Connection®
we solve IT®

MODERN INFRASTRUCTURE AND MULTICLOUD SOLUTIONS

Building Cyber Resilience: Securing and Managing the Edge

Table of Contents

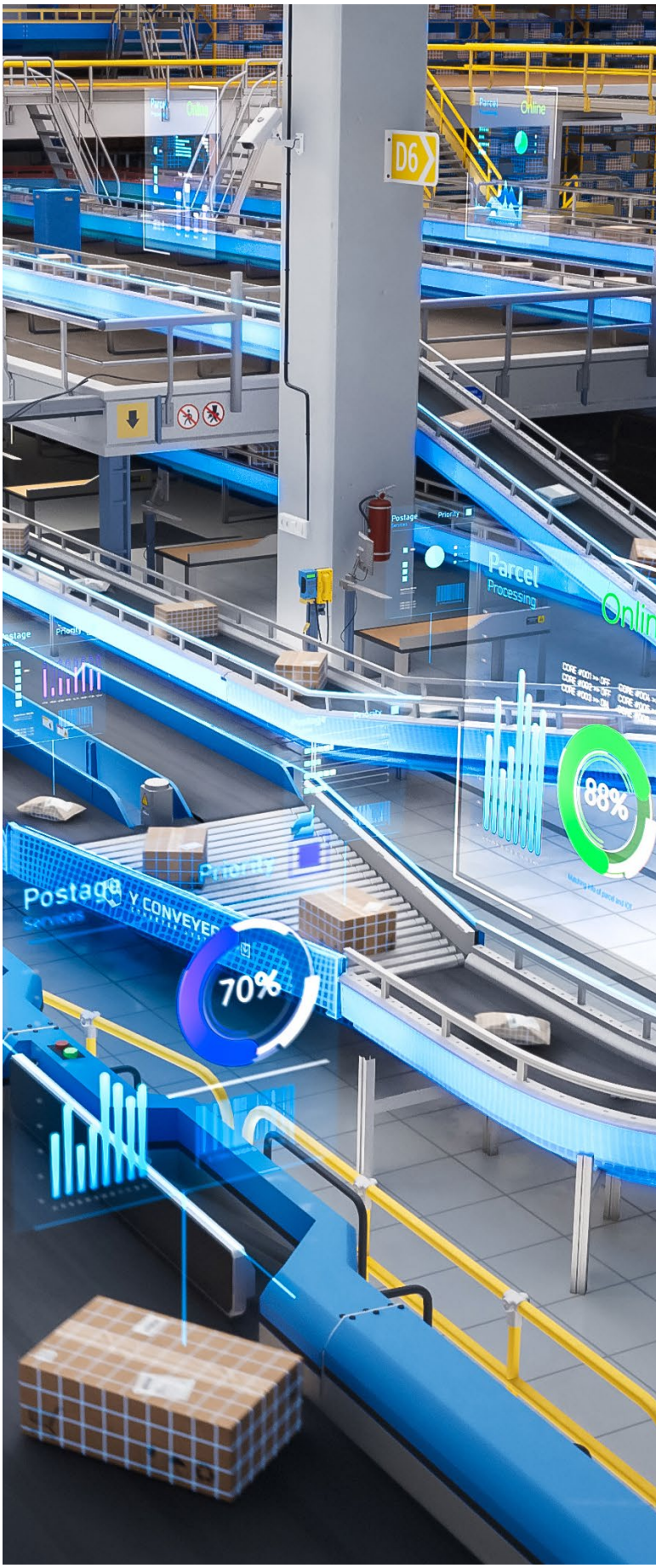
Introduction

Edge computing—where data is processed at or near its source—is on the rise. Whether they're deploying embedded devices in smart factories or installing sensors in smart office buildings, modern businesses are generating more and more operationally critical data outside of their data centers. In fact, Gartner predicts that 75% of enterprise data will be processed somewhere other than a traditional central data center or the cloud by the end of 2025.[1]

Edge computing strategies can create efficiencies that simply cannot be realized when large volumes of information must be streamed to the cloud or data centers for processing. As more data is generated at remote locations, faster, the inefficiencies associated with transmitting all that data to a central location are multiplied. Whenever data is sent off-site for processing, latency results.

What's more, growing numbers of enterprises now face regulatory constraints that prohibit them from sending data outside of their local geographic region. With edge computing, organizations can overcome such roadblocks and instead generate immediate value from their data near the point where it is created.

The benefits of decentralized computing are appealing, and enterprises are increasingly deploying processing power at the edge to fuel data-driven decision-making, improve operations, and boost customer experiences. Driven by this momentum, along with rising



[1] Gartner, What Edge Computing Means for Infrastructure and Operations Leaders.

enthusiasm for machine learning (ML) and AI, the market for edge computing is currently growing at an extremely rapid pace. It's forecast to see a combined annual growth rate (CAGR) of more than 35%, and to reach more than $155 billion in annual global spending by 2030.[2]

In today's world, the swift adoption of edge computing is reshaping business IT infrastructures. At the same time, however, it is creating new risks.

