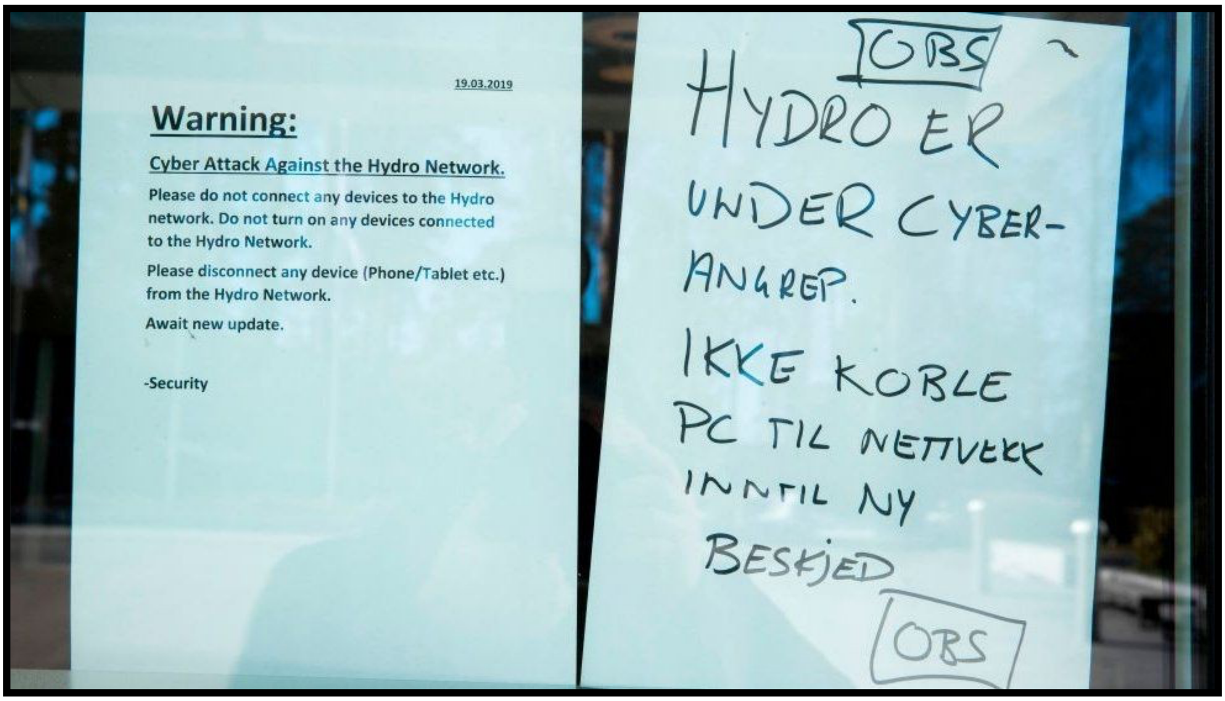
Something is fundamentally wrong, when cyber-criminals can trade, steal, compromise and hold organizational data for ransom – and get away with it. Here’s some highlights!

- The cyber-crime industry generates a revenue-stream of $1,600 billion p.a.
- Their behavior destroys organizational value of estimated $6,000 billion p.a.
- More than 30,000 web-sites are compromised daily
- 3 out of 4 organisations experience breaches every 12 months (PwC state 9 out of 10)
- 54% of all malware ARE NOT detected says Mandiant research
- At least 22 billion data-records are compromised yearly
- The ransomware attacks have increased by 90% year on year.
- e-Mail is your biggest risk – ‘importing’ the majority of malware
- 24,000 malicious mobile apps are blocked daily – many are NOT blocked
- 1 out of 2 internet users have had their account breached in 2021

Can you afford it?

In a 2022 FBI report – calculating cost of breach PER HOUR, the cost was $2,054 in 2001. In 2021 it was $787,671 – or nearly 400 times more in just 20 years. In 2041 => $302,465,664 pro-rated. Will any organisation survive that.

