FIRESIDE CHAT PAPER

Redmond MAGAZINE

THE END OF THE TRUSTED NETWORK

Adopting the Zero Trust framework can greatly improve an organization's security posture.

In these days of the rapidly evolving threat landscape, expanding network perimeters, and more services being provided in the cloud, the concept of security must evolve as well. Established security solutions that once worked perfectly well are likely no longer effective in this new environment.

With mobile devices, cloud services, and data stored in myriad locations, the very concept of the network perimeter has essentially evaporated. "There is no perimeter. The four walls surrounded by trusted network, that's quaint at best and actually very dangerous," says Stephanie Balaouras, vice president and research director serving security and risk professionals at Forrester Research.

Balaouras and several other security professionals spoke during a webcast, "4 Powerful Levers from Lenovo to Implement Zero Trust." The focus of the presentation was around the concept of Zero Trust, and how adopting that framework and a data-centric approach can greatly improve an organization's security posture. The Zero Trust model was originally developed by John Kindervag in 2010. Kindervag was a principal analyst at Forrester Research at the time.

While enterprises across the globe continue to make great strides toward better securing their infrastructure and their data, there is much left to be done. "As companies become more explorative, the risks go up as you move to unknown solutions and unknown types of networks and riskier environments," says Thorsten Stremlau, global commercial PC business management director at Lenovo. "The digital transformation and different solutions are opening new challenges in terms of security."

Balaouras agrees. "We're seeing the same thing," she says. "As organizations undergo their digital transformation, the cloud is critical to that transformation. It allows companies to scale, to be nimble, and to reduce costs; but it comes with an enormous amount of risk. Your sensitive data is with a third party."

And organizations are increasingly relying on the cloud. "Today 57 percent of companies are planning to adopt the public cloud in some form, if they haven't already done so," she says. "Next year, that number will be even higher."

THE ZERO FACTOR

Forrester's report "The Eight Business and Security Benefits of Zero Trust" zeros in on many of the aspects discussed during this webcast. The report specifies the following eight benefits to adopting Zero Trust:

Cover: Michael Traitov / Shutterstock.com

- Improves network visibility, breach detection, and vulnerability management
- Stops malware propagation
- Reduces capital and operational expenditures on security
- Reduces scope and cost of compliance initiatives
- Eliminates inter-silo finger-pointing
- Increases data awareness and insight
- Stops exfiltration of internal data into the hands of malicious actors
- Enables digital business transformation

“MOST LARGE ENTERPRISES ARE MOVING TO A HYBRID ENVIRONMENT; WITH SOME DATA STORED ON-PREMISES AND SOME IN THE CLOUD.”

—STEPHANIE BALAOURAS, FORRESTER RESEARCH

The changing infrastructure platform—from on-premises data centers to cloud-based services—requires an equally profound shift in security solutions and protocols. “Security leaders are planning to spend more on cloud security,” says Balaouras. “Most large enterprises are moving to a hybrid environment; with some data stored on-premises and some in the cloud.”

This dramatic change has not always mapped to an equivalent change in security. “The environment is changing, but security is not changing along with the environment,” she says. “Security teams are still spending most of their budget on on-premises solutions. How do you actually protect data and apps in the cloud with a bunch of on-premises security solutions?”

This shift is driven not only by the move to the cloud, but also the increasing importance and value placed on corporate data. Data is the new currency. Organizations are realizing that and trying to manage that data as a business-critical resource. “This is the data economy,” says Balaouras. “Today, 48 percent of enterprises are planning to commercialize the data they own.”

Some security professionals struggle to understand the full value and context around data. “They don’t know how sensitive it is. They don’t recognize its value to the business. This is another gap between the digital transformation and where security is today,” she says. “So that’s the current state of the union.”

According to Forrester’s research, more than half of enterprises have suffered at least one breach; and that’s just the enterprises that have even realized they’ve had a breach. Many industry reports indicate a sizeable number of enterprises don’t even learn about a breach until months after, says Balaouras.