The expansion of an enterprise's technology footprint that comes with moving processing to the edge inherently increases that company's attack surface. Plus, many edge deployments include Internet of Things (IoT) and medical devices (also known as Internet of Medical Things (IoMT)) that require protection from malware and security exploits, so proper policy-based device management is critical.

Oftentimes, too, ensuring the physical security of edge devices can be difficult, since their locations may be remote, inaccessible, or subject to harsh conditions. Managing these highly distributed environments can be complex. Distributing software patches, updating operating systems, and maintaining proper configurations across edge deployments isn't easy, and the difficulties are often amplified by organizational silos or a lack of standardization.

This is why it's vital to adopt a consistent edge security and management strategy. By relying on proven reference architectures and management paradigms, organizations can reduce the cybersecurity risks and operational headaches associated with expanding their reliance on the edge.

In this practical guide, we'll give you expert advice on managing and securing your edge from design to deployment, so that you can capitalize on the full array of benefits of edge computing while effectively mitigating its risks.

75%
of enterprise data will be created and processed at the edge by 2025[3]

$155 billion
in annual spending on edge computing by 2030[2]

70%
of security stakeholders are concerned that their edge deployments are vulnerable to cyberattacks[4]

[2] Grand View Research, Edge Computing Market Size & Trends: Market Analysis Report, 2024.

[3] Gartner, What Edge Computing Means for Infrastructure and Operations Leaders.

[4] S&P Global Market Intelligence, The State of Edge Security Report, 2023.

Building a Resilient Edge Strategy

Edge computing is all about location. By definition, it involves moving storage and compute resources out of the data center and closer to the place where data is being created or served. This way, real-time business analytics, equipment maintenance predictions, workplace safety monitoring alerts, retail inventory optimization suggestions, and many other high-value insights can be generated right in the retail store, on the factory floor, or at any other on-site location.

There are a near-infinite number of potential use cases for edge computing. Here are just a few examples of how it is delivering value across industries.

Vertical	Edge computing use cases
Manufacturing	• Error detection and quality control • Predictive maintenance • Industrial security • Industrial Control Systems (ICS) • Supply chain management
Retail	• Store security and surveillance • Stock tracking and real-time inventory management • Environmental monitoring and control • Customer behavior analysis • Point-of-sale (POS) device management
Healthcare	• Remote patient monitoring • Clinician safety • Medical device management • Clinical diagnostic support • Operations management

As even this short list makes clear, there's enormous diversity among the applications for edge computing technology. Every one of these different use cases brings unique security risks and operational challenges. Plus, each different use case has its own regulatory compliance requirements as well. Stakeholders in organizations adopting edge computing strategies need to think carefully about the specific protections that their edge deployments require.

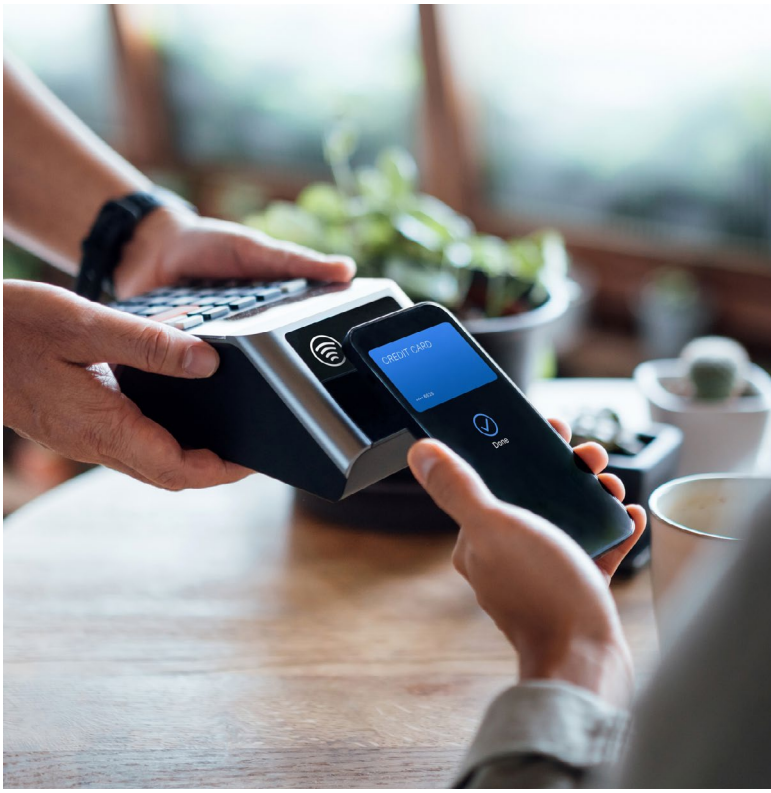
Edge Deployments Have Unique Security and Management Requirements

When devices operate outside of the confines of the traditional data center, they may need additional physical protections. Many edge devices must be rugged or extremely compact to suit their surroundings. Often, their physical form factors have to be weather-resistant and safeguarded against other environmental hazards. Because they may be situated in remote locations, they must be protected from tampering or physical interference.

