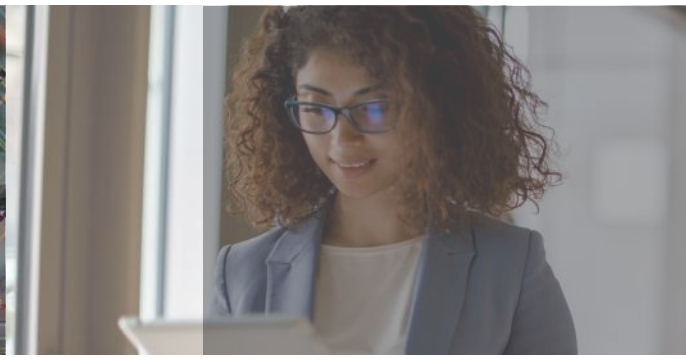
Software Security Across the Intelligent Edge

SECURITY MUST COVER EVERY SINGLE ENDPOINT DEVICE, THROUGH THE ENTIRE LIFECYCLE

WIND

Three Dynamics Impacting Security



Two billion PCs and 42 billion connected Internet of Things devices will be part of our world by 2025.

Nearly every device will work through the cloud in some way, and 80% of the data we all create, consume, and are part of will go through the 5G cloud.However, currently a mere 11.5% of all corporations are digitally transforming successfully,[1] which means that a majority of organizations still face huge challenges to their ability to thrive in the coming digital-centered world.

Security is foremost among those challenges. Imagine the complexities of designing security protocols in this new and evolving world. More than half of technology leaders see multiple security concerns directly connected to digital transformation initiatives, including increased cybersecurity risks (53%), cybercriminal sophistication (56%), and increased threat surface (53%). These threats are compounded by another concern shared by 40% of CISOs, CTOs, and CIOs: namely, the problems caused by rigid technology infrastructure—the sort of infrastructure tightly associated with embedded systems.[2]

40% of CISOs, CTOs, and CIOs are concerned about the problems caused by rigid technology infrastructure—the sort of infrastructure tightly associated with embedded systems.

Consider three dynamics that are changing constantly around us, detailed in the following pages.

1 Forbes/Inc.Digital
2 media.nominet.uk/wp-content/uploads/2019/07/Cyber-Security-in-the-Age-of-Digital-Transformation.pdf

EMERSON
Network Power

HOW DID EMERSON MAKE ITS OVATION DCS MORE CONNECTED *AND* MORE SECURE?

With machine learning, full-system simulation, and Wind River.

The Ovation™ distributed control system (DCS) platform evolves with changing technology to enhance power plant reliability and has been designated a Qualified Anti-terrorism Technology by the Department of Homeland Security (DHS) under the U.S. SAFETY Act.

Emerson uses Wind River® solutions for the entire Ovation lifecycle: accelerating development with virtual hardware, running VxWorks® as the underlying OS for the DCS, simulating the entire physical environment of the plant, and—critically for operational security—modeling control system operation. These lifecycle solutions provide a baseline for system parameters and performance that can help identify anomalous behaviors before they impact production systems.

WIND™

Dynamic #1

THE VALUE OF DATA HAS BECOME MORE DYNAMIC THAN THE .1% OF ITS LIFECYCLE IT WAS DESIGNED FOR

The act of putting one core focus on a device is unlikely to be the wave of the future. The value of information is far more dynamic in a digitally centered world. The fact that 75% of leaders of major corporations say they have 200% less time than before to make decisions[3] illustrates the need to have data rapidly available to support decision-making.

Data is more than ever dynamic in nature, in part because it originates from thousands or millions of different places, often coming in at the same time. What that data can be used for is driven by the moments that matter.[4] That moment may matter in only .1% of the device's lifetime—if we build it based only on the original design. In a dynamic world, the value of the information gathered in the other 99.9% of the device's life could be valuable for other parts of the data infrastructure. In a connected world, data has multifaceted value, often reaching far beyond the core design.

