HPE GreenLake

5 best practices all enterprises should apply to secure edge-to-cloud environments

The old hub-and-spoke approach to data networks isn't dead, but it's barely recognizable these days.

Between most workers going remote or hybrid, the emergence of IoT devices, and the arrival of electronic and autonomous vehicles, 50% of enterprise-generated data is expected to be produced outside traditional centralized data centers or clouds by 2025, according to Gartner.[1]

More than ever, that means organizations will start putting servers, storage, and processing power closer to where the data is being generated—shopping malls, oil fields, airports, hospitals, factory floors, and warehouses. It is basically any place where they can facilitate the rapid exchange and utilization of the data we'll use in our personal and professional lives.

[1] "Predicts 2022: The Distributed Enterprise Drives Computing to the Edge," Gartner, Oct 20, 2021

It's all good from an innovation standpoint. But cybersecurity professionals are more than justified in feeling a little stressed about the difficulty of safeguarding edge-to-cloud computing.

Indeed, even as 69% of organizations plan to boost edge investments in the next two years, IDC research found that 70% of survey respondents are highly concerned by the security challenges.[2] Further, with 25% of organizations surveyed saying the number of identities they need to manage grew tenfold between 2020 and 2021,[3] 70% of security and IT professionals admit to being overwhelmed by the **significant complexity** this presents, according to a recent survey by Axiad, which offers a passwordless security platform.[4]

"Security departments have spent decades improving how they protect data behind firewalls but now have to redefine and extend those models for highly distributed workloads," says Simon Leech, director with HPE Cybersecurity and Digital Risk Management Center of Excellence. "It can be a lot of pressure because edge-to-cloud computing is changing so swiftly, and security practitioners aren't always sure where to put their emphasis in order to keep pace."

Here are five best practices IT security leaders should adopt to get a better handle on today's complexity and to position their organizations for the future:

1 Embrace security by design

Most IT security professionals know that if they are the final stop in product design and development lifecycles, it's too late. The same goes for edge-to-cloud environments. Security must be actively involved from the get-go to ensure these protocols are integrated into every program, policy, and control. What's more, because there are so many specialized and attackable components in edge-to-cloud environments, holistic models must cover every part.

"Make sure every element of your infrastructure and data processing environments can be trusted and that everything is provisioned and configured in ways that reduce risk to acceptable levels," says Leech. "Strive to become a secure-by-design culture."

[2] "Securing the Edge: How Edge Is Architected Will Determine How Security Is Designed," IDC, Feb 2022

[3] "Identities and Security in 2021," Dimensional Research survey sponsored by One Identity by Quest

[4] "70% of Security/IT Professionals Say They Are Overwhelmed by the Complexity of their Authentication Systems," Axiad, Sep 29, 2022

Build unified platforms

The security discipline has long recognized the importance of having full visibility into everything that accesses the network. After all, you can't manage or protect what you can't see or don't even know exists. For this reason, it's often best to have a common platform and dashboard. But not just any platform. Organizations should strongly consider platforms built for this evolving digital computing landscape, advises Jennifer Cooke, research director for IDC Worldwide Edge Strategies. Also, consider platforms powered by technologies such as artificial intelligence to automate security management, policies, and controls at scale, she says.

"IT staff have a hard enough time keeping track of assets that are actually in their data centers and understanding what's running or being updated at any given time," Cooke says. "When you have exponentially more pieces of equipment outside the data center, it becomes almost impossible to make sure everything is up to date with security patches and adhering to policies without automation."

2

3

Insist on integrity and verification

Zero trust has been the name of the security game for several years now. The idea that every person and machine is considered untrustworthy until proven otherwise should also apply to edge-to-cloud computing, analysts say.

Of course, in increasingly distributed networks, identity and access control become exponentially more difficult with each additional user or endpoint. Monitoring and verifying who and what are accessing the edge-to-cloud path can be equally problematic.

From a technology standpoint, automation will help. Fine-grained network approaches such as compartmentalization and microsegmentation can also help enforce zero trust. But one-off tactics such as these are not enough. Organizations need a platform that brings it all together, enforcing security from the silicon level and infrastructure hardware to software and workloads.

Don't neglect physical security

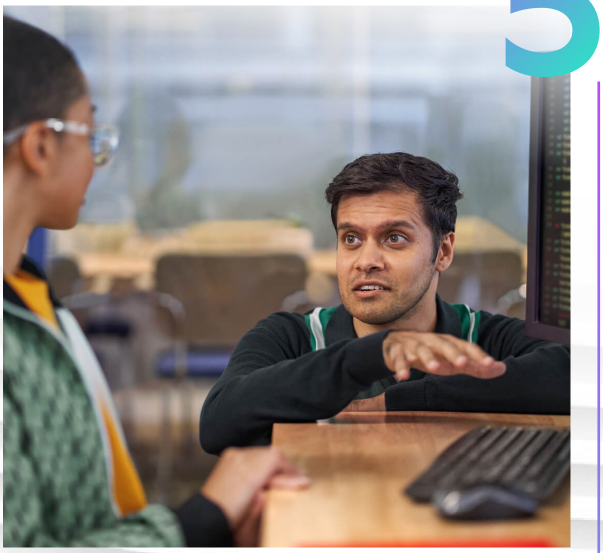
Back in the client-server days, most networking equipment sat in cooled and locked rooms in buildings employees weren't allowed to see. But with edge-to-cloud infrastructure, critical information could be hosted in a less secure or even hostile environment. It only takes one malicious or negligent act to undermine an edge device, and the risk of this is exponentially greater in an edge-to-cloud world.

As Cooke suggests, someone could easily, intentionally or unintentionally, walk off with a critical piece of edge equipment, resulting in network failure. A wandering hacker, or perhaps an angry insider, could similarly introduce malware into the device. The possibilities for disruption are endless.

One obvious solution is to lock edge computing devices behind closed doors where only vetted, authorized IT staffers can access them. Bonus points if biometrics such as retinal or palm scans are involved. An additional measure, says Cooke, is to put all critical equipment inside hardened boxes or cages.

4

5



Build a shared responsibility model

Many IT security practitioners prefer to do it alone when defining a strategy and implementing it. But in the emerging edge-to-cloud world, with data being processed in so many disparate and sometimes hard-to-reach locales, that can lead to disaster.

In many cases, the better alternative—especially for young or immature organizations— is to partner with an experienced and trusted service provider. Given an ongoing lack of skilled cybersecurity talent, this helps organizations tap into a pool of expertise they might not otherwise find.

"Right now, the defining quality of top CIOs is the ability to choose partners to complete their objectives," says Cooke. "Those who are more advanced understand their role is to be the orchestrators of their environment—not to be do-it-yourselfers."

Partnering with service providers on security also requires establishing a shared understanding of one another's roles and responsibilities so there are no misunderstandings or disputes. "The importance of being a cyber resilient organization continues to grow," says Leech, "and it's important to understand what your responsibilities are and how you can handle them in a hybrid world when working with service providers."

Securing edge-to-cloud computing will always be somewhat stressful, but it can be less so if organizations adopt best practices such as these and continually update them. Just as data never stands still, neither can IT security professionals.

As Bobby Ford, senior vice president and chief security officer of HPE Cybersecurity and Digital Risk Management, recently said, "Understanding and addressing security challenges upfront can give you the upper hand in preventing, detecting, and responding to cyberattacks."

That goes double for safeguarding the edge-to-cloud digital landscape.

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Learn more at
greenlake.hpe.com/security

Explore **HPE GreenLake**

Hewlett Packard
Enterprise