In some cases, data from the edge isn't processed at an off-site location, but instead computing is performed in a third-party data center. This means that the organization must partner with the data center operator or colocation provider to ensure that security controls are enforced in ways that are consistent with policies, compliance requirements, and cross-industry standards. Cybersecurity practices should be clearly spelled out and agreed upon by all parties involved in managing the data—at rest, in transit, and during processing.

In edge deployments, connectivity also needs to be secured. Edge devices do not always communicate via traditional wired or wireless networks. Instead, they may leverage mobile (5G or LTE) connectivity. This is a relatively unusual approach within enterprise computing, but it requires a mobile-focused strategy for securing data flows.

The edge often includes large numbers of IoT, IoMT, and Operational Technology (OT) devices. Controlling access to these devices can be challenging, as can hardening them against cyber threats, since many IoT, IoMT, and OT devices lack the computing power needed to run anti-virus software or other endpoint protection tools. Keeping operating systems, firmware, and other software up to date can be difficult when there's little tolerance for downtime, and the challenges are multiplied when devices are distributed across large areas. In these scenarios, maintaining consistent configurations and standardized management procedures can also be an issue.



Don't Let the Edge Be the Weakest Link in Your Security Strategy

Adopting an edge computing strategy need not require compromising on cyber resilience. Organizations moving towards an edge computing model should not loosen their security requirements or shift their security strategy to avoid the challenges involved in securing the edge. Instead, they should strive to maintain or even build upon their existing security standards.

An effective edge security strategy must include protections for devices and their communications, as well as the data and applications they interact with.

An effective edge management strategy must allow for centralized control and consistent adherence to standards.

To achieve centralized control, policy enforcement, and security protections, organizations need a strategy that will make it simpler and easier for them to implement security standards across large, diverse environments. Leveraging proven reference architectures and proven management paradigms does exactly this. It enables organizations to take advantage of built-in expertise (and standardization) to secure and manage their edge deployments while also adhering to regulatory requirements.

What Is a Reference Architecture?

A reference architecture is an abstract template that sets out the hardware and software components to be included in an edge computing solution. It's a document that describes how all of these products and services can be integrated into a complete solution, one that's grounded in accepted best practices. The reference architecture packages these best practice-based recommendations into an easy-to-understand format that simplifies and streamlines the implementation of complex technology solutions. Building your edge computing deployment on an established reference architecture means that it will include an entire ecosystem of trusted technologies. Each reference architecture is industry- and use-case specific, enabling its design to address the unique challenges inherent to that situation.

Using a reference architecture makes it easier for everyone engaged in the deployment of an edge computing solution to understand what's required for the project's success. The reference architecture includes answers to the most frequently asked questions about the deployment, reducing the complexities involved in planning, designing, and implementing the infrastructure. It can also serve as a fully-tested, validated guide to building a cyber resilient edge deployment—one that incorporates a secure-by-design approach from the outset.

Major enterprise hardware vendors such as Dell, HPE, Cisco, and Lenovo offer reference architectures, as do public sector and nonprofit organizations like the Edge Computing Consortium.[5] Commercial reference architectures typically include all the hardware, software, and implementation instructions needed to build and scale an organization-wide edge deployment.

[5] Edge Computing Consortium, Application Scenarios.

15 Best Practices for Edge Security and Management

Leveraging industry standard best practices is critical for organizations to protect the resources at edge locations, especially as reliance on IoT devices and distributed computing grows. Here are some best practices to consider.

1. Conduct regular risk assessments
Particularly since the risks associated with edge devices and networks can be different from those associated with campus networks and cloud services, it's imperative to regularly identify vulnerabilities in your edge deployments. This can be challenging when systems are widely distributed, so creating and maintaining an accurate asset inventory is an important first step. Understanding the severity of any vulnerabilities that you find—in terms of how it might harm your organization if they were exploited—can help you prioritize remediation efforts.

2. Implement strong authentication and access control measures
The same basic principles of robust identity and access management apply to all organizational computing systems, whether they're in the data center, in the cloud, or at the edge. Require multi-factor authentication (MFA) for your edge device remote access and/or remote management controls, and limit permissions to the minimum required for employees to get their jobs done using role-based access controls (RBAC).

3. Encrypt data at rest and in transit
Especially important in highly distributed environments where it's more difficult to enforce physical security controls, data encryption ensures that information assets that are accidentally accessed aren't compromised. Using strong encryption protocols for data

transmitted to and from edge devices can help to protect it—and this includes the data required for the remote management of the edge devices themselves. Sensitive or proprietary data stored on edge devices should also be encrypted.

