DEDICATED COMPUTING | POWERING THE WORLD'S MOST IMPORTANT DEVICES®

Security-First Mindset Drives Both Performance and Profits

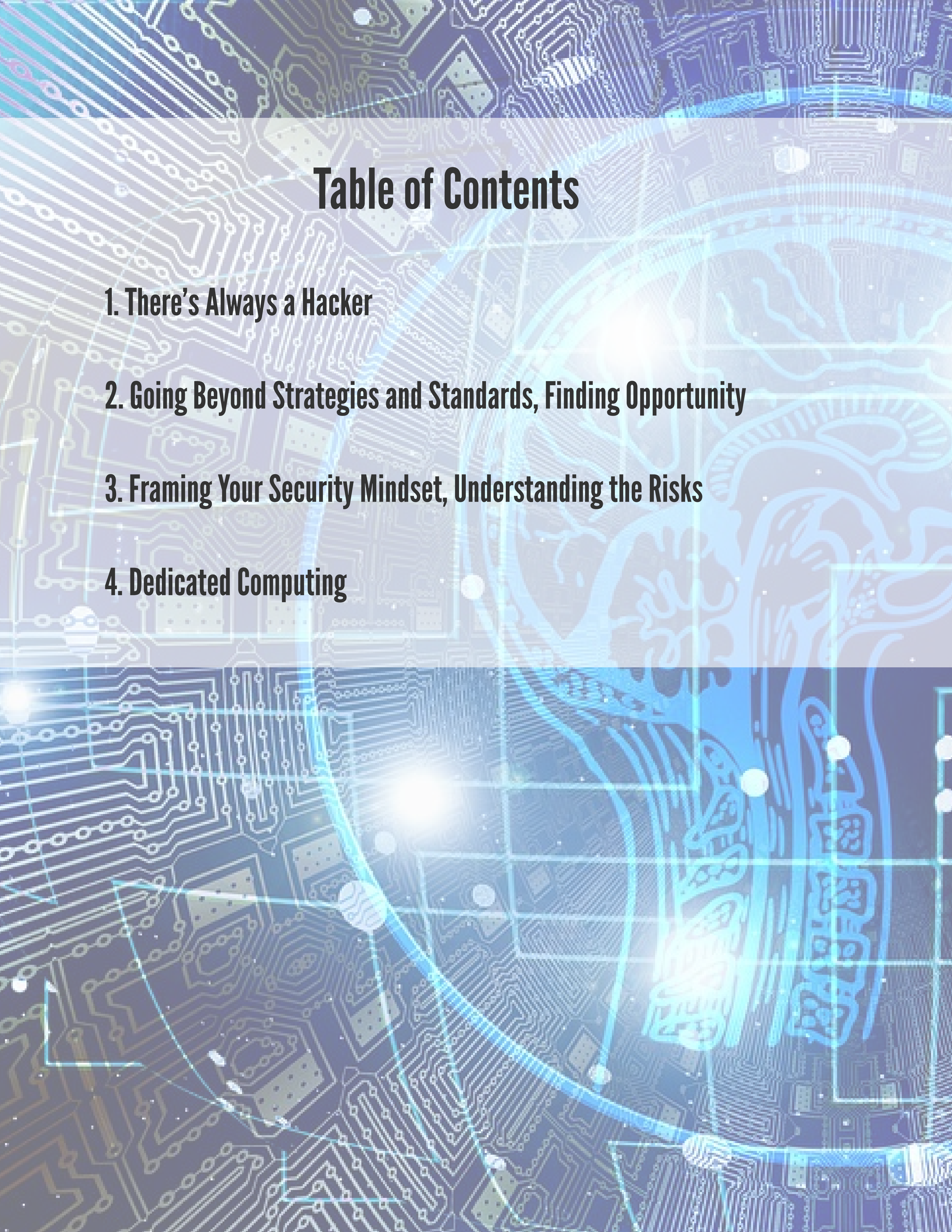


Table of Contents

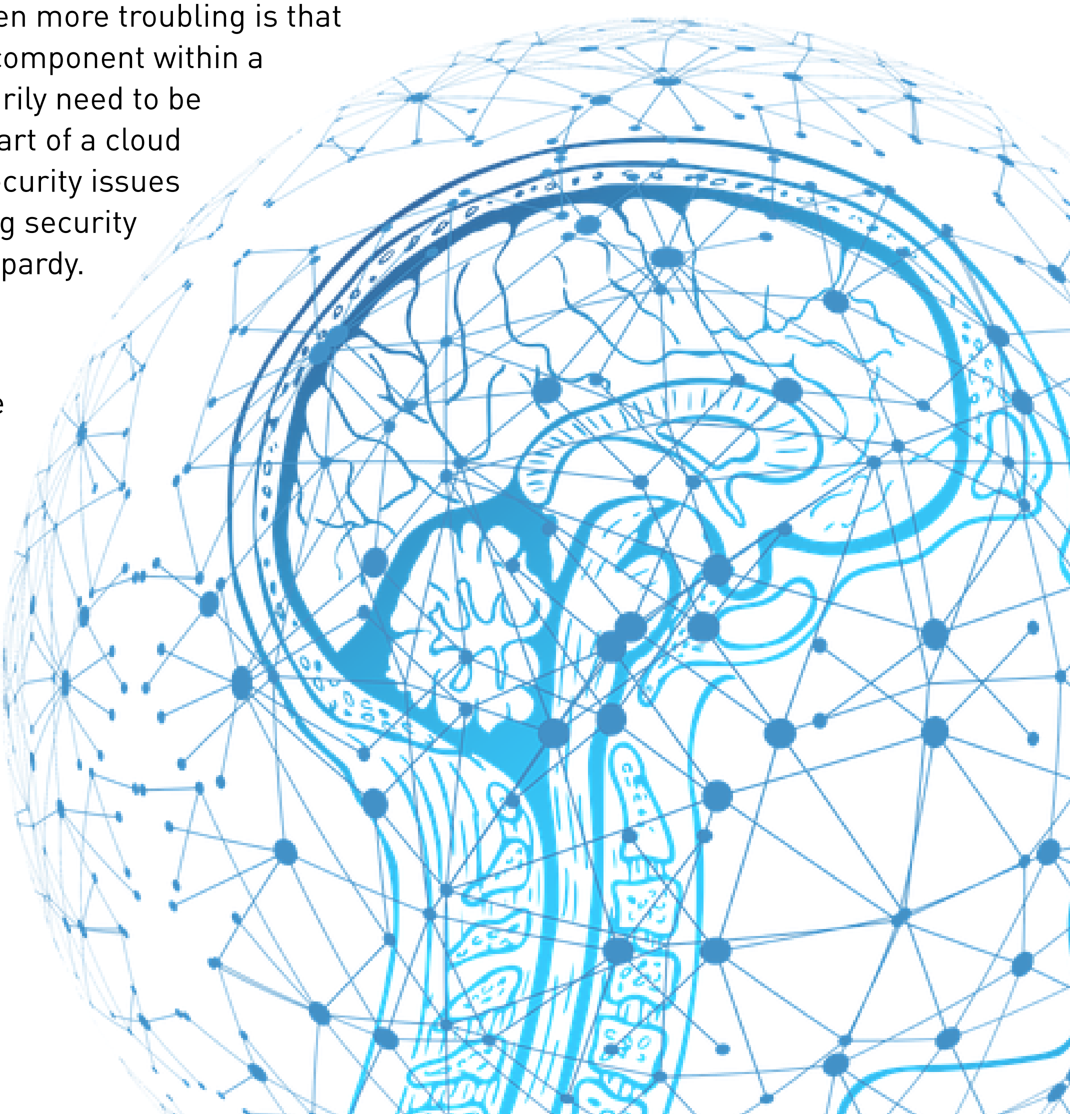
Designing with security in mind is proving to be essential for OEMs in the embedded space. But exactly what that means remains a moving target: What's secure today is not necessarily secure tomorrow.

In volatile industry environments where threats are non-stop, OEMs want to secure their devices and systems, but don't necessarily understand how to maintain protection for the long term. A smart approach features design strategies and standards, but as importantly, is grounded in a security-driven mindset that embraces security implementations and deals proactively with different risks. This kind of vigilance can prevail in many ways: protecting systems, distinguishing OEMs, and driving new opportunities to create long term profit centers from security services.

There's Always a Hacker

Manufacturing partners can offer plenty of smart protocols to initially secure a system: white-listing, freezing configurations, smart stack management, and much more. Yet if an OEM lacks a security-forward strategy, these protocols will be obsolete in a matter of months when all the rules change again. Even more troubling is that cyber-attacks can target any component within a system; devices don't necessarily need to be connected to the Internet or part of a cloud solution to be vulnerable to security issues or threats. Ignoring or delaying security processes only adds to the jeopardy.

Ideally, OEMs must instead consider the entire service organization, how systems are deployed and maintained, as well as the level of safety and support expected by customers. If you are promising protection for your customer, baseline activities must ensure promises are kept. Extended activities can build further on this promise, tailored to add value to applications that require even greater protection.



