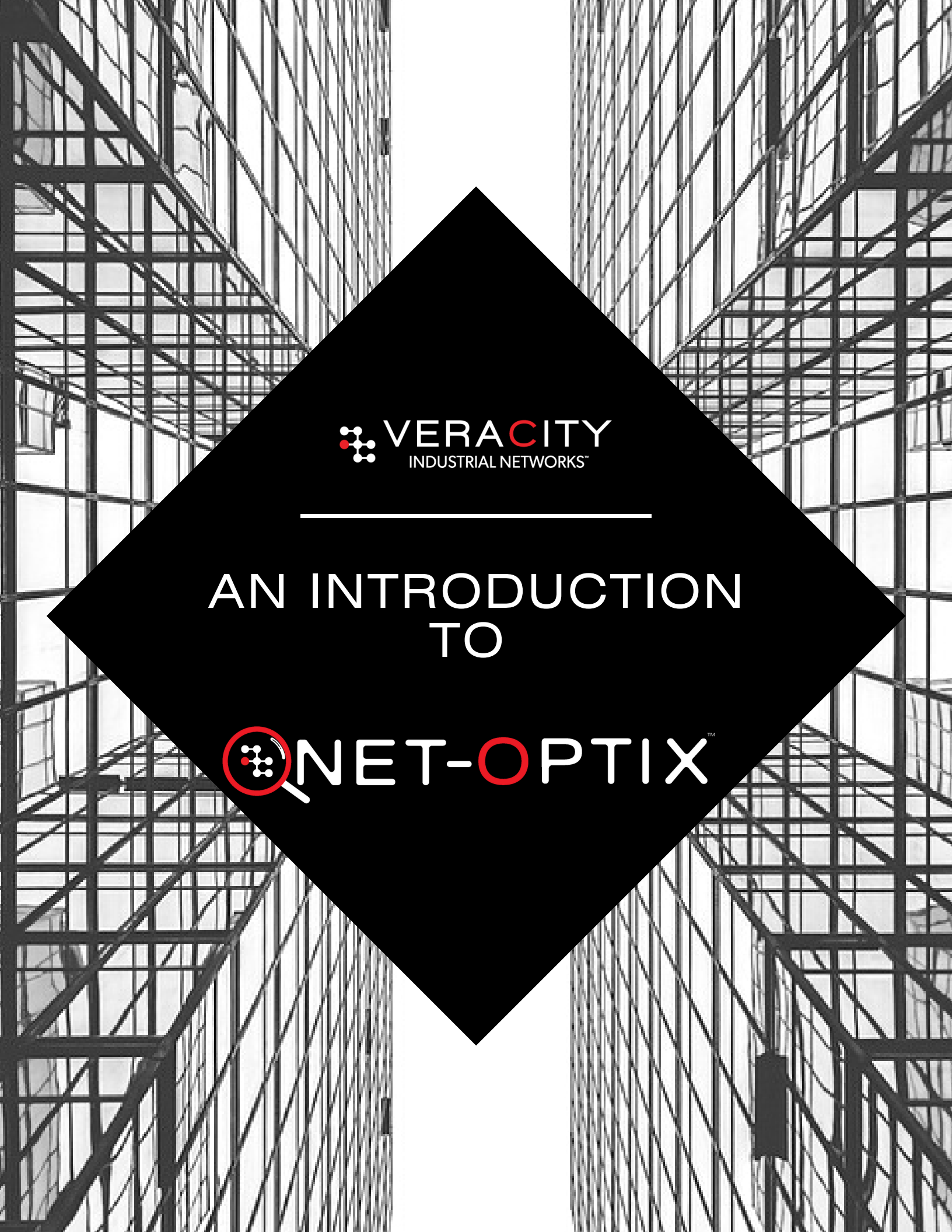
VERACITY
INDUSTRIAL NETWORKS™
AN INTRODUCTION
TO
NET-OPTIX™

OVERVIEW

In a world of continuous cyber-attacks, a tight labor market for networking professionals, and ever-increasing complexity in network design, there needs to be a simple and secure way to secure and manage your OT networks. In this paper, you will learn about Net-Optix and how it leverages software defined networking (SDN) to support a highly secure zero trust network infrastructure. At Veracity Industrial Networks, we believe that the best way to manage and secure your network is to present it to you the way you use it.

When you design a control system, you are concerned about how devices communicate with one another. You don't design your control system around network, routers, switches, subnets, VLANs, etc. With Net-Optix you define which devices talk to each other and the network handles the rest. No communication is allowed on the network which is not specifically authorized by you via a rule in Net-Optix. This is a true deny by default zero trust network.

WHAT IS NET-OPTIX?