4. Update software and firmware regularly
For many reasons, including the distributed nature of edge deployments, the importance of avoiding downtime, and the large number of devices in edge fleets, it can be very difficult to keep all edge devices up to date with software patches. Nonetheless, it's critical to do so. Leveraging automation wherever possible can reduce the effort involved, as well as the amount of human error that could occur.

5. Segment IT and edge networks to limit exposure
Network segmentation can isolate insecure IoT, IoMt, and OT devices from core systems. Make use of internal firewalls and virtual local area networks (VLANs) to create microsegments, control traffic flows, and enforce policies that prevent edge devices from automatically establishing connections to systems in other parts of the network.

6. Log and monitor activities on edge networks
Turn on logging so that security teams have a mechanism for keeping track of access to edge devices and changes that are made. An intrusion detection/prevention system (IDS/IPS) can help you monitor edge deployments for suspicious activities, too.

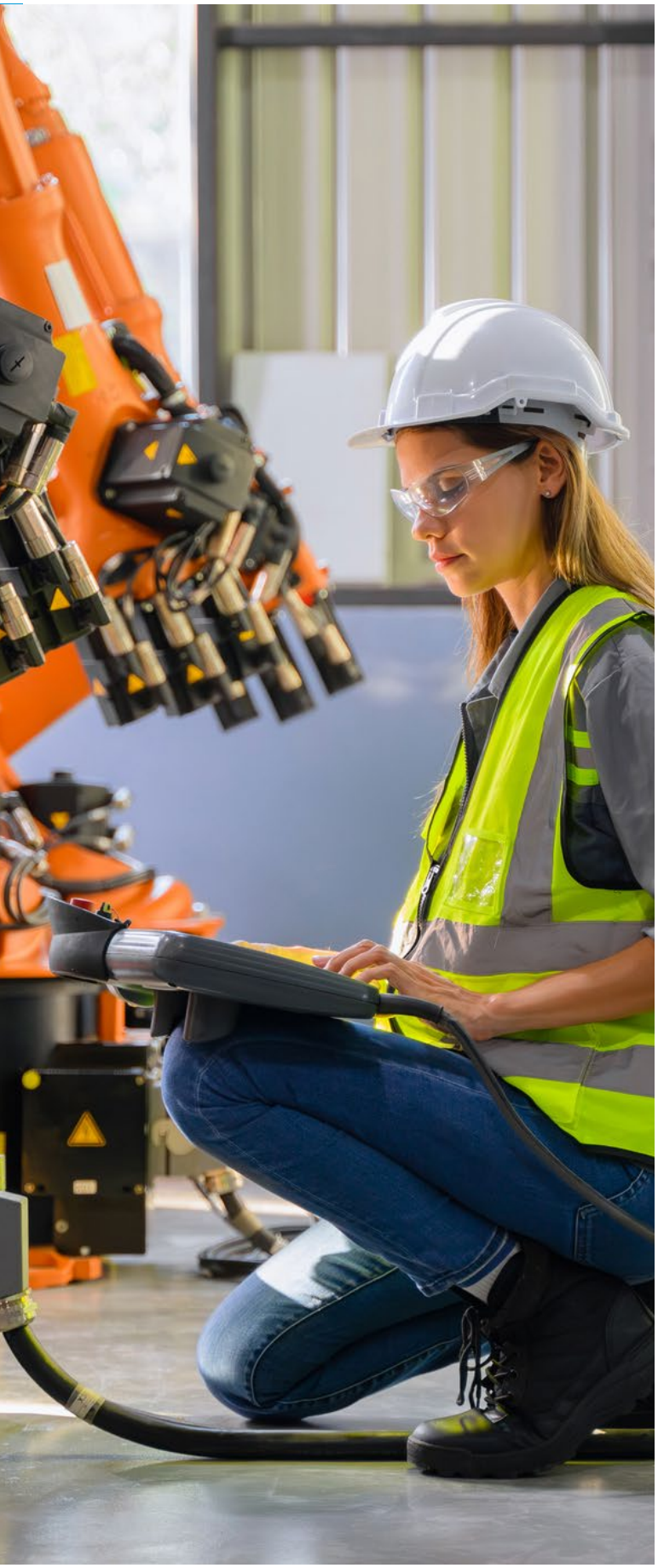
7. Establish an incident response plan for your edge deployment
If a malicious actor did gain access to your edge computing environment, what steps would your team take to minimize the blast radius and ensure rapid recovery? Developing and testing a response plan for edge-related security incidents can prepare you for worst-case scenarios. Be sure to clearly define the role that each team member would play, as well as communication strategies they should follow.

8. Leverage AI and ML
Endpoint detection and response (EDR) and intrusion detection and response (IDR) tools with embedded AI and ML (AI-SecOps) can help security teams identify and stop threats faster. AI-driven analytics enable real-time threat detection and response, while ML models can identify unusual patterns and anomalous behaviors accurately and automatically.

9. Ensure physical security of edge deployments
Protect edge devices from physical tampering and unauthorized access with access control systems, secure physical enclosures, GPS fencing, vibration or enclosure sensors, surveillance cameras, and other physical security measures.