Going Beyond Strategies and Standards

Internal operations must support a plan to constantly update and maintain systems at a stable level, remaining compliant and keeping up to speed with security implementations and evolving risks. Yet part of the complexity is that every customer's engagement is different. For example, OEMs developing military training and simulation systems may need to deliver a range of training levels or handle secure data. Meeting Department of Defense security mandates may be required before a machine is even authorized to perform in a specific building – secure machines must then be integrated into a secure infrastructure. An IT organization within a hospital may need to shield a system, even while sharing data with a range of other clinical stakeholders. FDA security guidance closely mirrors DoD mandates, demonstrating the growing expectation that OEMs will prioritize security from initial development through end-user deployment.

In both industry examples, OEMs are tasked with developing device features that serve end-user needs, while simultaneously instilling confidence the system has its own protected surface. Remote access also plays an increasing role and must empower system managers across the spectrum of embedded applications to make changes and updates without compromising device or data security. Taken together, all these factors challenge OEMs who fail to tap into a security mindset to meet the demands of continuous hardware and software maintenance.

> **"Instead of ignoring or struggling against security needs, proactivity and broad thinking is required. These are the attributes powering a shift in attitude that embraces security services as a powerful (and profitable) center for customer support."**

Finding Opportunity

Designing to standards and protocols is the easy part, with it being much more difficult to embrace security leadership as part of OEM operations. Instead of ignoring or struggling against security needs, proactivity and broad thinking is required. These are the attributes powering a shift in attitude that embraces security services as a powerful (and profitable) center for customer support.

When proactive security updates are part of the fabric of the organization itself, they become a feature – not a roadblock – that can connect with OS and hardware updates and be sold as a service. Keeping security update cycles in sync with application updates is a smart starting point - executing patches while updating to circumvent any vulnerabilities, performance improvements, and application upgrades. A routine cadence of updates is not only a selling point and competitive distinction, it is also a means of turning a cost center into a profit center.

Framing Your Security-First Mindset

Developing a security mindset is a process and is based on an understanding of what it important to you as a business, as well as what is important to your customers. What are your customers asking of you and how can your answer differentiate you from the competition? How can you remain compliant and secure while ensuring system performance? And what can your original design manufacturing (ODM) partners do to help you consider vulnerabilities at every stage of design, development, and deployment? Do you communicate well internally on security challenges and plans? Or are they considered constant roadblocks that are pushed down the development list?

There is a whole new dimension of liabilities to consider with these questions, and addressing them is not an entirely technical discussion. The concern will be different depending on which team is responding. Administrators are usually the first to acknowledge the need for security, if only as a path to make products more marketable. Engineers point out that resources are not available for constant updating and validation. The service team says there is not enough manpower to handle field updates efficiently. And the quality assurance staff questions how the OEM can document changes and ensure performance remains untouched. Progress, however, can be driven in large part by working with technology partners for security insight and support. ODMs often take on the role of negotiator, helping OEM teams communicate better internally and exploring options that help each of them maneuver to a strong security mindset.

Five Key Questions to Help Define your Security Protocol

Developing a security mindset is a process based on the understanding of what is important to the business and to your customers:

- **What are your customers asking of you and does your answer differentiate from the competition?**
- **How can you remain compliant and secure while ensuring system performance?**
- **What can your ODM partners do to help you consider vulnerabilities at every stage of design, development, and deployment?**
- **Do you communicate well internally on security challenges and plans?**
- **Or are they considered constant roadblocks that are pushed down the development list?**

Understanding the Risks

Embedded systems are under siege. It’s a hacking war of software team versus software team, and it is the good versus the bad. Simply put, OEMs must win more battles than they lose. The most essential question is how much do you have to risk? What data or applications are vulnerable, and what is the potential for harming end-users and reputations should they be successfully breached?

The security playground, however, really is just too big to ask two or three questions as a means of defining your path forward to a security-first mindset. In this landscape, threat assessment considers connectivity of end-users, existing frequency of updates, confidential or otherwise sensitive data on the device, the cost of any potential losses, and much, much more. Only the OEM building and managing the device can truly ascertain the according value of these issues – raising expectations for a security focus woven into every phase of development and manufacturing partnership.

DEDICATED COMPUTING | POWERING THE WORLD'S MOST IMPORTANT DEVICES®

Dedicated Computing is an original design manufacturer (ODM) of proprietary, highly engineered computing systems for blue chip original equipment manufacturer (OEM) customers in healthcare and life sciences, training and simulation, and industrial markets.

Our mission is POWERING THE WORLD'S MOST IMPORTANT DEVICES.

Our customers are building devices that save lives, train people to save lives or improve the lives of others. Dedicated Computing's products and services are at the core of those devices, powering complex calculation engines, providing near instant access to and serving vast amounts of data, and making sure those devices are secure, supported, and working properly.

Find out more at:

www.dedicatedcomputing.com