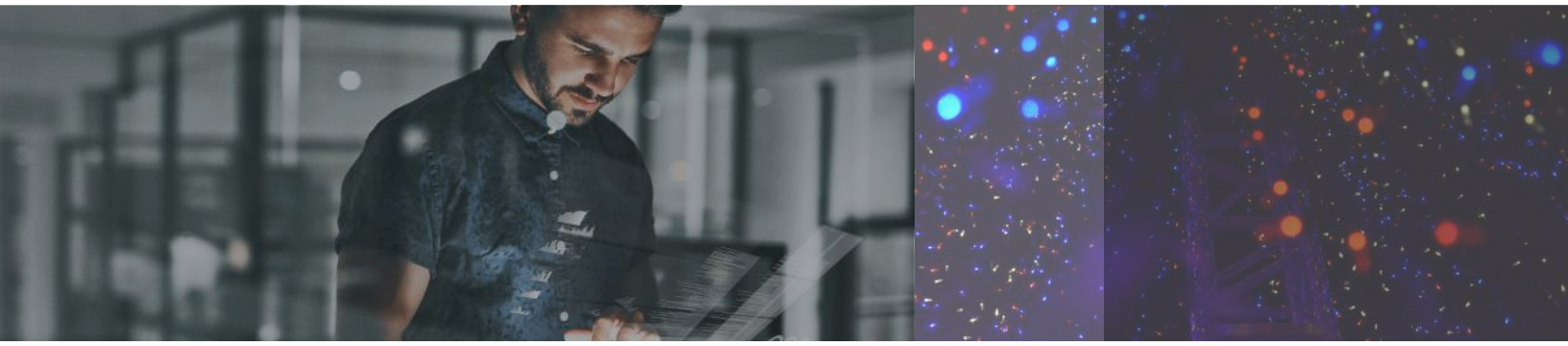
The significance of the data revolution underway in devices is underscored by the struggle to secure that data, with more than half of all IoT devices vulnerable to medium- or high-severity attack and 98% of all IoT device traffic—including medical device traffic—left unencrypted.[5] Specific classes of data require nuanced consideration of privacy implications, as the dynamic nature of data means it can inadvertently transform into Personal Identifiable Information (PII) subject to diverse regulations around the globe.[6]

> Think of data as having a network effect: The more devices connect in real time, the greater the value of the information and data to the organization.

98%

of all IoT device traffic—including medical device traffic— is left unencrypted.

3 Forbes/Inc.Digital
4 The Digital Helix
5 threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609
6 www.varonis.com/blog/data-privacy

