CYBERSECURITY IN THE EDGE ERA - A PRACTITIONER'S GUIDE

ALIGNING A ZERO TRUST STRATEGY TO THE IOT- FUELED EDGE

INTRODUCTION

In today's world, business intelligence is the fuel that drives digital transformation. Business intelligence starts with raw data, generated at "the edge" by devices and sensors that make up the world of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT). The exponential growth of IoT and IIoT has created a corresponding explosion of growth in data generated in the wild.

The reward of computing at the edge is the creation of an end-to-end data superhighway from edge to cloud. It is predicted that by 2025, there will be 41.6 billion connected devices generating 79.4 zettabytes of data[1]. Gaining insights from this data at the edge is a foundational requirement for generating business growth in the digital economy. The edge is a launch point for artificial intelligence to be applied - to sense, learn, think, and react in order to solve business problems in near real-time, at the edge. The proliferation of devices on an enterprise's network can also introduce countless security vulnerabilities which cannot be ignored. This paper will discuss the security challenges that come with this transformation and explore strategies to mitigate such risks, anchored by technologies from Hewlett Packard Enterprise (HPE) and Aruba, a Hewlett Packard Enterprise Company.

INTELLIGENCE DRIVES MOST SUCCESSFUL DIGITAL TRANSFORMATIONS

To compete in the digital economy, businesses have been transforming to unlock innovation and eradicate inefficiencies. Digital transformation initiatives are enabling organizations of all types and sizes to be better – and better can mean many things. Whether in the public sector, utilities, manufacturing, or healthcare industries, "better" is tangible and real. Results can range from improved safety, to more effective healthcare, to increased customer satisfaction.

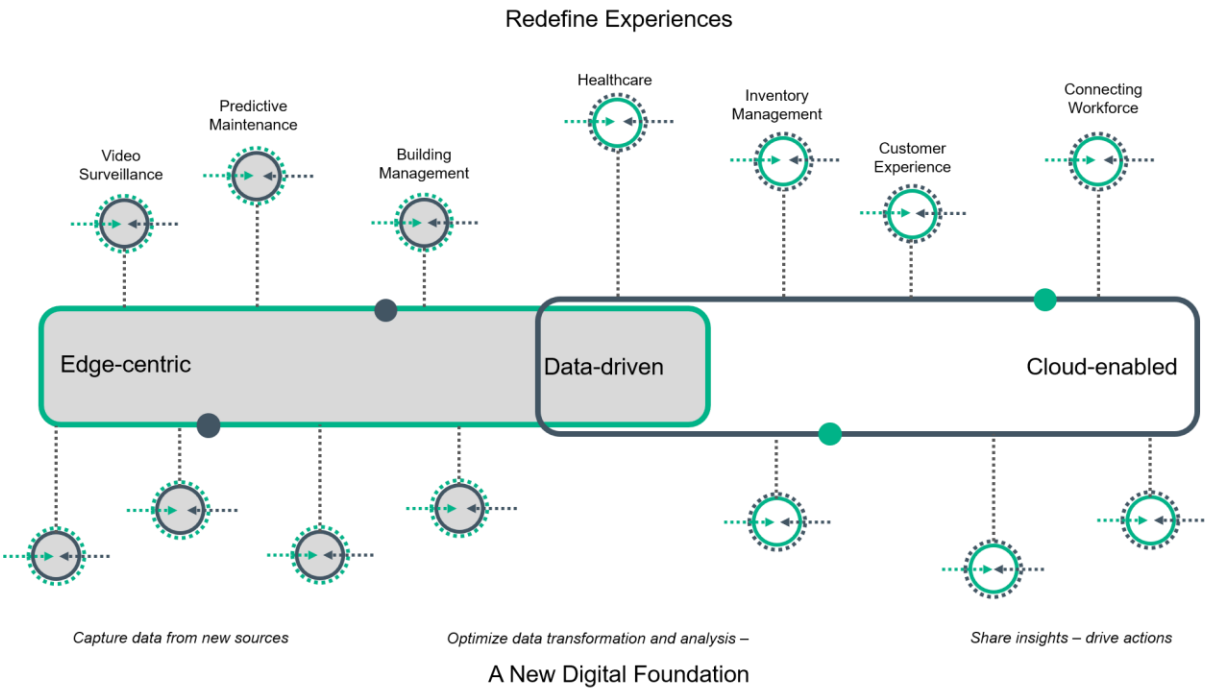
1 – IDC Forecast https://www.idc.com/getdoc.jsp?containerId=prUS45213219

According to a recent study conducted by HPE and Futurum, the top reasons companies undergo transformation projects and implement edge environments include improved security, operational agility, and user experiences.