10. Implement a Zero Trust architecture across your entire technology ecosystem
Adhering to the Zero Trust security model is a best practice across industries. This model requires verifying the identity of every entity requesting access to a resource, no matter where the request originates from. In Zero Trust, no network segment is assumed to be trustworthy; instead, continuous verification (of identity and context) is performed. Extending Zero Trust principles across your edge deployment is key for making sure that the edge doesn't become a weak point within your security ecosystem.

11. Conduct regular security awareness training
All employees should be taught basic principles for protecting their devices and accounts, and those managing edge devices are no exception. Promote awareness about present-day cyber threats targeting edge devices and best practices for protecting them among the members of this group.



12. Implement a centralized management system for edge devices
Centralizing edge management streamlines the process of maintaining large device fleets while making it easier to keep software updated and device configurations secure. A centralized approach to edge device management also ensures that you'll have visibility across the entire deployment. Leverage proven edge device management systems provided by OEMs and device manufacturers wherever possible.

13. Establish security standards for third-party edge device vendors
Assess and verify the security measures that your partners and vendors have put in place to protect edge devices and services. Be sure that your security requirements are clearly outlined in all contracts and agreements you establish with third parties.

14. Build backup and recovery solutions
Like any other part of your technology ecosystem, your edge deployment should be protected with robust backups. Regularly back up data and configurations from your edge devices, and test your recovery capabilities regularly to ensure that you'd be able to restore operations quickly if an incident should ever take place. Consider managed services offerings for onsite replacement of edge devices (and the systems that monitor them) where appropriate.

15. Integrate compliance requirements whenever they're in scope
If regulatory compliance requirements are applicable to your edge deployment, be sure to map these requirements to your edge management practices. This often means adhering to data localization restrictions and implementing data protection and privacy-by-design across the deployment.

Simplifying and Streamlining Edge Security and Management

Organizations across industries have long struggled with cybersecurity skills shortages, a familiar problem that's unlikely to be solved anytime soon. Research indicates that there are nearly 500,000 unfilled positions in the field within the U.S. alone,[6] and a global cybersecurity workforce shortfall of over 4 million professionals.[7]

Because edge deployments—especially newly-implemented edge deployments—can be challenging to secure and maintain, ease of operation is especially important for short-staffed organizations beginning to build out an edge computing strategy. Leveraging pre-built templates for a secure-by-design approach and incorporating extensive automation can make a huge difference when it comes to improving security without adding management complexity.

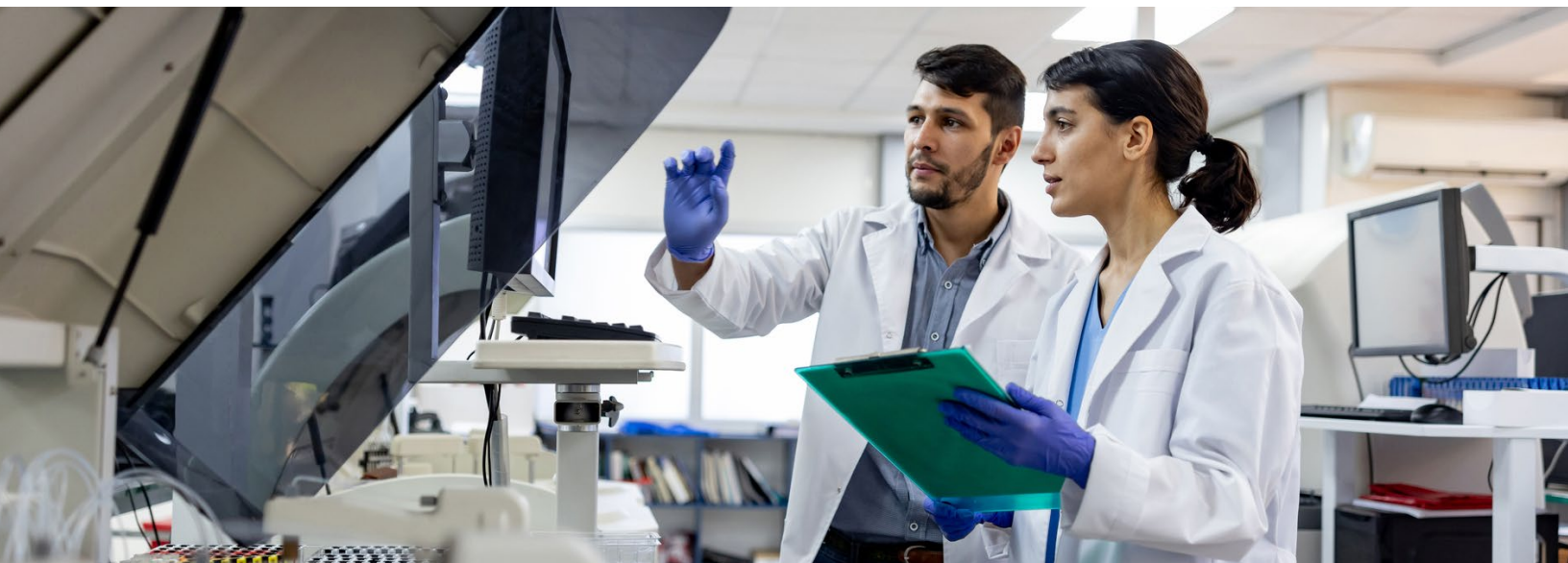
50%
of significant security incidents will be caused by lack of talent or human shortfall by the end of 2025.[8]

---

[6] CyberSeek, Cybersecurity Supply/Demand Heatmap.