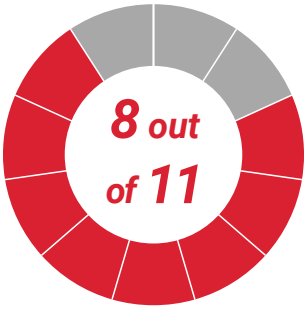


Dynamic #2

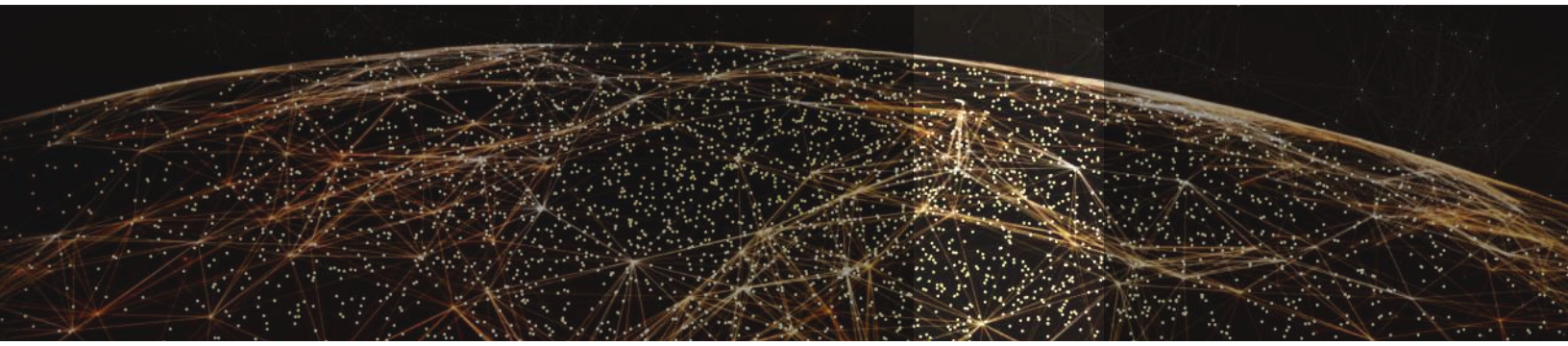
SECURITY HAS TO WORK ACROSS PARTNERSHIPS (INSIDE AND OUTSIDE OF ORGANIZATIONS)

Imagine you have a component inside an industrial machine managing complex power exchanges across a power grid. This device could also be in 10 other ecosystem partners' products that are all working together. You want to know how that component is performing and also how the overall data ecosystem is delivering value-added insights that can be used in real time. You might want to see how that data could be orchestrated in different ways going forward. Such opportunities for knowledge exist in the energy, distribution, medical device manufacturing, aviation and defense, and other sectors where the power of the device goes beyond its core functionality.

Think of data as having a network effect: The more devices connect in real time, the greater the value of the information and data to the organization. Given the digital transformation strategies researched by Forbes/Inc.Digital, 8 out of 11 industry leaders were convinced that the power of data in a digitally transforming world was going to help define their future success. And the more partners in the ecosystem, the greater the potential power of the data. That argument may sound abstract, but recent work by IBM's Cognitive Systems group shows that the best and most economically effective AI comes from running all four AI formats (machine, deep, visual, and natural language) simultaneously: multiple data sets working together in real time. With AI infused into nearly everything, the power of data partnerships is vast, delivering far more value than just one ecosystem can provide.



8 out of 11 industry leaders were convinced that the power of data in a digitally transforming world was going to help define their future success.



Dynamic #3

BY DEFINITION, THE NEW DIGITAL FUTURE IS NOT CLEAR. CAN YOUR SECURITY HANDLE THAT LEVEL OF AMBIGUITY?

Ambiguity is our new digital future. Transformation is difficult, and transformation of our security design and delivery is just as difficult. However, major corporations (Fortune Global 2000 companies) that are thriving in their digital transformations are exponentially more confident about their futures because they are building environments to handle that ambiguity.

Our volatile, uncertain, complex, and ambiguous (VUCA) world requires us to think about new ways to be secure. Being able to lean into this reality is essential, because the rate of effective digital transformation (CAGR) has been slow: 11.5% since 2013.[7] What we need to design for is a future of being able to secure data and enable the insights from that data to be used in real time and, ultimately, shared across multiple ecosystems.

In the pre-digital world, the idea of security was well understood. Now the constructs needed to build in security must adapt daily, just as AI, the cloud, and 5G do. A future of intelligent edge devices designed for an adaptive world must be the prime goal for developers and applications management.

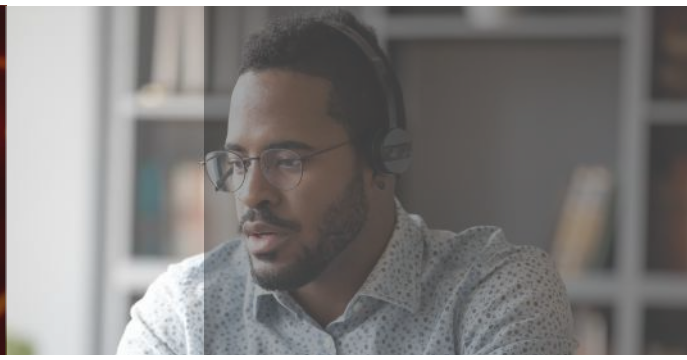
Think through three simple questions to see how well you are organizing for this new digital world:

1. Are you increasingly working with new design security requirements for your devices?
2. Is the VUCA world we live in seen as an asset by the organization, and do security requirements hold you back or accelerate your ability to thrive?
3. Is your core security strategy likely to be very different in five years' time, as you digitally transform as an organization?

