PROTECTION FROM THE PERFECT STORM

HOW NETWORK VISIBILITY CAN KEEP YOUR ORGANIZATION SAFE IN A DARKENING THREAT LANDSCAPE

Gigamon® | NOZOMI NETWORKS

TABLE OF CONTENTS

WELCOME TO THE CONNECTED WORLD

Connectedness is defining our lives as never before. With Internet-enabled IoT devices multiplying exponentially and 5G promising a revolution in connectivity, enterprises and organizations have to deal with the convergence between IT and OT technologies and the challenges that may arise.

CONDITIONS FOR THE PERFECT STORM

But the more connected organizations become, the more they open themselves to digital exploitation from cybercriminals on an unprecedented scale. Ominous rises in DDoS attacks, East-West infiltration and state-sponsored cybercrime are creating a darker, more dangerous threat landscape.

Could enhanced connectivity and heightened cyber-risk **combine to create a perfect storm?** This whitepaper explores the threats posed by the latest trends and how network visibility and protection tools can help to keep your organization and people safe.

CYBER-ATTACKS: BIGGER AND MORE DESTRUCTIVE THAN EVER

FLORIDA WATER BREACH THREATENS THE HEALTH OF 15,000 RESIDENTS

Attackers of a water treatment plant in Oldsmar, Florida took control of levels of sodium hydroxide, a highly corrosive substance used to balance water acidity. The attack in February 2021 briefly boosted concentrations from 100 parts per million to 11,100 ppm, until an operator averted disaster by taking immediate action to restore correct levels of the chemical. **Left unchecked, the attack would have put the health of 15,000 local residents in serious jeopardy.**

2021

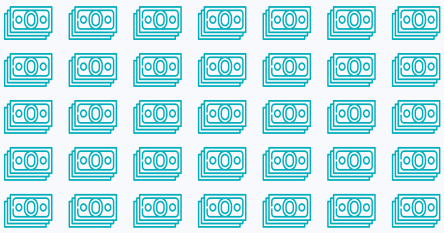
15,000

$100 BILLION US CLEAN-UP FOR STATE-FUNDED SOLARWINDS HACK

In 2020, cyber-attackers exploited security weaknesses in Microsoft, SolarWinds and VMware software to execute thousands of data breaches across NATO, Microsoft, the European Parliament, US and UK governments and many other organizations. Identified as the work of state-sponsored Russian hackers, the attack went undetected for months and caused billions of dollars in damage worldwide, including predicted costs of over **$100 billion for US companies and government departments.**

2020

$100B



WANNACRY ATTACK COSTS ORGANIZATIONS OVER $6 BILLION WORLDWIDE

In 2017, the WannaCry cyber-attack became the world's most serious ransomware incident, affecting over **200,000 computers** across 150 countries. Targets included the UK's NHS, Spain's Telefonica, FedEx in the USA and German rail company Deutsche Bahn. Across NHS England, at least 80 out of 236 trusts and 603 primary care organizations were infiltrated. Essential IT and phone systems were disabled, resulting in the cancellation of thousands of operations and patient appointments, and **costs exceeding $92 million.**

2017

200,000

THE THREAT LANDSCAPE

1. CONVERGENCE OF IT AND OT MAGNIFIES THREAT

Across industrial sectors, the convergence of **OT** *(Operational Technology)* and **IT** *(Information Technology)* environments is accelerating.

While IT cybersecurity is a well-established industry with sophisticated solutions to deter the cyber-criminals, OT cybersecurity is in its infancy, making **OT a relatively soft target for hackers.**

Once upon a time, OT was relatively isolated from the Internet and immune from cyberthreats. But, as more and more manufacturing processes are driven by IoT devices and cloud computing, the resulting confluence of technologies has ballooned the attack surface, **enabling malware to migrate seamlessly between IT and OT.**

OT breaches often go undetected for some time and lead to disrupted production, defective manufacture or interrupted services, with **evident damages to brand reputation, financial income** and **customer confidence.**

Protecting OT involves a two-prong approach:

+ **Identifying** and **eliminating** vulnerabilities in existing long life-cycle technologies
+ **Building** cybersecurity into the design of new OT systems