Interestingly, the barriers to enterprise organizations finding success in digital transformation projects are the very same – lack of security controls implemented, lack of resources, and organizational barriers − that lead to unmanaged devices.

Data-driven intelligence is the core of digital transformation. For instance, a merchant must know a lot about its shoppers – identity, interests, and buying history for starters - to increase customer satisfaction. Likewise, smart cities must process raw data in many forms to deliver safer conditions for citizens and better traffic management for commuters. These usage scenarios start with large amounts of raw data captured from potentially hundreds of thousands of cameras, sensors, and crowdsourced applications.

FIGURE 1: THE DATA JOURNEY AND INTELLIGENCE-DRIVEN OUTCOMES



Source: Moor Insights & Strategy

This is edge computing at its heart – the aggregation, transformation, and analysis of data to drive real-time operational decisions, such as the rerouting of traffic due to an accident on a main artery; the dispensing of life-saving medication to patients during an emergency; or merely a friendly "welcome" and shopping tips to a frequent customer at a grocery store.

For organizations to succeed in their transformation, connectivity from the device to the edge, and from the edge to the cloud and core datacenter, is imperative. Otherwise, the latency associated with the data transformation journey would render many of the benefits related to edge computing moot. The result? Medicines delivered too late, alerts received after traffic routes are clogged, and personalized greetings received by the wrong shoppers.

SUCCESSFUL DIGITAL TRANSFORMATION REQUIRES EQUAL PARTS TECHNOLOGY AND PEOPLE

The most exciting part of digital transformation is how an organization best leverages technology to drive greater efficiencies and effectiveness. However, people are the most critical element of a successful digital transformation. Information Technology (IT) and Operational Technology (OT) must partner deeply, owing to the fact that 72% of edge-computing projects are initiated by OT and Line of Business (LoB) leaders, while digital transformation has typically been initiated by Information Technology (IT) leaders.

In the industrial world, IT and OT have happily co-existed with little to no interaction, with IT managing the “back office” and OT managing “the plant” or “the factory floor.” In today’s digitally transformed operation, these two organizations must work together seamlessly, leading to systems that work cohesively to enable the data-transformation journey.

This cross-organizational integration is more significant than an edict from the CIO or VP of Operations. Overcoming organizational inertia begins with the boots on the ground and must be driven through standard operating procedures (SOPs) and processes. Middle managers and IT/OT professionals must be committed to the success of a digital transformation project.

Because of this, the most effective digital transformation projects Moor Insights & Strategy (MI&S) sees are those that utilize a third party to drive the implementation. When partnering with a consulting and services organization, companies can leverage a broader depth of experience. The partner can act as a broker and an unbiased agent of

change, both technically and organizationally. HPE Pointnext Services is proving to have that depth of expertise and experience.

Security At The Edge Is Critical

A productive edge is a critical and foundational element of a successful digital transformation project. But, for all of the good that comes with deploying a robust edge, wary organizations must account for another critical need: security. Security is a moving target, with constantly changing vectors exposing new vulnerabilities across the network. The explosion of IoT and IIoT as intelligence-contributing devices can make incredibly complex cybersecurity strategies seem out of reach for many organizations. How does IT deliver the required connectivity without exposing the larger network infrastructure as an entry point to hackers?

Though this thinking is understandable, cybersecurity in the era of IoT and edge is achievable. However, a thorough and tested cybersecurity strategy requires a very systematic approach. This begins with a collective "Zero Trust" foundation for every IT project, every product decision, and every action throughout the entire organization, every day. Creating a cyber-resilient organization also requires developing Zero Trust policies that affect the thinking and behavior of all employees. This approach includes training, policies, and exercises that drive an ever-vigilant state.

The cornerstone to a Zero Trust environment begins with infrastructure that is designed and built with an equal, if not greater, focus on security - from the silicon, to the software, to the data. Comprehensive infrastructure security is based on hardware and software and evolves at a pace that enables organizations to stay a step ahead of the shifting threats in the marketplace.

When evaluating infrastructure that spans from the edge to the cloud and the core datacenter, IT organizations should look at security capabilities as a critical evaluation criterion, alongside performance, price, and overall manageability. Companies should also look for IT solutions vendors, such as HPE and Aruba (a Hewlett Packard Enterprise Company), that deliver solutions spanning from the wild west of the edge to the racks of servers that populate the datacenter.

