Microsoft

Secure your IoT deployment during the security talent shortage

Published: December 2019

For the latest information, please see
www.microsoft.com/azuresphere

Introduction

Businesses across industries are starting to place big bets on the Internet of things (IoT) and the value it will deliver in the coming years. Even now, real-time data and insights can improve performance and bottom lines. Innovative new experiences for customers can propel revenue and earn coveted market share. However, to take advantage of the lasting value that IoT can unlock, organizations must prioritize security. The simple act of connecting devices or equipment introduces new threats to privacy, intellectual property, revenue, and physical safety. Building a foundation of security will ensure durability of innovation and business growth. Simply put, to be competitive in the long run, there is no choice: securing your IoT investments is a necessity.

Companies should carefully consider how the decisions they make now about IoT security could affect business projections, even in the short term. The complexity of IoT and its associated risks—to the company, its brands, and its customers—can be overwhelming; the security vulnerabilities and requirements of IoT environments are still evolving and can be difficult to frame and address. Many manufacturers and enterprises are still working to clearly define an IoT security strategy that can leverage existing protocols, practices, and expertise. Incorporating a comprehensive security strategy into your IoT business objectives is made even harder by a record-setting, three-million-person shortage of security pros[i]. This truly massive talent shortage causes an overextension of existing security teams and leaves organizations without coverage for new IoT projects.

IoT is especially vulnerable in a security talent shortage

The worldwide shortage of security talent is especially dangerous for IoT because its unique risks are difficult to detect and costly to mitigate. Sometimes it's easy to identify the risks: a compromised connected car or gas furnace could injure or even kill someone. But other vulnerabilities are not as obvious: a connected thermostat could spoil the entire contents of a food storage unit, shutting down a restaurant for a week. Whenever IoT is integrated into the business, especially when depended upon for primary operations, there is high risk to revenue. Companies of every size stand to suffer significant financial loss in the event of a breach or other IoT security incident, the effects of which can drag on beyond just the hours or days of downtime.

The scarcity of security talent is most prevalent in emerging disciplines and technologies like IoT. Although IDC projects IoT spend grow year over year, passing $1 trillion by 2022, fewer than 50 percent of surveyed executives reported standalone budget for IoT security[ii]. Even if companies were to prioritize spend on IoT security, they would still find it incredibly difficult to hire qualified personnel. As IoT market value grows exponentially each year, so too will the demands on legacy security teams.

Despite the risks inherent in IoT, and the strain on security teams during the talent shortage, the potential of IoT is too valuable to ignore or postpone. Eighty percent of companies that invest in IoT see increased revenues while benefiting from reductions in costs and downtime[iii]. As IoT becomes mainstream, organizations that don't pursue IoT-driven innovation are missing the opportunity to secure their place in the future economy. Decision makers evaluating how to pursue both IoT innovation and security don't need to steal from one to feed the other. It isn't a binary choice. There is a way to augment existing teams and resources, even amidst the talent shortage, with trustworthy solutions that help meet the ongoing security needs of IoT—without diminishing opportunity for innovation.

Avoid shortcuts and common fallbacks when planning IoT security

Organizations are eager to find methods that improve the success of their IoT deployment. A common approach is establishing checklists that employees can work with to avoid making IoT security mistakes. Checklists are a long-standing security tool favored by companies like airlines that depend on the accuracy of repeated processes to meet safety standards. Although they've been relied upon for years across industries, checklists alone do little to ensure correct implementation of complex and nuanced IoT deployments and their maintenance, and attackers will happily target weaknesses created by missed details.

The primary shortfall of checklists is that IoT security is not a "set it and forget it" task and there is no substitute for expertise. Security expertise requires a mix of best practices, knowledge of exploits, and the ability to test security capabilities against a full range of attack vectors. It also includes learning from new threats as they emerge and prioritizing updates. Security expertise is necessary to safely plan for IoT and to ensure solutions are securely implemented and kept up to date over time.

Solve for functional practices and focus your security team on strategic initiatives

As organizations reach the limit of available resources, the key to success becomes differentiating between **core activities** *that require specific organizational knowledge* and **functional practices** *that are common across all organizations*. Utilize your security teams to focus on core activities such as defining secure product experiences and building strategies for reducing risk at the app level. This critical thinking and creative problem solving is where your security teams deliver the greatest value to the business—this is where their focus should be.