2. 5G ROLLOUT BRINGS GAME-CHANGING RISK

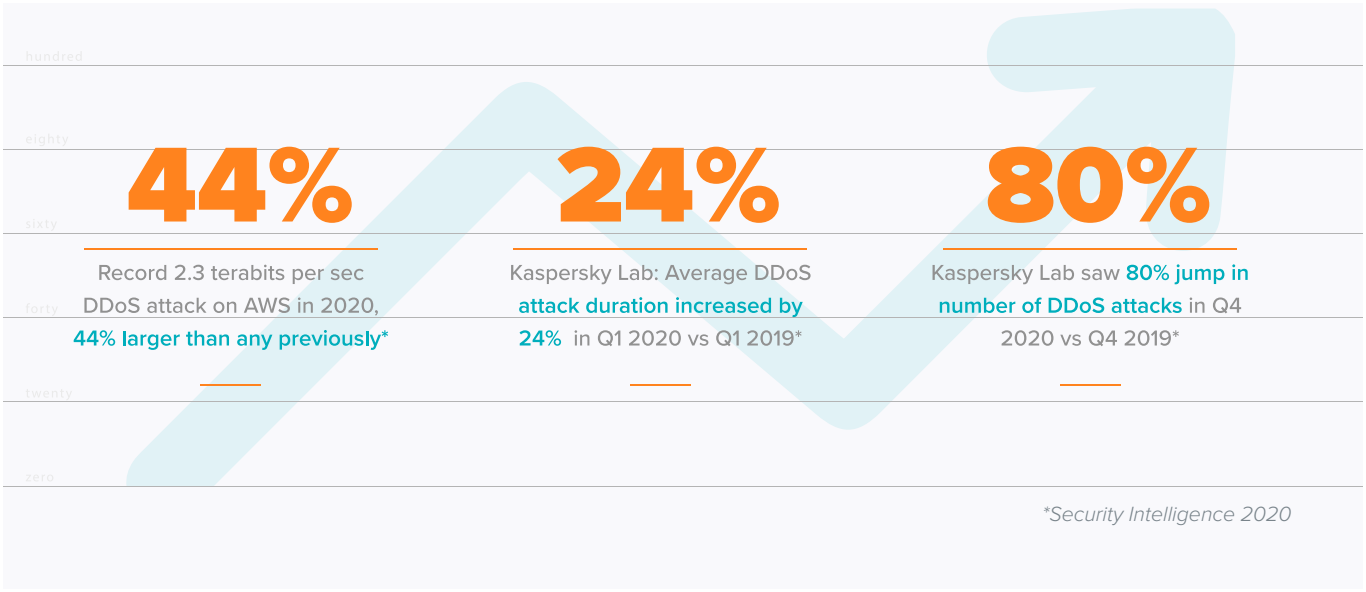
Many predict that 5G has the potential to empower malicious hackers to wreak chaos on an epic scale **for individuals, corporates and state organizations across the globe**.

5G applications will be endless and provide new ways of managing infrastructures, resources and organizations – think about smart cities, healthcare, transportation, urban planning or public safety.

But along with increased efficiency and scalability, comes the much-anticipated 'total connectivity' of 5G as the glue binding billions of Internet-enabled IoT devices that offers attackers rich opportunity to bring down essential power, health and security infrastucture. On a personal level, 5G gives hackers greater scope for infiltrating everything from personal wearables or medical devices to vehicle control and home security systems.

5G will see exponential growth in small-cell antenna deployment across urban areas, creating a vast array of 'hard' targets. Meanwhile 5G's software-defined digital routing and network management offers up a vulnerable underbelly for cyber-attackers.

3. DDOS ATTACKS: MORE SERIOUS, MORE OFTEN



DDoS (Distributed Denial of Service) attacks are growing in scale, duration and frequency. Proliferation of IoT devices is a major contributory factor and 5G's high-speed, mega-bandwidth super-connectivity creates an attractive conduit for bigger, faster, more serious DDoS attacks.

DNS amplification enables a single actor to launch a **highly effective, low-cost, large-scale DDoS attack by harnessing a huge estate of compromised IoT devices, each running one or more bots.** This net of bots (botnet) facilitates a high-volume attack which overwhelms the victim's bandwidth and disables its operations. Botnets often encompass thousands of source IP addresses, making some attacks almost impossible to block with traditional approaches.

4. STATE-SPONSORED CYBERCRIME

Attempts to influence national elections, to industrial cyber-espionage and personal attacks on the rich and influential...state-sponsored cybercrimes take different forms. Perceived as an easy alternative to well-defended military or government targets, businesses often find themselves in the crosshairs, especially if they are keepers of sensitive data, highly profitable, connected to government agencies, providers of essential public services or vulnerable to IT downtime.

Government-backed cybercrime is growing year on year. Cyberwarfare is a relatively inexpensive, low risk and highly rewarding means for nations to carry out espionage. Today, while Russia, China and North Korea are commonly seen as the usual suspects, low barriers of entry are tempting poorer countries to punch above their weight and wage war by weaponizing technology to expand their influence in the world.