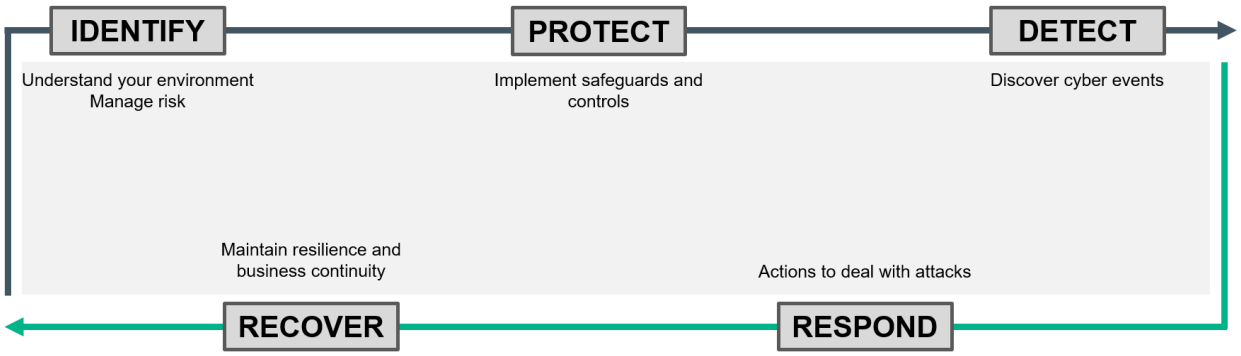
ZERO TRUST IS A MULTIDIMENSIONAL JOURNEY

There is no absolute for an organization seeking to leverage the power of IoT-connected edge in a secure environment. Absolute security – a total lockdown of the network – inhibits business and the benefits of the edge. Conversely, a lax approach to securing the edge is an invitation to hackers. Every organization is unique, with distinct requirements that dictate an adaptive approach to security.

In the context of cybersecurity, comprehensive protection is multidimensional. The right people and devices must have access to the right resources through granular policies based on a number of factors. The granting of access and privileges in a one-dimensional fashion is not enough.

When engaging a third-party to deploy an edge environment that fully comprehends security, companies must consider the vendor's entire portfolio of products, processes, and services. It's the ability to leverage each one of these security elements with the others that turns products into a solution. A professional services organization that understands how to deploy and tune products based on the unique needs of a company will deliver the optimized edge environment, rather than a combination of products with minimal integration.

FIGURE 2: THE ELEMENTS OF A CYBERSECURITY FRAMEWORK



Source: Moor Insights & Strategy

Because of its portfolio of products and services, HPE deserves consideration. The company developed its own security readiness framework, the Intelligent Cyber Security Framework, based on the National Institute for Security and Technology (NIST) standards. This approach enables the mapping of products and services against US government standards to create a globally universal benefit. Solutions such as Aruba

ClearPass enable the creation of granular access-control policies that can be used to provide “least privilege” access to sensitive resources.

The following sections detail how organizations can achieve comprehensive security, from the device to the datacenter, based on the NIST framework. These sections also outline HPE’s technologies and services to demonstrate the completeness of the company's portfolio.

IDENTIFY – THE FIRST STEP TO CYBERSECURITY READINESS

Before an organization can begin to address its cybersecurity vulnerabilities, it must know what those vulnerabilities are. The Identify phase of the HPE Intelligent Cyber Security Framework is designed to assist in understanding the current state of cyber readiness and mapping a path forward to achieve comprehensive security along the edge and in the datacenter.

Organizations can have confidence that HPE and Aruba technologies will enable an exit from the Identify phase with a green light.

- Aruba ClearPass enables full discovery of all users and devices on the network. ClearPass uses artificial intelligence (AI) to find and characterize devices and automatically assign access-control privileges based on policies established by IT.
- HPE Secure Supply Chain delivers assurance that HPE-based infrastructure exits the manufacturing process with a chain of trust established.
- HPE’s Pointnext vulnerability scanning service thoroughly tests the protective measures implemented by IT, delivering a detailed assessment following the scan.
- HPE Infosight’s Security Dashboard provides IT with a quick look into overall network and infrastructure security health.

The strength of HPE and Aruba's portfolio lies in the depth of the collective technology and the ability to leverage a consulting organization that has a wealth of experience in cybersecurity across virtually every industry and every geography.

PROTECT – LOCKING DOWN THE ENVIRONMENT

Once an organization has a sober assessment of its cyber readiness, implementing protections is the next phase. Protection begins with infrastructure designed with

hardware-based security measures complemented by software that manages and protects the edge environment by identifying and controlling the access of devices and people.