If you're an SMB – you are in a bad shape. 80% of SMBs don't have the knowledge, skills or resources to mitigate cyber-risk properly. Manufacturing and Production (OT and IoT) environments are experiencing higher exposure. March 18 (2019), Norwegian giant Norsk Hydro lost $35-41 million in the first quarter as direct result of a ransomware attack and expects additional losses of $23-29 million in the second quarter. They were hit by a ransomware named LockerGoga. Several Norsk Hydro plants was infected and caused operational disruption, forcing workers to rely on manual processes for several weeks.



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

OBS

HYDRO ER UNDER CYBER-ANGREP.

IKKE KOBLE PC TIL NETTVERK INNTIL NY BESKJED

OBS

Adversaries know the factory floor and it's systems are critical and sensitive (often the spine) within these organisations – and very often these systems are kept separate from the IT side, but as IoT is more and more introduced to these environments, they become vulnerable to new attack vectors.

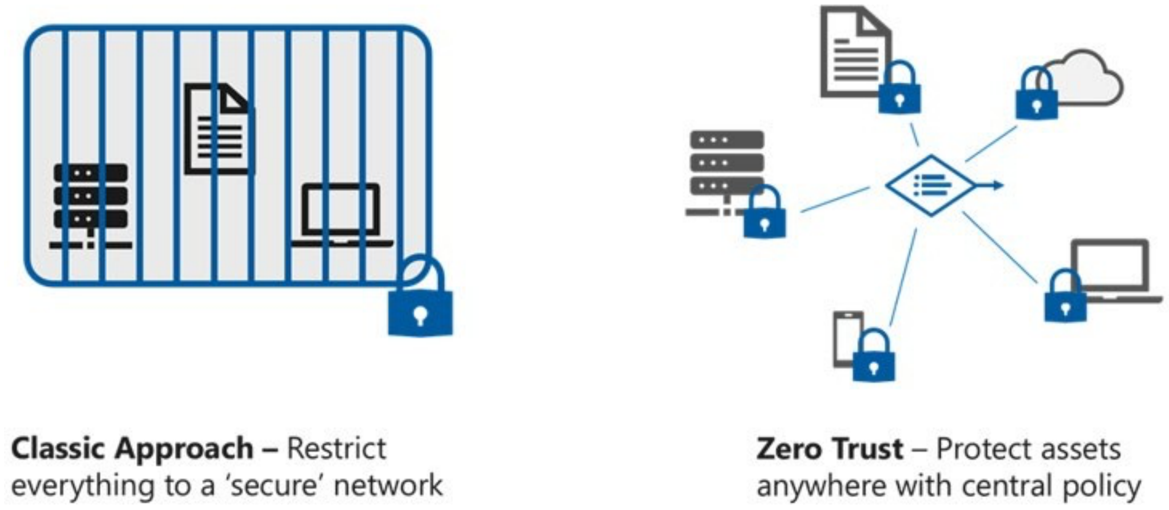
The question is – who wins? … especially, if you do nothing different?

As indicated above – Russian hackers are effectively inside the perimeter in less than a half hour. Once inside, APT groups either expand quickly, causing the loss of data, interruptions to operations, and more, or stay dormant for long periods of time.