This fluid security and threat landscape, the increasing reliance on cloud-based platforms, and the business-critical nature of data has led to the disappearance of the trusted network. “The trusted network is gone. We should assume all networks and network traffic is untrusted,” she says. “The digital transformation already makes for a challenging backdrop. The attack surface continues to grow. You have rapid development and non-linear supply chains; it just makes the environment more challenging every day.”

DIVE INTO THE DATA

Getting closer to the Zero Trust model can help companies cope with the rapidly evolving nature of the cloud-based infrastructure and threat landscape. And fundamental to that effort is adopting a data-centric approach. “Using a data-centric approach, you can maintain control of data no matter where it’s stored, where it’s processed, and where it’s transmitted,” says Balaouras.

Taking a full inventory of corporate data, properly and clearly classifying that data, and achieving a level of visibility into that data are important first steps. “You have to get your arms around your data,” she says. “You can start small if you have petabytes of information, but you need to start.”

Once an enterprise has a more accurate view of its data store, then it can begin applying the appropriate security controls based on the data sensitivity. Not all data needs to be protected in the same way. Take the most sensitive data, then apply controls such as encryption and limiting access.

Another critical capability is to maintain visibility into that data no matter where it resides. Just because a cloud service or storage provider may be storing corporate data elsewhere, that does not transfer the liability for that data. Liability always stays with the company. “You have to maintain that level of visibility to identify threats to the data, any existing vulnerabilities that leave you exposed, and any breaches that may be in process,” says Balaouras.

> “WE CALLED IT ZERO TRUST BECAUSE WE REALLY WANTED SECURITY PROFESSIONALS TO RECOGNIZE AND ELIMINATE THIS DANGEROUS IDEA THAT THERE IS A TRUSTED NETWORK.”
>
> — STEPHANIE BALAOURAS

Security solutions and protocols focus on the data itself, not some device or endpoint. “The policies apply to the data itself: who has access, how it should be protected,” she says.

While it can seem overwhelming for organizations with massive data stores, it’s important to at least start the process.

Taking this data-centric approach can help enterprises get closer to the Zero

Trust model. And even the name Zero Trust is important because it captures the philosophy behind this security model. “We called it Zero Trust because we really wanted security professionals to recognize and eliminate this dangerous idea that there is a trusted network,” she says.

While it may be comfortable to assume partners will treat your corporate data as if it were their own, that can be a dangerous assumption. Zero Trust eliminates those assumptions. And that helps achieve a stronger level of security because those dangerous and misplaced assumptions of trust can undermine the security posture. Simply stated: with Zero Trust, you operate under the assumption that someone is already stealing your data.

You are always inspecting traffic, so you have that visibility across your environment no matter what.”

Another approach is the idea of eliminating the perimeter. Instead of a larger, monolithic network perimeter, think of creating smaller subsets of the perimeter. By creating micro-perimeters or micro-segmentation around certain classes and categories of data, that can improve data protection across hybrid environments.

And as with any security initiative, there is also a strong focus on the people. “Every year, [Forrester writes] a big report of biggest breaches we’ve seen over the year, and I can’t tell you how many breaches could have been stopped in their tracks or the damage significantly limited by things like two-factor authentication and stricter access controls,” Balaouras explains. “Make sure people don’t have excessive privileges to sensitive systems.”

“MAKE SURE PEOPLE DON’T HAVE EXCESSIVE PRIVILEGES TO SENSITIVE SYSTEMS.”

—STEPHANIE BALAOUAS

GETTING TO ZERO

There are different ways to achieve the Zero Trust architecture, explains Balaouras. One critical point is the security travels with the data itself. Regardless of its location—where it is stored, where it may be transmitted, and which resources may access that data—the security travels with the data.

“All your devices, your workloads, your apps, all your resources are accessed in a secure manner,” she says. “You limit and enforce access control. You inspect and log all traffic regardless of hosting model or location. There is no trusted network.