Net-Optix takes the advantages of SDN technology and optimizes it for an industrial network. For purpose of example, think of a typical network as a neighborhood where everyone has a fenced in back yard. If you are in that yard, you can talk to anyone who is in there as well. If you want to talk to someone in a different yard, you have to go through a gate (firewall) to talk to them. But anyone in your yard is fair game. With Net-Optix, it's as if everyone is in their own room with a cell phone. That cell phone has two phone directories on it - one for speaking to and one for listening from. It also specifies which language you must speak to communicate, English, Spanish, French, Chinese, etc. If someone tries to communicate to you and they are not in the directory or speaking a different language, then it's blocked. You can only speak with people you are explicitly allowed to. Under normal circumstances, in an industrial network, if you gain access to the subnet (yard) with a device in it, you can communicate with that device. With Net-Optix, unless you are given access to a device, you may not communicate with it.

WHAT IS SOFTWARE DEFINED NETWORKING?

Software Defined Networking (SDN) allows the definition of point-to-point communication between devices programmatically instead of fixed paths based on network topology. This flexibility makes SDN ideal for managing dynamic networks such as cloud services, making existing networks more efficient by optimizing data flow in real time, and even reducing energy consumption at large data centers by managing network traffic. SDN became even more prevalent with the COVID-19 pandemic and a rapid shift to work from home and many devices remotely connected. The ability to manage the ever-changing networks while still maintaining security became critical and the adoption of SDN for IT networks has taken large strides forward since then.

RULES AND FLOWS

Our paradigm is referred to as deny by default. Net-Optix accomplishes this by having the user create a set of rules that the network must follow. Without a rule in place, communication is blocked. For example, if you want a PLC to speak with an HMI via Ethernet/IP you have to tell the system that it is allowed. These rules then become data flows in the system that the network switches enforce. You can create rules that are point to point between devices or more open rules that allow traffic to flow freely which can be useful if you are making many changes to your network. Net-Optix also has the ability to watch existing traffic to learn what is typical traffic and create rules based on that. These rules are then to be verified by the administrator making setup on existing networks much quicker.

WHAT IS ZERO TRUST NETWORK ACCESS

Zero Trust Network Access (ZTNA) is an approach for the design and implementation of networks. The main concept of ZTNA is that no device on the network can be trusted, even if it is connected to a managed network. Most networks have fenced off segments like subnets and VPNs that once inside, a device has free reign to communicate with other devices in that area. With ZTNA, each communication path must be explicitly allowed.

THE CONTROLLER AND SWITCHES

The Net-Optix solution requires two components, the Net-Optix controller (software) which runs on a computer (server, virtual machine) and SDN enabled network switches. Many vendors have SDN enabled switches. We recommend switches from Dynics and Schweitzer Engineering Laboratories (SEL), but many others are also compatible. The controller contains all of the rules for the network. The controller also monitors the network and stores statistics about the network traffic. The switches do not know any of the rules when they are first put into service.

When a switch sees communication for which it has no rule, it queries the controller to see if that traffic is allowed. The controller then either confirms or denies that communication flow and the switch with allow or continue to block the data. A beneficial side effect of this is if a device happens be moved from one switch to another, the network automatically rebalances. No changes required to make it work on your part.

BENEFITS OF NET-OPTIX

As you sort through all of the information above, it's helpful to understand where you can get the most out of Net-Optix.

1

CONSOLIDATED NETWORK MANAGEMENT

With 95% of all network changes being performed manually, having all of your industrial devices and switches managed via a single tool how you think about them will save you time as well as reduce inadvertent errors.

2

INCREASED NETWORK VISIBILITY

70% of network policy violations are due to human error. With Net-Optix, you can easily see the data flow through your network so you can easily identify and eliminate network errors.

3

ROBUST / INHERENT NETWORK SECURITY

With frequent cyberattacks by independent and state sponsored actors, you want the tightest control over your industrial networks, but need to balance that with the cost of managing those networks. Net-Optix provides a deny by default posture to physically connected devices as well as easy collection and analysis of network traffic from the controller. This provides a robust security solution for all of your OT devices.

4

PROACTIVE APPROACH TO MANAGING DOWNTIME (HENCE RELIABILITY)

A typical OpEx network budget has 75% of it dedicated to network visibility and troubleshooting. Net-Optix has automated networking processes allowing changes to be carried out faster and more accurately without having to take the system down. Net-Optix™ also eliminates the necessity of many human interventions for network changes, avoiding costly errors and downtime.

CONCLUSION

As you can see, Net-Optix is a completely new way to manage and secure your industrial OT network using the same ethernet you use today. Anything that runs on your ethernet network today will run on a Net-Optix managed network. Net-Optix simplifies network management, provides robust deny by default security and supports a zero-trust network architecture. The ease of management will allow large companies to reduce the pressure on over-extended IT staff by simplifying the network architecture. Net-Optix also allows small companies to have a robust OT cyber-security solution that can be managed themselves and might be out of reach otherwise. We invite you to learn more about Net-Optix by visiting our website at www.veracity.io.