> "By using a simulation model (VxWorks Simulator) in parallel with its equivalent embedded hardware, we can have it serve as the gold standard and potentially be able to detect anomalous behavior before it actually manifests itself as a system failure."
>
> **—Rick Kephart,**
> *Vice President, Software Development, Emerson*

7 Inc.Digital

The Edge



We are building and securing the new digital reality during two seismic shifts: a massive transition toward edge compute, specifically in the way enterprise data is captured, processed, and stored; and a generational shift in the workforce that will develop and operate the mission-critical intelligent connected systems of the future.

In 2018, only 10% of enterprise data was captured and processed outside of a traditional data center; by 2025 that number will exceed 75%.[8] Meanwhile, in 2020, Millennials became the largest percentage of the workforce.[9]

EXPERIENCE MATTERS

The generation of developers and operators who are most experienced with legacy embedded systems are approaching retirement age, while a much smaller pool of embedded engineering talent is waiting in the wings. Eighty-two percent of executives reported a shortage of qualified technical candidates, with 60% of companies identifying electrical engineering jobs as the most difficult to fill.[10] Experience with IoT systems is vital to keeping them secure, as programming errors are a leading cause of vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database: "Operating systems and firmware suffer the most attacks: programming errors in these pieces of software and weak access control or weak authentication enable attacks at the lowest software-based level but the undisclosed vulnerabilities often affect these pieces of software as well."[11]

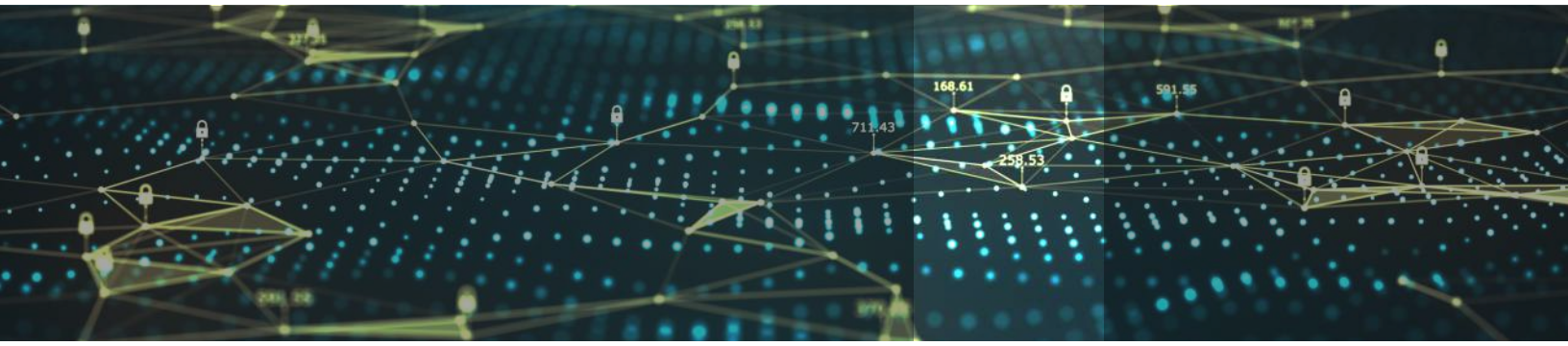
TOSHIBA

HOW DOES TOSHIBA SECURE PERSONAL DATA IN A MARKET WHERE CYBERCRIME WILL COST COMPANIES $5.2 TRILLION OVER THE NEXT FIVE YEARS?