Establishing reliable functional practices is critical to ensure that your IoT deployment can meet the challenges of today's threat landscape. Outsourcing functional practices to qualified partners or vendors will give you access to security expertise that will multiply your team's effectiveness and quickly ramp up your IoT operations with far less risk. When considering partners and vendors, find solutions that deliver these essential capabilities:

Holistic security design
IoT device security is difficult. To do it properly requires the expertise to stitch hardware, software, and services into a gap-free security system. A pre-integrated, off-the-shelf solution is likely more cost-effective and more secure than a proprietary solution, and it allows you to leverage the expertise of functional security experts that work across organizations and have a birds-eye view of security needs and threats.

Threat mitigation
To maintain device security over time, ongoing security expertise is needed to identify threats and develop device updates to mitigate new threats as they emerge. This isn't a part-time job. It requires a dedicated resource that is immersed in the threat landscape and that can rapidly implement mitigation strategies. Attackers are creative and determined, the effort to stop them needs to be appropriately matched.

Update deployment
Without the right infrastructure and dedicated operational hygiene, organizations commonly postpone or deprioritize security updates. Look for providers that streamline or automate the delivery and deployment of updates. Because zero-day attacks require quick action, the ability to update a global fleet of devices in hours is a must.

Tap into Microsoft security expertise for functional practices

Microsoft Azure Sphere delivers holistic security design, ongoing threat mitigation, and continual update deployment in a single, comprehensive solution. This end-to-end security solution for IoT devices brings together the best of Microsoft's expertise in cloud, software and silicon—resulting in a unique approach to security that starts in the silicon and extends to the cloud. Together, Azure Sphere chips, our secured OS, and our turnkey cloud security service give you the freedom to focus on your business with the confidence that your functional security practices are actively managed by Microsoft.

> *Hardware*
> Every Azure Sphere chip includes built-in Microsoft security technology, built-in connectivity, and the power of a Cortex-A processor. To provide a dependable hardware root of trust, every Azure Sphere chip has a unique identity that is born in the silicon, protecting the integrity of the device key. Advanced security measures built into each Azure Sphere chip guard against physical attacks, device impersonation, and supply-chain tampering.
>
> *Software*
> Azure Sphere Operating System is built to offer unequalled security. The four-layer, defense-in-depth OS includes a custom Linux kernel. In the event that a device is compromised, the multiple layers of security work to limit the reach of the attack, making it much more difficult for the attacker to take control of the device and making it possible to restore the health of a device. To maintain integrity over time, Microsoft services the OS for over 10 years: we build, manage, and deploy OS updates directly to devices.
>
> *Services*
> The final element of Azure Sphere is our cloud security service, which delivers certificate-based authentication to eliminate the need for passwords, automates online error reporting to detect emerging threats, and renews security automatically through software updates.

The integrated components of Azure Sphere work seamlessly together and deliver active security by default. Microsoft offers a simplified business model, with a one-time upfront price, that includes Azure Sphere certified hardware, The Azure Sphere OS, The Azure Sphere Security Service, and over a decade of OS and security updates. Together these Azure Sphere components provide defense in depth for your devices.

Set innovation free with Azure Sphere

When you build your IoT deployment on a secure platform, you can transform the way you do business: reduce costs, streamline operations, light up new business models, and deliver more value to your customers. With Azure Sphere, you can both securely connect your existing mission-critical equipment and create innately secured IoT devices. Guardian modules make it fast and simple to securely connect mission-critical equipment with little to no redesign. Azure Sphere development kits are designed to streamline prototyping and planning for all your scenarios and use cases. And when you're ready for production, there are a variety of Azure Sphere modules from our trusted partners to help you reduce costs and get to market faster.

Flexible deployment, development, and delivery models can help you optimize your IoT strategy and reduce or even eliminate the need to invest in additional infrastructure or staff, effectively skirting the challenges of the security talent shortage. Further, by building comprehensive, defense-in-depth security for your IoT initiatives, you can focus on what you're in business to do.

Azure Sphere is designed to help you bring your legacy investments into the future and help you design new products and experiences—with powerful connectivity and security for every IoT device. With Azure Sphere you can drive innovation and deliver lasting value.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

[i] (ISC)^2 Cybersecurity Workforce Study https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0%5Ch

[ii] IDC Worldwide Semiannual Internet of Things Spending Guide https://www.idc.com/getdoc.jsp?containerId=IDC_P29475

[iii] Tata Consultancy Services Global Trend Study on IoT https://www.prnewswire.com/news-releases/over-80-of-companies-increased-revenue-by-investing-in-internet-of-things-tcs-global-trend-study-300117013.html