5. EAST-WEST LATERAL SPREAD

Typically, cybersecurity measures focus on securing the perimeter (so called North-South protection). But today, **many attackers choose to breach perimeter defenses unseen and once inside stay dormant and undetected for months.** When the time is right, malware is then activated and dispersed laterally throughout the network, finding a path from one internal host or segment to another.

This tactic of East-West spread takes advantage of the recent trend in interconnecting IT, OT and IoT devices on the same infrastructure. With average breach detection times of 207 days, attackers inside the perimeter have ample opportunity to explore networks unchallenged, seek out weak spots and select the most valuable assets to steal, exploit or damage.

THE PERFECT STORM IS BREWING

IT/OT convergence, 5G rollout, DDoS attacks, east-west spread, state-empowered hacking: all these security threats are on the increase. Taken individually, each has the potential to cause significant harm. But **collectively, these risk factors could combine to forge attacks on a scale hither to unseen in the history of cybercrime.** This perfect storm could have devastating and dangerous outcomes for people, companies and economies on a global dimension.

207* DAYS:

Average time to identify a breach*

073* DAYS:

Average time to contain a breach*

**IBM 'Cost of a Data Breach Report' 2020*

OT/IOT VISIBILITY FOR MORE PRODUCTIVITY, MORE SECURITY AND LESS DOWNTIME

UNDERSTANDING AND SECURING YOUR OT/IOT NETWORK

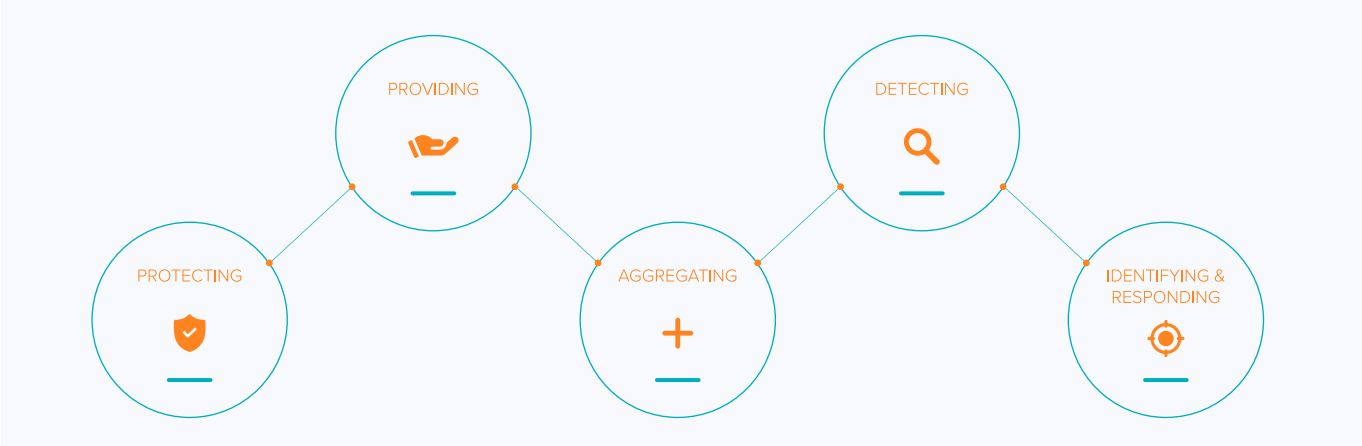
To better manage the risk of IT with OT integration, **organizations need complete visibility of their network by tracking and monitoring assets, vulnerabilities and operational controls,** as well as quickly identifying any abnormal changes.

OT networks are often populated by numerous 'ghost' devices, unknown to managers and posing a significant security threat. With such uncertainty, **it's important that IT, OT and IoT tools work together to lock down your network.** Intelligent network filtering and shaping capabilities protect your valuable OT assets by ensuring that network packets are always delivered to the right place at the right time.

HOW ORGANIZATIONS PROTECT THEIR OT WITH GIGAMON AND NOZOMI NETWORKS

Together, Gigamon and Nozomi Networks provide large enterprises and organizations worldwide with real-time network visualization and up-to-the-minute threat detection for their OT assets:

+ **Protecting industrial control networks** from cyberattacks and operational disruption through passive network traffic analysis
+ **Providing full OT asset inventory** and vulnerability assessment
+ **Aggregating data for hundreds of distributed industrial installations,** providing consolidated and remote access to your ICS data from Guardian appliances deployed in the field
+ **Detecting known and unknown threats,** enhanced with Nozomi Network's AI and machine learning technology to detect anomalies
+ **Identifying and responding** to the most **important security alerts** faster



COMPREHENSIVE VISIBILITY ACROSS IT AND OT

You can't secure what you can't see. **Visibility is fundamental for cyber resilience, detection, protection and mitigation.**

Gigamon sits between the OT business network, manufacturing, process network and tools, such as Nozomi Networks, to provide visibility regardless of medium (physical, virtual, cloud) and including East-West traffic.