[7] World Economic Forum, Bridging the Cyber Skills Gap, October 2023.

[8] Gartner, Gartner Predicts that Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025.



Take Advantage of Templates

Standard reference architectures include templates that you can use to remotely provision and configure every edge device in your environment.

This makes initial deployment easier, but it also ensures that standard configurations are applied consistently across the device fleet, eliminating individual device-based security gaps. When you rely on templates, devices can be configured remotely, and you can automate their management with a virtualization platform

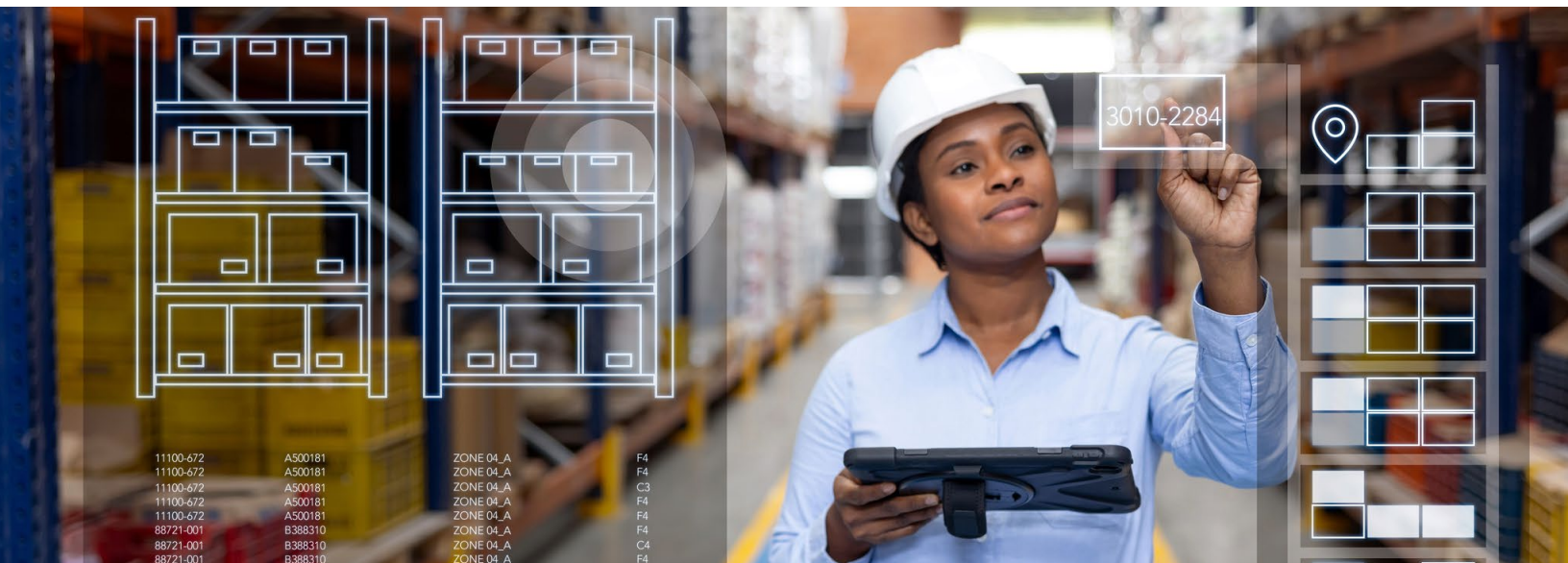
Modern edge management platforms leverage container platforms like OpenShift, Kubernetes, and Docker. All of the software should originate from a pre-scanned repository, so you can be confident from the outset that the code deployed has not been compromised.

Look for an edge management platform that integrates with the security information and event management (SIEM) solution you're using, or any other security monitoring tools you rely on. This will enable your security operations team—regardless of whether the capability is in-house or outsourced to a managed security service provider (MSSP)—to rapidly respond to any edge security incident that might occur.

Take note:

You cannot securely manage huge fleets of edge devices when every one of them is a snowflake.

Repeatability is key.