60% of 2019 breaches involved vulnerabilities for which a patch was available but not applied. Wind River Linux helps Toshiba change the odds.

In 2019 there were more than 45 CVEs logged per day. The electronics and IT conglomerate Toshiba, recognizing the risks CVEs pose to the personal data it holds, partners with Wind River to secure its data and reduce costs. The Wind River security team is constantly monitoring the CVE database for potential issues affecting VxWorks and all the Wind River Linux kernel features, user packages, and tools. In addition, the team monitors notifications from U.S. Government agencies and organizations such as NIST and US-CERT, as well as public and private security mailing lists for alerts.

8 www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders
9 Forbes/Inc.Digital
10 www.semi.org/en/node/581
11 www.cse.psu.edu/~pdm12/cse597g-f15/readings/cse597g-embedded_systems.pdf



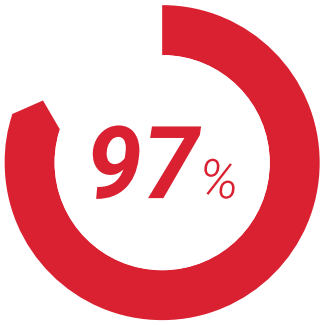
ACCESS IS EVERYTHING

IoT and other devices at the edge are often physically accessible, exposed to a range of hardware-based attacks that are not common in more controlled environments. Risks are compounded by after-market availability of such systems for purchase, enabling cybercriminals to develop attacks at their leisure. Devices that are small, individually owned, and not built with security in mind may not be updated regularly and can provide easy access to the broader network to which they are connected. In a 2018 Ponemon Institute survey, 97% of risk management professionals stated that they believed that unsecured IoT devices could be open to a "catastrophic" security breach.[12]

Three questions to ask as you near the edge:

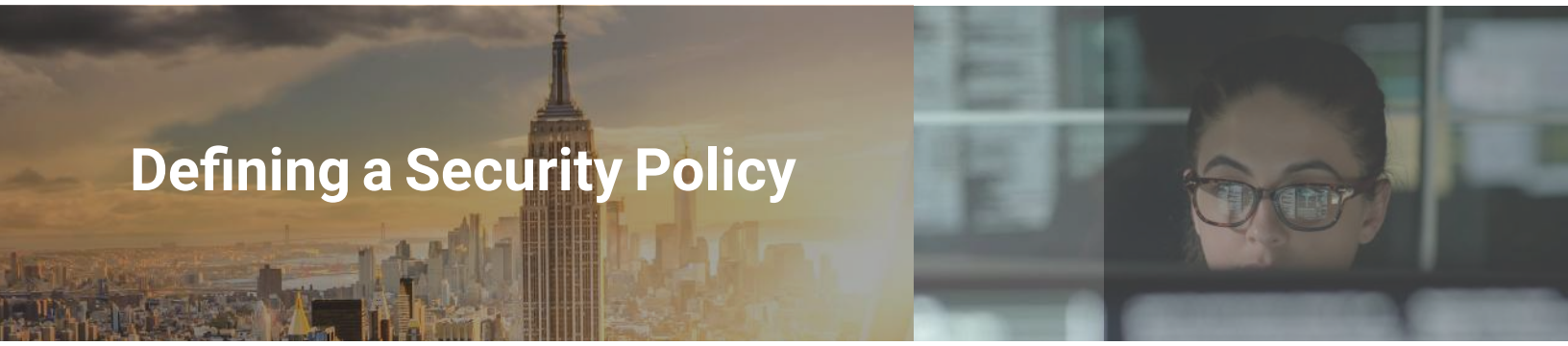
1. Do you have access to engineering talent with the diverse set of skills required for the development, deployment, and maintenance of today's IoT devices and related systems?
2. Do you have a digital experience strategy that will ensure that your devices are readily operable by a majority Millennial and digital-native workforce?
3. Do you have a complete understanding of the supply chain your device fits into—including your software supply chain—and encompassing after-market suppliers?