The data-centric approach remains the essential aspect of moving to Zero Trust. The key is understanding the data and moving the controls closer to the data itself. There are other capabilities you will need like visibility into the data and advanced data analytics to help predict threats. “Analytics can help you understand weaknesses in your environment and help you detect any breaches or intrusions in progress," says Balaouras. "We're not waiting for data to leave the building to be stolen on the dark web. We're going to take an automated response to anything we detect. We're going to orchestrate machine and human activity. And that is the [Zero Trust] framework."

The Zero Trust framework helps enterprises target and protect sensitive data and systems. They can use micro-segmentation to achieve stronger access control. They can achieve much better visibility into their data and what is happening with their data. They can more easily detect threats in progress. On the business side, they can also reduce capital and operating expenses, and limit the scope and cost of compliance initiatives. With the greater degree of insight into their corporate data, they can also more effectively ensure compliance with statutes like GDPR.

"The security team becomes more responsive and able to keep up with the digital transformation," she says. "We've seen pharmaceutical companies protecting their drug discovery processes and hospitals protecting their clinical systems. We've seen critical infrastructure, government agencies, airlines—industries that have low risk tolerance and high security requirements."

ZERO TRUST IN A DATA-CENTRIC WORLD

Applying the Zero Trust framework in a data-centric world requires a focus on data, devices, and the people and processes involved. "In trying to address the digital transformation and the Zero Trust framework, we looked at the pain points [companies] are facing," says Lenovo's Thorsten Stremlau. Lenovo has focused on four categories—or levers—that correspond to the Zero Trust framework. Those four levers, which Levono calls the DIODe model, are:

- Data
- Identity
- On-line
- Device

"We align the Zero Trust approach with solutions to address key levers in the data quadrant," he says. "If somebody leaves [a device] in a taxi or someplace they should not have, how do I prevent data leakage from that device?" In the event of device loss, theft, or even simply decommissioning, ensuring the data is completely erased from that device is a critical and often overlooked step.

"IN TRYING TO ADDRESS THE DIGITAL TRANSFORMATION AND THE ZERO TRUST FRAMEWORK, WE LOOKED AT THE PAIN POINTS [COMPANIES] ARE FACING."

—THORSTEN STREMLAU, LENOVO

Protecting the data both on the device and during transmission and preventing data leakage at any point in the data lifecycle is critical. “In a data-centric world, a company may ask, ‘How do I protect data at rest and on the device?’” says Stremlau. The solutions that fit into the data quadrant of the DIODe model include Secure Data Erase, WinMagic, and Bitlocker.

John Rajunas, desktop technology specialist at Microsoft, agrees, “How can we extend the idea of conditional access? How can we ensure the user only has access to trusted devices? With this idea of Zero Trust, we can’t assume that since the user is using a managed machine they can be trusted. We can use Windows protection features to protect individual data sets … and put conditions on where and when a user can access data.”

For the identity component of the DIODe model, the impetus is ensuring identity and access control, ensuring trusted devices, and reducing the use of passwords. Intel Authenticate, fingerprint readers, FIDO, and FIDO2 and other two-factor solutions come into play here.

Moving to on-line quadrant, the focus is preventing identity theft and ensuring safe surfing, eliminating malware and phishing, and preventing data leakage. Solutions that can help here include Lenovo Unified Workspace, Lenovo Wifi Security, and Windows Defender System Guard.

Focusing on the device, it’s critical to protect it and prevent it from being compromised, update the device securely, and be able to locate and disable the device in the event of loss or theft. Lenovo Patch, TPM 2.0, and Intel Transparent Supply Chain can help defend at the device level.

By embracing the Zero Trust framework, enterprises can protect themselves from advanced cyberthreats and better mitigate the impact of breaches. It can also help ensure simplified and more cost-effective regulatory compliance. The notion of trust and security has changed, and enterprises need to adapt their strategies and tactics to suit.

Find out more:
solutions.lenovo.com/