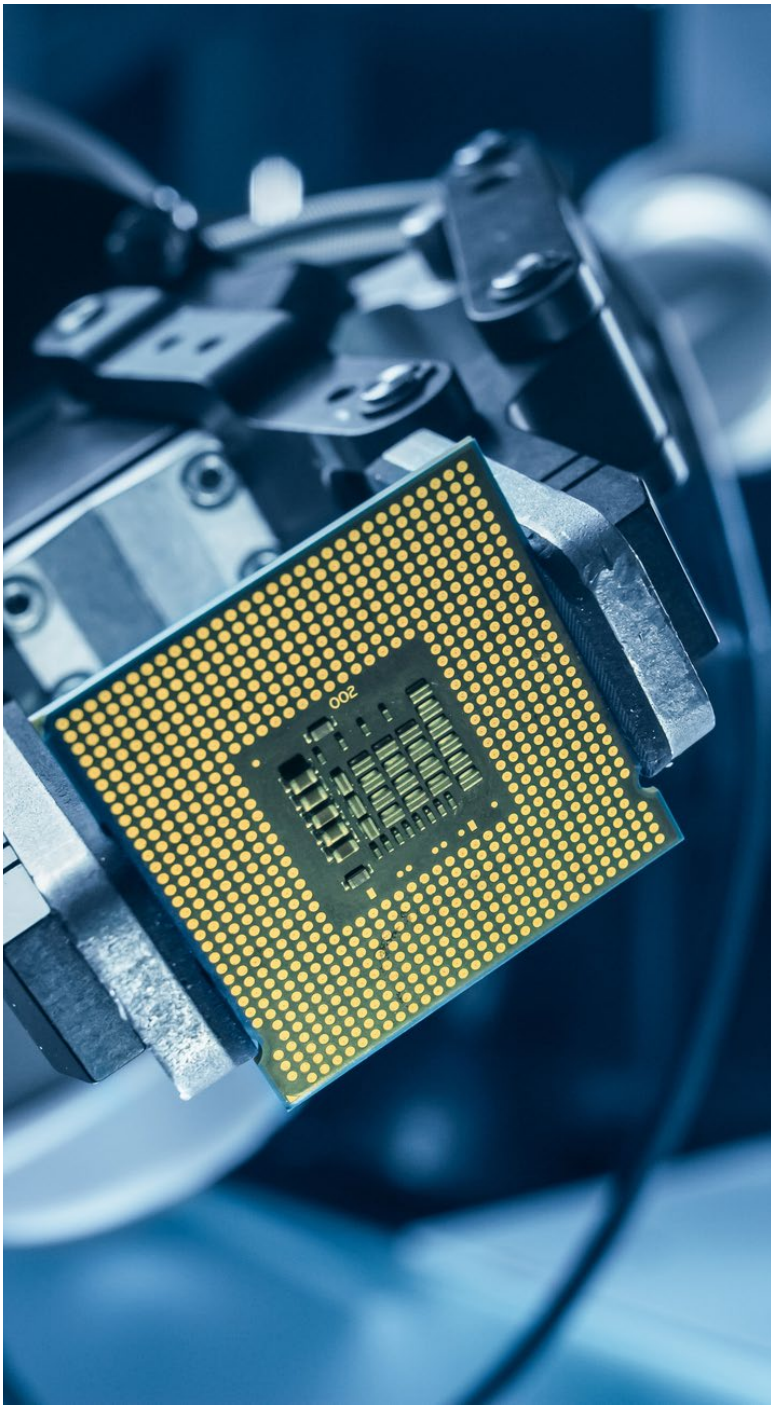


Leverage Intelligent Automation

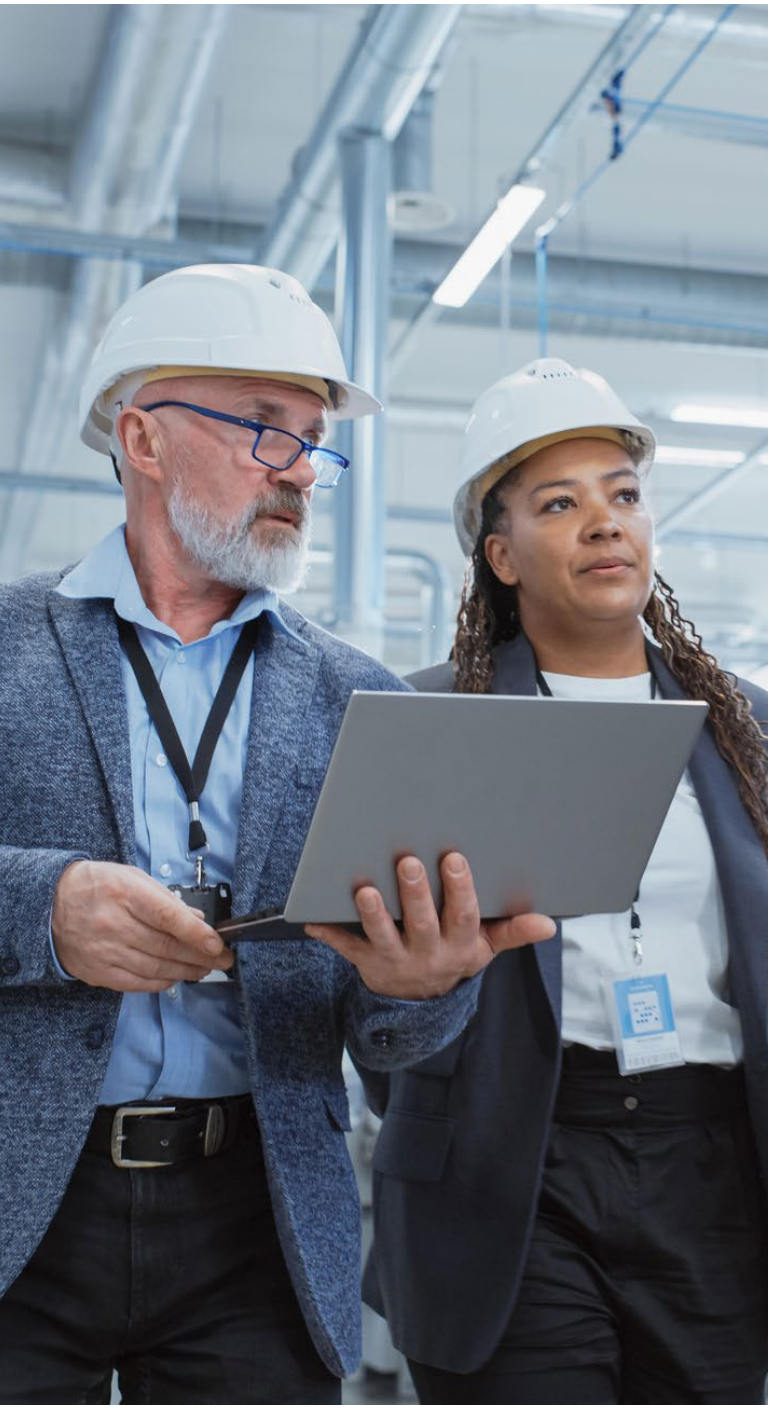
Choose a reference architecture that includes (or readily integrates with) a management platform with embedded AIOps functionality and Infrastructure as Code (IaC) automation features for consistent provisioning and configuration management. Such features and functionality are not rare: they are quickly becoming integral to nearly all major vendors' solutions today.

AI also enables the core functionality of edge computing use cases like machine vision, which can serve in numerous applications ranging from loss prevention in retail or to physical security monitoring.

The use of embedded AI/ML can also simplify and streamline device fleet management in the form of AIOps. AI-driven operations (AIOps) not only powers a more efficient and secure approach to managing the deployment of devices and applications, but it can also enable a responsive infrastructure approach to edge security. In practice, AI-SecOps can analyze edge computing environment data in real time to detect the anomalies that may signal an in-progress attack. While this enables security teams to rapidly respond to known and unknown threats, such systems can auto-remediate or quarantine threats before human intervention is required.



The Value of Working with a Trusted Partner



Building and scaling a new edge deployment—or securing an existing one—can be challenging. The right technology partner will be well versed in all the technology products, services, and solutions on the market today, so they'll have a keen sense of which ones would be best for your business. Look for a partner with expertise in integrating across public and private clouds and edge platforms. Your partner should also have experience operating at enterprise scale.

Your partner should be able to help you choose a reference architecture. They should have the expertise needed to understand your use case, build out your deployment, and ensure that it operates smoothly over the long term. They should understand—and be able to support—your compliance requirements while helping you build and maintain an intelligent risk management strategy.

