SECURITY FOLLOWS COMPUTE TO THE EDGE

THE DRIVE FOR BETTER AGILITY & BUSINESS RESULTS MUST ENCOMPASS DATA PROTECTION

EXECUTIVE SUMMARY

Edge computing is becoming more prevalent for both the Industrial Internet of Things (IIoT) and traditional operational applications. Companies need to protect their data better at remote locations and all along the path back to central datacenters.

Businesses want real-time analytics for their operations to accelerate decision making. However, the speed to deploy and manage, combined with lack of automation / instrumentation required to get this critical data, leaves businesses without the information essential to drive real-time insight. When data is acquired, accessed, and processed at the edge, businesses realize superior insight through real-time analysis. Proximity to the data-generating devices enables a business to achieve faster responses for better decision making.

Latency, traffic congestion, and high bandwidth costs are the primary barriers that arise from moving data back-and-forth between the cloud and the factories, mines, oil rigs, or other remote locations where data is generated. These factors are putting extreme pressure on the traditional centralized IT model, and in the process, transforming how enterprises operate.

As a leader in compute and mobility, Hewlett Packard Enterprise (HPE) has positioned itself to help businesses better navigate this edge-based security structure.

NETWORK EDGE NOW TRANSFORMING IT ARCHITECTURES

To become more competitive, businesses are turning to new technologies such as the Internet of Things (IoT) or accessing data through apps running on mobile devices like tablets and smartphones. Sensors connected to a wide range of industrial equipment such as pumps, motors, and conveyer belts are also enabling everything to be instrumented, monitored, and managed.

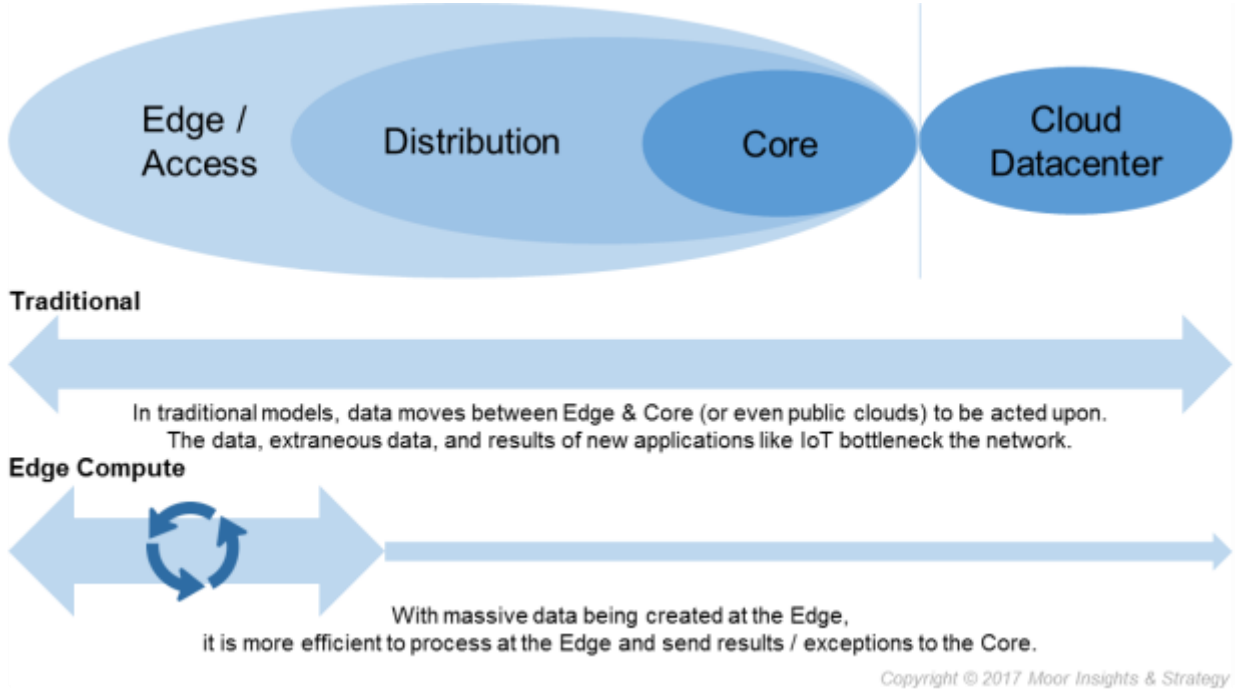
However, these devices live out on the network edge at remote locations far away from the datacenter. The data these devices create has challenges in both location and magnitude. These challenges are leading IT leaders to change where compute resources reside to obtain better value from the data. Organizations that have successfully moved compute resources to the edge have realized two key benefits.