> "There are updates that happen every single day about potential security exposures. We have a team here at TGCS that focuses on that; we partner with Wind River to make sure that the known risks are identified and that we respond quickly for our retailers."
>
> **—Gregg Margosian,**
> *COO, Toshiba*



97% of risk management professionals stated that they believed that unsecured IoT devices could be open to a "catastrophic" security breach.

12 sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf



Defining a Security Policy

49% of design teams consider defining a security policy one of their most important projects.

The CIA Triad is an industry-standard model that guides development of a security policy, defining the necessary principles needed to protect a device from unauthorized access, use, disclosure, disruption, modification, or destruction.

The CIA Triad is based on the following three principles:

- **Confidentiality** implementations are used to protect the privacy of data in IoT systems. This includes data in motion, data at rest or stored on the device, data being processed by the device, and data passing to and from the device.
- **Integrity** implementations ensure that the device data has not been modified or deleted by an attacker. This includes data being generated or consumed by the embedded device as well as its programming data (the operating system, applications, configurations data, etc.).
- **Availability** implementations are used to ensure that an IoT device performs its intended function. This means an attacker cannot change a device's intended functional purpose. This is of paramount importance to devices that perform life- or mission-critical tasks.

Project teams determine which components of the CIA Triad are required based on risk exposure, regulatory requirements, and IP protection needs balanced against cost, performance, and the device deployment operational environment. There is no single silver-bullet solution for protecting a device or system from all possible attacks. Rather, a layering approach that uses different mitigation controls delivers a multifaceted protection shield and, ultimately, a much stronger cybersecurity implementation.

There is no single silver-bullet solution for protecting a device or system from all possible attacks. Rather, a layering approach that uses different mitigation controls delivers a multifaceted protection shield and, ultimately, a much stronger cybersecurity implementation.

Questions to Ask As You Near the Edge

ARE YOU SUCCESSFULLY TRANSFORMING OR INADVERTENTLY EXPANDING YOUR THREAT SURFACE?

Five Security Questions to Answer As You Digitally Transform

As the world of embedded systems and the operational technology (OT) domain become increasingly digital, and as the lifecycle of devices moves beyond fixed-function and break/fix, fundamentally different strategies will be required to securely design, deploy, orchestrate, and adapt the next generation of mission-critical systems.

1. Is your security strategy focused primarily on end points or is it a truly system-level approach encompassing the cloud and providing a chain of custody for the data at the heart of digital transformation?
2. Do you have an established methodology for the simultaneous development of functionality and the security elements of your IoT systems, and if so does this methodology support the proliferation of threats that come with digital transformation?
3. Does your system architecture support efficient management of and updates to edge devices from deployment onward, anticipating the next generation of security threats and affording the flexibility required to ensure security across decades in the field?
4. Do your existing enterprise security tools recognize the diverse industry-specific protocols of your IoT systems and, if not, how will you detect intrusion over these protocols as digital transformation accelerates enterprise and edge convergence?
5. Does your enterprise security perimeter encompass devices deployed to the field and, if not, how will you ensure secure connectivity between these devices and the enterprise?

IS YOUR DATA IN THE CLEAR?

Three Security Questions to Answer As You Build and Deploy Data-Centric Devices

Device manufacturers must embrace the new digital paradigm of interconnectivity and data dynamism, designing in security not only for data in memory or storage but also for data passing through a system or over a network, and for the keys used to encrypt that data. Meanwhile, they must also ensure that software and hardware are hardened against tampering that compromise data integrity. Does your organization have a comprehensive approach to data security and privacy, or are your development efforts focused exclusively on end-point security?