An ideal partner is an organization that could participate in a one-time consulting engagement if needed, but who may also deliver (or integrate with) managed services over the long haul. This way, you can be confident that you won't encounter excessive administrative burden, and you'll have a partner that can come alongside you to help as much or as little as you need.

This type of support ensures that you'll be able to rapidly realize the full value of your investments in edge computing solutions.

Optimizing Returns on Your Investments in Edge Computing

Relocating compute to the edge has major benefits for today's enterprises. It reduces latency and improves scalability, making it possible to perform real-time analytics at the place where data is generated. This allows companies to deliver new, interactive employee and customer experiences. Whether you're a retailer seeking to improve shoppers' in-store experiences, a manufacturer looking to decrease production downtime, or a healthcare provider seeking better patient outcomes, these benefits are hard to ignore.

But managing an edge deployment can be complicated. Ensuring that the deployment will meet your organization's existing security standards, such as Zero Trust, ups the ante even further. Leveraging the expertise of a trusted partner can accelerate your progress in building a reliable and secure edge computing ecosystem and keeping it up and running—and delivering value—for the long term.

Connection
we solve IT

How Connection Can Help

Connection is your partner for edge strategy, security, and management. From hardware and software to consulting and customized solutions and services, we're leading the way in areas critical to success with edge computing and security.

Explore our Solutions and Services
Modern Infrastructure
Cybersecurity

Reach out to one of our Connection experts today:

Contact Us
1.800.998.0067