Copyright © 2017 Moor Insights & Strategy

First, acting on data as close as possible to where it is generated and collected reduces latency in decision making. Sending data from the edge back to the datacenter (or a public cloud) takes too much time and reduces effectiveness. For instance, real-time operational decisions for equipment operating deep inside a coalmine can be executed quicker when closer to the managed drills, conveyer belts, and ore carts.

Second, by acting on edge-generated data, the time and cost impacts on networks can be greatly reduced. Some networks are already overtaxed with traffic today, and this congestion will only get worse as traffic from IoT devices and digital transformation projects increases. Satellite communications for remote locations can be tens of thousands of dollars per month, significantly increasing costs if data from these remote locations needs to be backhauled to the corporate datacenter. By reducing the amount of traffic back-and-forth, businesses can extend the value of their transport network, optimizing those investments by amortizing the costs over a longer useful life.

FIGURE 1: COMPUTE AT THE EDGE



(Source: Moor Insights & Strategy)

Edge compute reduces the network load and extra transmission costs by acquiring, filtering, and analyzing locally. Only the results of data processing and analysis need to be moved to the datacenter, not the complete dataset. In applications where resulting control and actuation takes place at the edge, there may be no need to send any

Copyright © 2017 Moor Insights & Strategy

information at all to the datacenter. In addition, bandwidth restrictions, security, reliability, or data sovereignty policies may prevent (or render unnecessary) any edge to datacenter communications.

ATTACKS ARE BECOMING MORE SOPHISTICATED

Businesses today are embracing the concept of "digital transformation", the wholesale change in how they operate. Digital transformation aligns the company direction around information and data sources to help drive better agility and deeper insights. A change to digital transformation requires a company not only to retool its IT environment but also refocus the skills that the IT staff will require.

A key step to evolving an organization's digital transformation strategy is addressing security when moving compute to the edge. This compute at the edge now exposes the network and applications to new vulnerabilities. Different vectors of attack are increasing every week, creating new challenges for both profiling and responding. Additionally, the increase in sophisticated attacks is coinciding with changes in how businesses are organizing IT and leveraging devices.

In August 2016, at the DEF CON 24 hacking conference, researchers reported they found 47 new vulnerabilities affecting 23 devices from 21 different manufacturers. It was the second year that the IoT Village was held, resulting in the discovery of 113 critical vulnerabilities across consumer and business IoT products in that two-year span. Success in identifying these IoT threats shows that many device manufacturers in this tech segment continue to ignore security best practices.

Threats that use IoT devices, such as the Mirai and Dyn attacks, can create massive distributed denial of service (DDoS) attacks that flood networks, blocking out legitimate traffic and overloading systems. If these attacks start at a company's edge, they could easily overwhelm a company's core datacenter services by consuming an undue amount of resources. Even if the attack is targeted at an outside company, because the traffic is flowing over the host network, the host company may suffer the same impact as the targeted company. These attacks have become more pronounced, driving a stronger need to protect a business' bottom line. It is estimated that this year will see over half a million IoT devices compromised.

Additionally, the new mobile-centric environment sees emerging threats coming from smartphones, tablets, and their associated apps. With an estimated 50% of all mobile devices communicating via unencrypted channels, mobility also presents a large challenge to security.

Copyright © 2017 Moor Insights & Strategy

With the increase in devices and use cases at the edge, businesses need to be more thorough about security as the changing face of client access exposes a company to new and previously unseen vulnerabilities.