1. Will systems you develop be part of the 98% of IoT devices sending data in the clear, or will you encrypt your data?
2. Do you have a clear understanding of the deployment environment into which your systems will be fielded, the attacks that environment may be subject to, and how the deployment environment may or may not introduce privacy considerations?
3. Do you have a testing strategy to address the full range of threats to data security?

Why Wind River

For nearly 40 years, Wind River has helped the world's leading technology companies power generation after generation of the most secure devices in the world.

And in a new era of autonomy and connectivity, Wind River continues to lead the way. Our software runs the "can't fail" computing systems of the most important modern infrastructure, including mission-critical aircraft, rail, automobiles, medical devices, manufacturing plants, and communications networks.

Our technology is in more than 2 billion devices throughout the world and is backed by our industry-leading professional services, award-winning customer support, and robust partner ecosystem.

Our customers can leverage state-of-the-art, robust, and reliable software platforms that protect privacy, maintain data integrity, and ensure availability with seamless system integration and developer collaboration. Our platforms serve as a trusted foundation so you can innovate securely and protect your device against current and future threats.

Our proven secure-by-default platforms and deep industry experience allow you to build your device with confidence on industry-leading technology, knowing private data is protected, critical systems are isolated, and system management is securely built into the ecosystem. This allows you to reduce risk, speed up iterations, and deploy with confidence throughout the product lifecycle.

Our platforms serve as a trusted foundation so you can innovate securely and protect your device against current and future threats.

Wind River is a global leader in delivering software for the intelligent edge. Its comprehensive portfolio is supported by world-class professional services and support and a broad partner ecosystem. Wind River is accelerating digital transformation of critical infrastructure systems that demand the highest levels of safety, security, and reliability.

WIND™

Appendix

Security Worksheet for the New Digital World

ARE YOU ORGANIZING FOR A NEW DIGITAL AND VOLATILE, UNCERTAIN, COMPLEX, AND AMBIGUOUS (VUCA) WORLD?

1. Are you increasingly working with new design security requirements for your devices?
2. Is the VUCA world we live in seen as an asset by the organization, and do security requirements hold you back or accelerate your ability to thrive?
3. Is your core security strategy likely to be very different in five years' time, as you digitally transform as an organization?

ARE YOU SUCCESSFULLY TRANSFORMING OR INADVERTENTLY EXPANDING YOUR THREAT SURFACE?

1. Is your security strategy focused primarily on end points, or is it a truly system-level approach encompassing the cloud and providing a chain of custody for the data at the heart of digital transformation?
2. Do you have an established methodology for the simultaneous development of functionality and the security elements of your embedded systems and, if so, does this methodology support the proliferation of threats that come with digital transformation?
3. Does your system architecture support efficient management of and updates to edge devices from deployment onward, anticipating the next generation of security threats and affording the flexibility required to ensure security across decades in the field?
4. Do your existing enterprise security tools recognize the diverse industry-specific protocols of your edge systems and, if not, how will you detect intrusion over these protocols as digital transformation accelerates enterprise and edge convergence?
5. Does your enterprise security perimeter encompass devices deployed to the field and, if not, how will you ensure secure connectivity between these devices and the enterprise?

IS YOUR DATA IN THE CLEAR?

1. Will systems you develop be part of the 98% of IoT devices sending data in the clear, or will you encrypt your data?
2. Do you have a clear understanding of the deployment environment into which your systems will be fielded, the attacks that environment may be subject to, and how the deployment environment may or may not introduce privacy considerations?
3. Do you have a testing strategy to address the full range of threats to data security?

DO YOU HAVE THE NECESSARY KNOWLEDGE TO SUCCEED AS YOU NEAR THE EDGE?

1. Do you have access to engineering talent with the diverse set of skills required for the development, deployment, and maintenance of today's IoT devices and related systems?
2. Do you have a digital experience strategy that will ensure that your devices are readily operable by a majority Millennial and digital-native workforce?
3. Do you have a complete understanding of the supply chain your device fits into—including your software supply chain—and encompassing after-market suppliers?