In summary, **the joint solution enables comprehensive and integrated visibility across IT and OT assets.** The Gigamon Deep Observability Pipeline ensures relevant traffic is delivered to Nozomi Networks Guardian and other tools efficiently and in the format they need.

It aggregates low-volume links before forwarding, de-duplicates packets to avoid unnecessary overhead and offers easier control of asymmetric routing to collate session information for analysis by Nozomi Networks security tools.

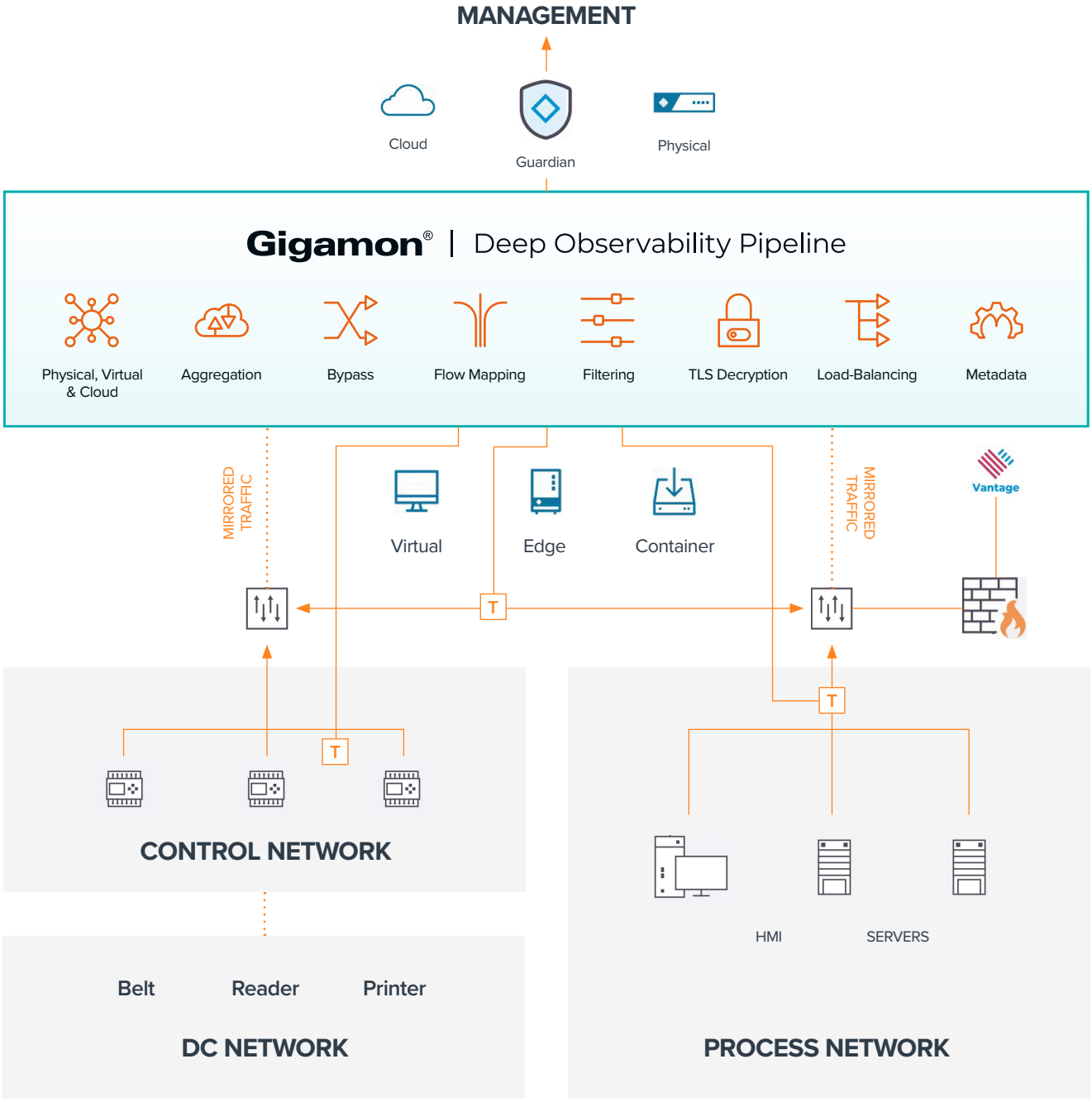
PROTECT YOUR OT WITH GIGAMON AND NOZOMI NETWORKS

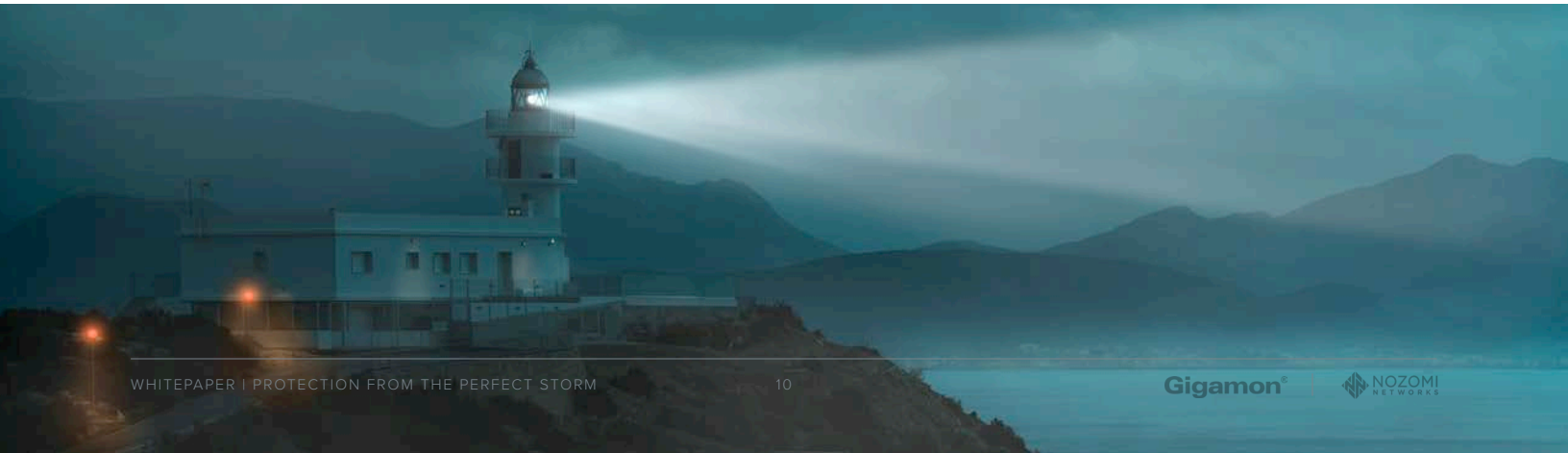
+ The Gigamon optional unidirectional taps ensure that OT product traffic is not negatively impacted
+ No matter where your device traffic is coming from, including wireless sources for remote devices, Gigamon ensures no blind spots across your network. This even includes visibility into identity and access management activity to further ensure fundamental security
+ Availability is mandatory for OT production networks. The Gigamon active/passive taps and inline bypass provide fail-open capability to ensure constant availability, including when maintenance may be required on security tools
+ If required, Gigamon can provide centralized SSL/TLS decryption of encrypted traffic, where malware likes to hide
+ Nozomi Networks catalogues operational technology assets across your network, analyzes its vulnerabilities, and baselines normal state to minimize downtime
+ Nozomi Networks provides anomaly detection of operational and security events with its unique AI and machine learning technology

In addition, the Gigamon Deep Observability Pipeline provides:

+ Load balancing to spread the volume of traffic across multiple instances of Nozomi Networks tools
+ Header stripping to make Nozomi Networks tools more efficient
+ Masking for data privacy compliance
+ Single pane-of-glass management to simplify and reduce the burden on operators and security professionals.

NOZOMI NETWORKS DEPLOYMENT WITH GIGAMON





ABOUT GIGAMON AND NOZOMI NETWORKS

Gigamon enables your organization to run fast, stay secure and innovate. We are the first company to deliver a unified deep observability pipeline on all data-in-transit.

Across your physical, virtual and cloud infrastructure, we aggregate, transform and analyze your network traffic to meet your critical performance, rapid threat detection and response needs, freeing your organization to drive digital innovation. We are trusted by over 4000 customers including 83 of the Fortune 100.

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats.

Our solution delivers exceptional network and asset visibility, threat detection and deep operational insights for OT and IoT environments. Customers rely on us to minimize risks while maximizing resilience.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831 - 4000 | gigamon.com