ESTABLISHING A NEW SECURITY MODEL FOR EDGE COMPUTING

Similar to centralized data management, today's enterprise security models feature a hierarchical structure, whereby a control plane governs both access and security. The control plane is centralized in the datacenter core and is accessed through a smaller set of controlled data entry points. IT can then exert a tight rein on both access and security, which works well for traditional applications. However, as applications have grown in complexity, creating even larger datasets, this governance model becomes more difficult to manage, because at the edge, things are different.

Edge-generated data often enables time-sensitive decision making that is considerably more difficult in a hierarchical security model because of the latency involved. As a result, businesses need to ensure that the data and resources at the edge are as secure as if they were in the core.

Data security is even more important when control decentralizes. Adding complexity is the intersection of Information Technology (IT) and Operational Technology (OT). The melding of these two worlds brings new equipment, protocols, and devices into the IT domain that had previously lived within their own proprietary environments. Knowing that 20 billion IoT devices will be deployed by 2020, each most likely carrying a number of undiscovered vulnerabilities, staying ahead of edge security protects businesses.

Security is not simply a wall that is erected; it must be holistic and span the entire infrastructure. It is not enough to put up a defense and believe it is impenetrable. Businesses should assume attackers can get through and, once inside, could reside within the network for a while, testing for vulnerabilities—from the edge back to the core.

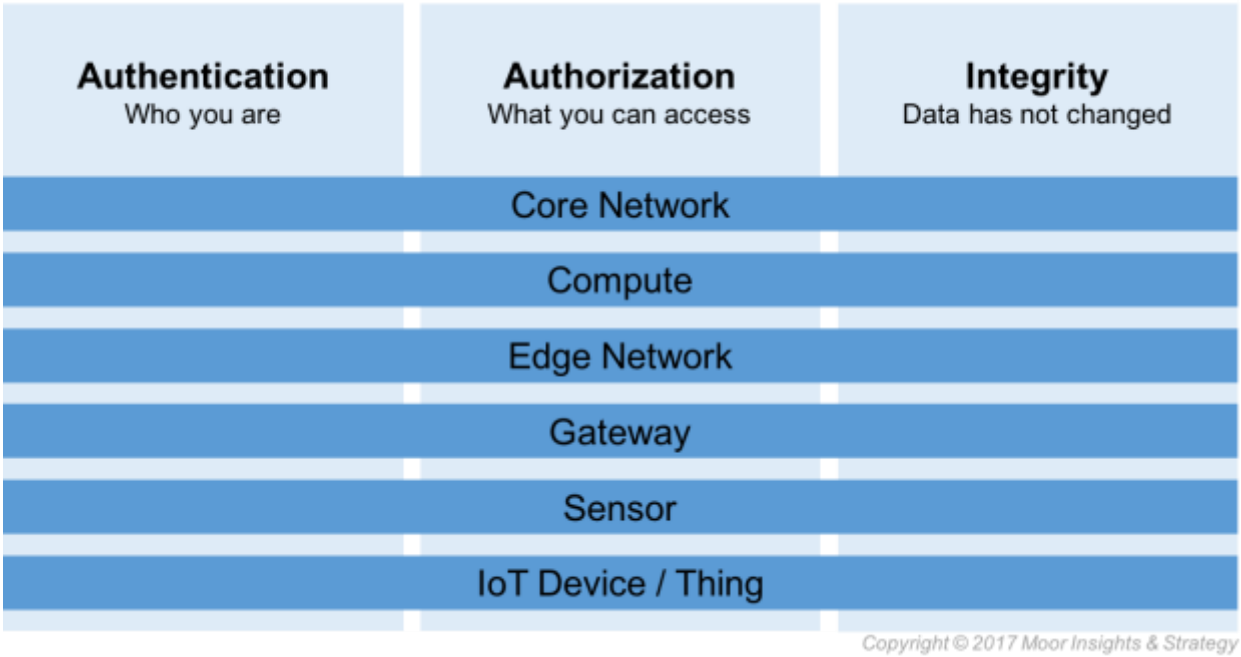
As within the datacenter, edge-resident vulnerabilities can result in data loss, data corruption, compromise of systems, denial-of-service, loss-of-control, or even ransomed information. Failure to secure the entire edge chain up and through to the cloud or corporate datacenter can result in severe business impacts, as edge-based vulnerabilities can ripple throughout the rest of the IT and OT environments.