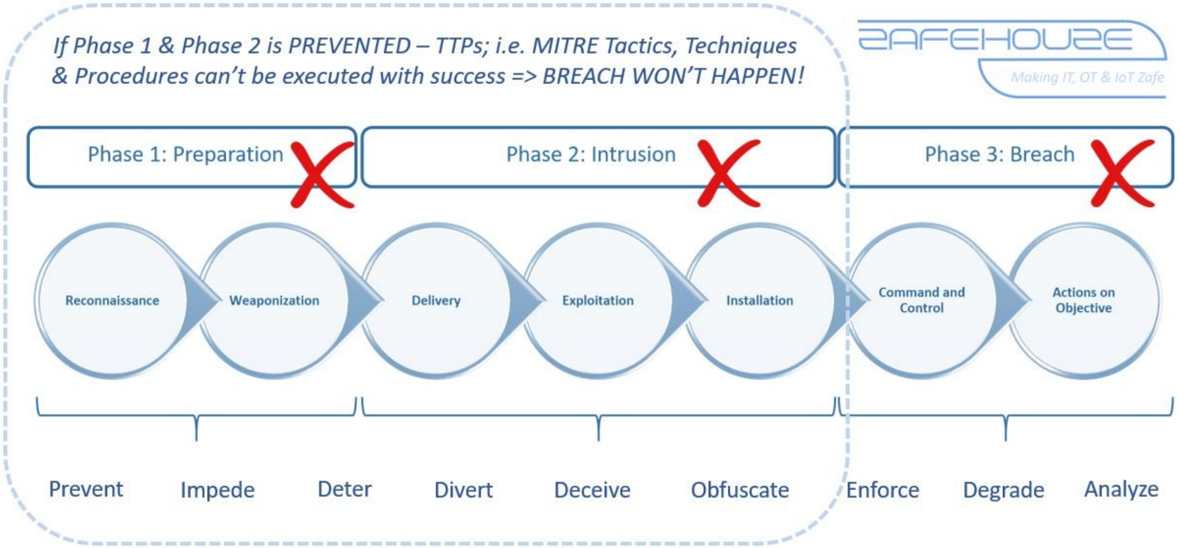
These threats require an answer, one that detection-based tools are failing to provide. New solutions, however, are making it possible to prevent cyber threats in real-time, before they can execute or access and hide in wait on a company's network.

Micro-perimeter Sealing by Focusing on Prevent & Protect

Emerging technologies have finally outstripped the capabilities of detection-based (aka Defending the Castle) tools, and Prevent & Protect platforms are now making a bigger entry and impact in cybersecurity.


Classic Approach – Restrict everything to a 'secure' network
Zero Trust – Protect assets anywhere with central policy

The most significant advance in micro-perimeter based Prevent & Protect solutions is being able to eliminate what hackers need in order to successfully action on their objectives. The technology is rooted in preventing the approx. 300 MITRE defined (based on real attacks) tactics, techniques and procedures adversaries use to do reconnaissance, weaponization, mal- and ransomware delivery, exploitation and installation. This is highly unlikely to happen in a Prevent & Protect platform – adversaries will NOT get to the Command & Control stage.



As a result, Prevent & Protect has immediate payback and ROI, eliminating post-breach wheel spinning and false alerts that are holding security teams back.

Why Detection Alone Is Not Enough

Detection-based tools, on their own, simply can't provide the level of security needed to keep an organization secure. On average, most threats go undetected for upward of 100 days or more. Because detection-based tools rely on signatures, threats that have yet to be seen readily slip through traditional defenses. A staggering 360,000 new malicious files are detected every day.

And that is on the technology side. From a financial and resource perspective, its expensive and costly to maintain and often require specialized skills and resources.

Security professionals also has to realize that. Besides the fear of a major security incident, predicting threats based on machine learning, heuristics, or file reputation provide less-than-perfect accuracy. Security teams are facing a huge volume of false alerts, more than they can realistically manage. The cost of chasing alerts, the reality of overstretched security teams, and the cybersecurity talent gap are all factors causing – in fact, forcing security professionals to rethink the balance between detection and prevention.

Breaches will remain a daily occurrence until a) cybersecurity tools are able to block new threats as quickly as they evolve og b) platforms are making it impossible for users ad adversaries to subvert the platform, whether by malice, accident or trickery.

Preparing for the Next Era of Cyber Threats

Threats that lurk on networks for sometimes months at a time are a grave danger that need addressing. Recent tales of the TRITON malware framework show just how deadly ATPs can be, and IT-teams who think they are better than most of their peers – should start focus on the question of how to prevent threats from ever entering a network in the first place.

Many organisations are starting to implements a Prevent & Protect platform strategy that will enhance security for the current threat landscape, and apply resistant capabilities to their users, devices, applications and data.

However it's worth noticing that Prevent & Protect, doesn't replace detection & response, as a balance is necessary – but with a much larger Prevent portion. Organizations can easily start supplementing the existing defense setup with Prevent & Protect platforms as these are designed to support non-disruptive implementations and with high accuracy increasingly preventing attacks before they can cause harm.

The reduction in costs and time for an IT team is worth the investment.