Aruba and HPE's combined portfolio is uniquely positioned in the market to deliver comprehensive cybersecurity protections from the edge into the core datacenter. Protecting the edge environment begins with HPE's Silicon Root of Trust (S-RoT) built into its ProLiant and Edgeline server families (MI&S has written extensively on S-RoT, found here). HPE's protections continue through its Secure VM Isolation capability, which includes a variety of tools designed to lock down the server, applications, and data.

Protection rooted in hardware is only half the solution. In this era of IoT, controlling what devices can access a network and what resources are available to that device is critical. Similarly, a simplified process of allowing guest network access to users is essential to managing network protections. Aruba's ClearPass Policy Manager, combined with network traffic segmentation via Policy Enforcement Firewall (PEF), delivers lockdown protection as organizations deploy more and more devices to the edge.

DETECT – DISCOVERING CYBER EVENTS IN REAL-TIME

Cyber events are inevitable. Even the most prepared organizations will encounter an attack. Speed is the key to dealing with cyberattacks. How quickly can the threat be detected, mitigated, and removed, with all systems restored to a pristine state? This immediate recognition requires tools that are constantly scanning and searching for anomalies that indicate an organization is under siege, such as spoofed drivers and firmware, new executables, unusual network traffic patterns, and excessive read/write/copying of files.

The strength of HPE and Aruba is a Zero Trust philosophy in the design and development of products, combined with the simplicity of use and management. Together, HPE's security-focused infrastructure and Aruba's depth and experience in network security are far stronger than the individual parts. The integrated approach to securing the edge environment is stronger than point products that simply co-exist.

RESPOND – DEALING WITH ATTACKS IN REAL-TIME

Once a threat is detected, the effectiveness of responding to a cyber event is measured by the speed at which such a response takes place, as well as the thoroughness of such actions.

After a threat is detected and verified, Aruba's ClearPass Manager quarantines and blacklists the malware, protecting against future attacks.

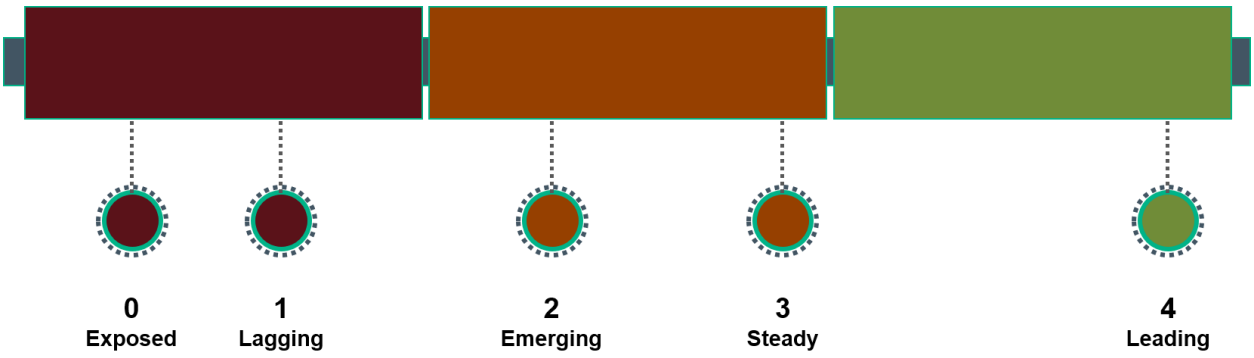
RECOVER – COMPLETING THE INTELLIGENT CYBERSECURITY FRAMEWORK

Detect, respond, and recover: the three elements of cyber resilience. The question is – how fast can your organization recover from a ransomware attack that has "bricked" servers and encrypted customer data? If the answer is in days or weeks, you lose. Similarly, if the answer is, "once the hijackers have been paid," again, you lose. Without a fast and complete recovery, nothing else matters, and this is where HPE shines.

HPE's Server System Restore capabilities, combined with data stored in StoreOnce Integrity Plus, allow IT organizations to restore edge and datacenter servers with just a few clicks (MI&S has covered this capability extensively here).

For recovery on the edge, Aruba's ClearPass Manager quarantines and manages the re-authentication of impacted devices.

FIGURE 3: CYBERSECURITY CAPABILITY AND MATURITY MODEL



Source: Moor Insights & Strategy

CYBERSECURITY READINESS – HOW READY IS YOUR ORGANIZATION

Much like IT maturity, an organization's cybersecurity readiness can be measured. While a variety of models with deep levels of granularity exist, this paper will use a higher-level scale to measure readiness. In this model, we rank an IT department's cybersecurity readiness by the organization's implementation of each of HPE's Intelligent Cyber Security Framework phases – identify, protect, detect, respond, and recover.

0 = Exposed No real consideration of security. Unknown vulnerabilities. Infrastructure deployed with default settings. No training. No policies. Basic back-up and disaster recovery policy.

