Security of Things: Dealing properly with the explosion of connected devices

Published 16 February 2021

Team8
Global venture group

Technology advances are fueling Internet of Things (IoT) device connectivity that is driving the Industrial Economy to digitize and unlock new business value. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and the stakes are raised. Cyber threats move from data to people – disrupting supply chains and infrastructure critical to health and safety.

Fueled by advancements in lower-power compute and communication, there's an explosion of connected devices, with the International Data Corporation (IDC) predicting there will be 55.7 billion connected devices worldwide by 20251. Entirely new devices are coming online, while old technologies that have been online for years under the radar, such as in manufacturing, remain vulnerable. The 5G spectrum enables ubiquitous connectivity because it expands the frequencies and bandwidth for data transfer. As critical infrastructure and manufacturing sectors go online, spurred by advancements in smart machinery, IT and OT networks are converging. Legacy systems are being connected to the Internet, along with Industrial IoT (IIoT) technologies like smart meters, automated asset distribution systems, and self-monitoring transformers, or production lines and farm equipment outfitted with sensors. Done right, IT-OT convergence unlocks tremendous business value - enabling improvements in operational efficiency, performance, and quality of service. But new threat types expose the need for better endpoint defense. Novel attack patterns and approaches are cropping up every day - ransomware, cryptojacking, new kinds of advanced persistent threats (APTs) - that require a shift from signature-based detection to more advanced and dynamic behavioral-based techniques. Enterprise security teams simply can't stop them all and a lack of asset visibility and management, and security updates compounds the problem. Successful attacks go beyond data breaches -- widespread disruption and harm, both physically and economically, is often the attacker's endgame.

Impact - Although there has been an evolution in this field over the last few years, the shift in ransomware from focusing on data and IT infrastructure, to disrupting OT environments is accelerating and is perhaps the single greatest threat facing Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) today. Furthermore, as 5G proliferates, everything will become "a thing" and even in domains like OT, the concept of networks will dramatically change. IT security controls can't adapt to work in OT environments. To mitigate the risk of threats that cross the IT/OT boundary, new models and mindsets are needed.

Solution Categories - Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP), Vulnerability Management, IoT Security, Deception, Managed Detection and Response (MDR), User Behavior Analytics, OT Security, Antivirus.

Perspectives:

- **Defender's Perspective** - *The global supply chain is immense and growing with more connectivity and automation in the Internet of Things driving efficiencies and improved performance throughout. Concurrently, this growing web of interconnectivity has the potential to make our production systems more fragile because one change can have a cascading and tangible impact in the overall physical world. The ability to adapt cyber techniques, such as security monitoring, visibility, and remediation, to a totally different environment of inter-connected devices operating our physical manufacturing world, will be foundational to creating a safe and resilient global supply chain. The industry must grow beyond managing this retroactively and manually via spreadsheets toward a real-time, always available and highly precise, layered network design approach.*
  - Jim J. Labonty, Head of Global Automation Engineering, Pfizer
- **Team8's Attacker Perspective -** IoT devices are prime targets for attackers. These devices contain all the hallmarks attackers like - they are black boxes, are rarely designed with security in mind, and use embedded code that isn't updated and is full of security holes that are usually not patchable. Adding connectivity to the corporate network transforms IoT into the perfect entry point for the sophisticated APT.

In our next blog, we will cover the Perimeterless World.

Author who has contributed to this blog: ***Ben Borodach****, VP, Strategy & Operations at Team8.*

The views expressed in this blog are those of Team8, any reference to "we" should be considered the view of Team8 and not necessarily those of WisdomTree Europe.

Team8 is a global venture group with deep domain expertise that creates companies and invests in companies specializing in enterprise technology, cybersecurity, and fintech. Leveraging an in-house, multi-disciplinary team of company-builders integrated with a dedicated community of C-level executives and thought leaders, Team8's model is designed to outline big problems, ideate solutions, and help accelerate success through technology, market fit and talent acquisition. For further information, visit www.team8.vc.

1 https://www.idc.com/getdoc.jsp?containerId=prAP46737220

Related blogs

+ Cloud security: A necessary component in digital transition planning

+ Introducing cybersecurity the megatrend of the 2020s

Related products

+ WCBR - WisdomTree Cybersecurity UCITS ETF - USD Acc

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an oer for sale nor a solicitation of an oer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.