These vulnerabilities are not necessarily limited as a threat only to the edge. They may open holes that enable intruders back into the heart of the datacenter. As an example, the 2013 Target Stores hack was staged through the edge. The hack exploited an

Copyright © 2017 Moor Insights & Strategy

HVAC vendor to gain access to Target's core networks and ultimately its most valued asset—customer payment information.

FIGURE 2: EDGE SECURITY LAYERS



(Source: Moor Insights & Strategy)

At the edge, security must be localized to reduce the probability of data compromise from traversing across vast network distances to datacenters.

Security enforcement teams must answer these questions:

- **Are you who you say you are?** Authentication ensures devices and users are who they say they are by comparing them to known profiles / managed identities.
- **Are you authorized to use the network or resource?** Authorization gives known users and devices the right to use the network or resource as policies dictate.
- **Can the data integrity be ensured?** Security analytics are another layer of checks and balances that provide validation (in real-time or in retrospect) to help ensure protocol is being followed, policies are being enforced, and data is not changing through the process.

Securing every level of edge resources is critical, as it is expected that 2017 will experience large-scale IoT security breaches.

Copyright © 2017 Moor Insights & Strategy

TABLE 1: LAYER SECURITY CONSIDERATIONS

Layer	Security Considerations
Device	As the first step in the chain, devices must be identified, authenticated, & secured from physical & operational issues, as well as identity spoofing that may enable an outside attacker to inject compromised data into the system.
Sensor & Access Point	Security systems for this layer must authenticate devices & network connections to grant access to gateways. Integrated sensors / APs will need to be authenticated, often during the purchase process or after installation. Constant connectivity authentication is required to ensure that the device's data stream has not been compromised.
Gateway	Gateways collate traffic & assign the right streams & data to corresponding applications or data lakes. Because gateways have a CPU / OS, the security solution will also need to provide machine-level authentication to maintain data integrity up the chain. Policy managers running on the gateway help ensure authentication & secure access.
Network	Processing edge-generated data locally reduces the number of flows that must be aligned within the network security model. All network edge devices need the ability to handle distributed security policies. Machine-to-machine (M2M) communications for IIoT devices must be authenticated & continuously monitored to protect against tactics such as spoofing, man-in-the-middle attacks, content compromise (changed data), replay attacks, & more.
Compute	Physical access control is an important piece of security, as edge systems may lack the strict physical access control that datacenter systems receive. Ruggedized configurations & features can also assist in protecting data integrity as well.

THE HPE SOLUTION FOR EDGE SECURITY

As a key component of the company's Intelligent Edge strategy, HPE delivers security to the edge through a combination of hardware and software. Hardware security is delivered through edge computing solutions (Edgeline gateways and converged systems), as well as through Aruba access points and sensors. On the software side, the Aruba ClearPass and the newly acquired Niara products provide authentication, access control, and monitoring of users, systems, and software along the edge.

- **Edge computing** HPE Edgeline Converged Edge Systems feature embedded security designed to prevent tampering. I/O ports can be disabled, a secure BIOS password is available, and secure boot process are integrated into the systems.
- **Gateways** Edgeline gateways feature the same hardening and physical access security capabilities of the converged systems. Both the wireless and 3GPP interfaces can be secured through the Aruba ClearPass policy manager to help ensure only appropriate devices have access. Additionally, their ability to run Aruba ClearPass and also Aruba Secure VPN means these devices can help protect the integrity of both the connections and data at the point of acquisition while providing the secure handshakes as the data moves to the compute layer.