1 = Lagging Basic protections in place. Basic policies in place and enforced. Minimal technology deployed for protection, detection, and recovery.

2 = Emerging Employees trained. An incomplete collection of policies for cyber incident response. Maybe basic cyber insurance policies. Some level of IT staff training. Software deployed for discovery, authentication, access controls, and incident response. Documented and tested cyber response and recovery policies.

3 = Steady Regularly scheduled organization-wide training. IT cyber-response team identified. Strict enforcement of cyber policies. Scheduled cyber incident exercises to shore up readiness. Deployment of software utilizing AI/ML to hunt, detect, and mitigate threats.

4 = Leading Zero Trust infrastructure. Zero Trust policies. Cybersecurity strategy co-developed and implemented with an unbiased third party. Cybersecurity strategy regularly tested for vulnerabilities and organizational readiness. Hardware-based security combined with software for complete cyber-incident detection, response, and recovery capabilities.

For more comprehensive models based on government standards, MI&S recommends the following models:

- US Department of Energy Cybersecurity Capability Maturity Model (C2M2) found here.
- The NIST Cybersecurity Framework can be found here. While NIST does not consider this a traditional Capability Maturity Model (CMM), this framework is useful in measuring and tracking cybersecurity readiness.

TYING IT ALL TOGETHER: FULLY EMBRACING DIGITAL TRANSFORMATION WITH CONFIDENCE

While organizations may be aware of the benefits of digital transformation, they have not fully embraced the power of IoT and IIoT, due to the misperception that these environments cannot be adequately managed. This management includes the integration of organizations, the ability to leverage raw data generated at the endpoint, and a security strategy that must be a vital element of any edge deployment.

Moor Insights & Strategy believes HPE can assist enterprises across virtually any industry in their IoT-fueled digital transformation journey. HPE does more than design infrastructure that can fit in tight spaces with high (or low) thermal requirements. The company develops strong integration between the analytics tools that transform data into intelligence and the proprietary sensors and devices from which that raw data originates. In this regard, the company is unique (for more information on HPE's enablement of edge computing, read this research paper from MI&S).

MI&S believes HPE is uniquely positioned to secure the edge environment, from factory floors and office buildings to retail outlets and oil refineries. The combination of HPE and Aruba to manage infrastructure, network, applications, and data is currently unmatched.

EVERYTHING AS A SERVICE, EVEN SECURITY

One area in which HPE and Aruba seek to establish leadership in the IoT and edge market is delivering its security portfolio as a service. The company has publicly stated that by 2022, all HPE product offerings will be available as a service. This go-to-market model can have great appeal for organizations wanting to deploy an end-to-end IoT/edge solution that fully embeds security. The complexity and upfront costs associated with such a solution can seem prohibitive, but consumption-based pricing simplifies the barriers to adoption by shifting costs.

Delivering security as a service also democratizes digital transformation, enabling companies of all sizes to deploy, manage, and secure IoT environments without the in-house expertise and budget previously required.

CALL TO ACTION

Digital transformation without leveraging the power of the IoT and IIoT is incomplete. It's the business intelligence gleaned from the edge that enables better outcomes across any industry.

Every opportunity has an element of risk. In an IoT-fueled edged environment, that risk is rooted in - and can be mitigated with - cybersecurity. The risk is significant. Anecdotally, feedback from MI&S clients has shown this risk to be a barrier to the adoption of edge-integration efforts. While virtually no IT organization is comfortable with its security efforts, introducing an environment with so many more potential vulnerabilities is unfathomable.

Moor Insights & Strategy believes this collective thinking, though understandable, is misguided. The integrated HPE and Aruba portfolio of cybersecurity products and services can provide complete security to any environment – from the device connecting a wireless network on the far edge to the servers that power the data transformation necessary to deliver business insights. Additionally, the HPE and Aruba portfolio enables adherence to every phase of NIST's Cybersecurity Framework.

Finally, building a comprehensive cybersecurity strategy is difficult due to internal and external dynamics. Lack of expertise, resources, and budget coupled with organizational biases (the proverbial "it only happens to others" mentality) can impact an IT organization's reach and ability. Trying to navigate the laws and standards around data governance, privacy, and the resulting impacts on a security strategy can be overwhelming. Because of this, enlisting the help of an organization such as HPE Pointnext to navigate these waters can reduce the cost and time associated with implementing security controls.

For more information on HPE and Aruba, visit here.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR
Matt Kimball, Senior Analyst at Moor Insights & Strategy

PUBLISHER
Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
This paper was commissioned by Hewlett Packard Enterprise. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.