Copyright © 2017 Moor Insights & Strategy

- **Wi-Fi Infrastructure** HPE Aruba Wi-Fi access points are designed to deliver a secure and monitored ingress point for IoT and mobility. By adhering to the 802.11i security protocol (WPA2) and integrating with Aruba ClearPass for role-based policy assignment, these access points enable security enforcement at the edge of the network to help minimize risk.
- **Access control** Aruba ClearPass Policy Manager delivers visibility and enforcement that can also be integrated with third-party products for end-to-end security at the edge.
- **Device profiling** Aruba ClearPass Universal Profiler helps businesses see what is on their network through multi-vendor identification and classification, granting access based on characteristics like device type, ownership status, or OS.
- **Behavioral analytics** HPE recently acquired Niara, a behavioral security analytics firm that uses machine learning and advanced analytics to identify anomalies at the edge, helping prevent attackers from reaching the core. Once identified by Niara, ClearPass can be used to isolate the attacker and the exposed network until it can be fully investigated by security teams.

To wrap these tools into a complete solution, HPE offers a full set of security services to assist with risk management, security operations, identity & access management, infrastructure, and endpoint security, helping businesses secure their edge compute environments. Businesses can engage HPE as a "full suite provider" of not only the infrastructure and knowhow to implement, but also as a company that can help define, execute, and even run the security for that infrastructure.

THE MI&S VIEW OF EDGE SECURITY

Edge security is critical to businesses, because new agile business models can expose new vectors for attack, while the overworked IT teams struggle just to keep the existing infrastructure secure. The growth of IoT data in both size and velocity, as well as its growth in business value, creates an intersection of concern for many.

The combination of IT and OT creates an environment where a shared ownership must exist to protect a business' critical data. Over time, we predict that the edge—especially considering the growth of IoT and mobility—will present itself as the largest opportunity for attackers. Just as the edge presents the largest opportunity for businesses who want to transform their operations and drive additional efficiencies, it can also be their largest liability if not secured properly.

Copyright © 2017 Moor Insights & Strategy

Edge security must evolve rapidly to keep up with the threat landscape. There has been a large increase in state-sponsored attacks that focus on businesses (Sony, Yahoo!, *etc*.), and Honeywell recently reported state-sponsored activities in 20 of the 30 industrial sectors they follow.

Sophisticated attacks, such as Mirai will continue as the universe of insecure devices grows quickly. A key dynamic of attacks is the volume of traffic that can be created to assist the compromise. We are beginning to see attacks, like the Dyn DDoS attack, driving terabit-level traffic.

As the edge becomes a more critical part of the network, more attacks will focus there. Protecting the data and compute at the edge is essential to protecting key business assets. But just as important as protecting the edge is protecting the border between the edge and the core network. A terabit-scale attack, if it can overrun the edge security, could then flood the core network very easily.

With the liability from attacks continuing to rise, an implicit cost comes both from compromise of the network as well as from theft of IoT data that could be used by a nefarious third party, either as industrial espionage or ransom. In the past year, the worldwide average cost of a compromise increased 23%, with the typical US company suffering a $17M impact from compromise. Clearly, there is a significant business impact in not securing data. The data that resides outside the datacenter is potentially the most vulnerable in the enterprise and must be protected the same way.

Call to Action

To match the changing needs of today's agile businesses, the focus of control is moving from the core towards the edge of the network, driven primarily by IoT and mobility. While this transition can help drive more efficiency, it fundamentally changes the security approach, creating a more distributed model that must stress the same degree of protection out at the edge that IT traditionally delivered within the datacenter.

HPE offers a diverse portfolio to help businesses make a secure move towards the edge. Edgeline and Aruba are two portfolios that can help enable IT to deploy and secure at the edge. As this change unfolds, businesses should research their options. A good starting point is the 7 reasons that businesses need to compute at the edge as well as how HPE can help keep compute secure at the edge.

Copyright © 2017 Moor Insights & Strategy

IMPORTANT INFORMATION ABOUT THIS PAPER

AUTHOR
John Fruehe, Senior Analyst at Moor Insights & Strategy

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

EDITOR & DESIGN
Scott McCutcheon, Director of Research 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
This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

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 considering new information or future events.

© 2017 Moor Insights & Strategy. Company and product names are used for informational purposes only and may be trademarks of their respective owners.