citrix™

Customer Story

Synopsys protects smart chip IP with Citrix security

"Today, no matter what a user is connecting to – whether it's an enterprise data center, cloud data center or a SaaS service, we want that connection to be secure and optimized," says Sriram Sitaraman, CIO at Synopsys. "That's crucial."

Joe Fu, IT director of engineering and applications, adds: "In serving the needs of remote workers, our most important issue has been to determine how the team will approach Citrix Secure Workspace Access and app protection policies," he says. "Citrix has been our primary access model for employees when they interact with applications hosted in our internal data centers, on public clouds or delivered as SaaS," Fu elaborates. "Especially critical during the coronavirus pandemic and the resulting work-from-home situation, we have implemented a very stringent process for data protection and data transfer. Citrix has been essential in that mission."

The Synopsys world before COVID-19

Synopsys security was quite different before the COVID-19 outbreak. There was a 'hard exterior shell' that protected the environment from external threats, and there was lateral trust across it. Business units were sharing code. All of the computing occurred in the data centers.

As Synopsys grew, its requirements expanded. For example, Synopsys had clusters of compute and storage that needed different types of protection. The IT team had to be vigilant about who could gain access and isolate the compute and storage relevant to special development that was taking place. That is when the team began to look at cloud computing and zero trust framework.

"We are now looking at multiple clouds that allow Synopsys employees, contractors, customers, partners and various combinations of those groups to be collaborating with each other," notes Sitaraman. "In all of these instances, we know that the only things we can trust are the things that we control. Citrix technology is critical because it provides single pane of glass visibility into the security of the entire environment."

SYNOPSYS®

Industry
Technology

Location
USA

Citrix products

- Citrix Workspace

Citrix solutions

- Citrix Analytics for Security
- Secure Workspace Access

Key benefits

- Citrix Secure Workspace Access enables the Synopsys team to securely manage data protection and data transfer, especially when it comes to remote workers
- Citrix Endpoint Management enables secure management of all devices from a single platform
- Citrix Secure Workspace Access helps Synopsys to consolidate access points and tighten its security posture
- The Citrix zero trust architecture helps prevent malware, data exfiltration, or VPN breaches and attacks

Security part one – zero trust

Sitaraman is quick to describe the first part of the Synopsys security strategy. He says: “Our position is that we can’t trust other networks. We want users to come into our data centers through encrypted channels. Citrix enables us to do this.” By unifying access to all its corporate applications, Citrix has not only helped tighten the security posture around these apps, but also helped improve overall employee experience.

In the Citrix world, the definition of zero trust can be reduced to one axiom: ‘Trust no one.’ No user or device should have default access to an organization’s network, workspace or other resources. Even if someone is employed by the organization, access is granted only after authorized users pass through security protocols. Those protocols are based on identity, multi-factor authentication and device posture.

“A Citrix zero trust architecture helps prevent malware, data exfiltration or VPN breaches and attacks. Citrix Secure Workspace Access, user identity verification and secure workspaces are the mechanisms that help alleviate these risks,” Sitaraman clarifies.

Sitaraman notes that the device type really doesn’t matter either. “Synopsys doesn’t control its contractors’ or customers’ devices. The company does, however, control the connectivity and the authentication,” he says. “With its zero trust security posture, Citrix has uniquely positioned Synopsys as an engineering company that really cares about both security and the employee experience we deliver.”

Connecting endpoints

Now that the Citrix infrastructure at Synopsys enables users to connect securely from home, customer locations, coffee shops, other corporate campus settings and more, users have secure access from literally anywhere. “Synposys manages more than 30 access points, including the VPN for intranet apps, direct access for SaaS apps and Citrix Gateway points for Citrix Virtual Apps and Desktops,” Sitaraman notes. “Secure Workspace Access helps consolidate all of these access points. That ultimately enables Synopsys to tighten its security posture, and yet, at the same time, continue to provide the high quality employee experience that is so important to success.”

In order to support remote workers, many different types of users had to be managed differently. Workers at Synopsys were using a host of devices – in some cases ‘bring your own’, or unmanaged devices – to access apps. Knowing the potential for security gaps, the team put app protection policies in place to mitigate risk.

> **“A Citrix zero trust architecture helps prevent malware, data exfiltration or VPN breaches and attacks. Citrix Secure Workspace Access, user identity verification and secure workspaces are the mechanisms that help alleviate these risks.”**
>
> **Sriram Sitaraman**
> **CIO**
> **Synopsys**

Multifactor authentication and what happens inside the environment

"We strongly believe in the importance of contextual policies and multifactor authentication (MFA)," says Sitaraman. "An inordinate number of global data breaches have been found to be related to weak passwords."

Citrix experts believe that the strength of an organization's security posture is determined by its weakest link – most often users' passwords. One of the most common remedies proposed by Citrix security subject matter experts is to mandate MFA for external entry points. Because an attacker must know a secondary authentication factor in addition to a password, MFA protects against password spraying.

"Once the user has successfully gained access to our environment, we also want our IT team to be able to impose prudent controls – blocking copy-paste capabilities, prohibiting file downloads or file uploads, and more," he continues. "However, there's a balance we must achieve. We never want to negatively impact the user experience."

Security part two – the enterprise data center, the cloud and SaaS

The second piece of the Synopsys security strategy is already mature. A set of Synopsys services is in its enterprise data centers. A different set of services are hosted in the cloud through SaaS providers. Users are distributed across multiple locations to ensure better service. "The idea is that no matter where you are across the globe, or how you are connecting back into the enterprise data center, we want users to have a secure optimized experience connecting to apps and data," says Fu. And the company's IT department ensures good connections for all of these users and capabilities in a secure and optimized manner.

Getting security right

For one of its largest customers, the Synopsys team tested and implemented a host of user-controlled solutions. This was risky, however, simply because users were the ones who actually had to put the security measures into action. It was for this reason that the organization implemented Citrix in its U.S. security design center. Now, thanks to the implementation of Citrix, security measures are in the hands of IT. In this particular instance, the customer agreed that the choice of Citrix worked well to meet security and zero trust needs.

Because of the success in the customer scenario, the company will replicate the process for several of its own locations, as well as for several other customer environments. The team also plans to use Citrix to manage security for contractors and vendors who have been authorized to work in the engineering environment.

How Synopsys enables the security model

The team is pleased with the fact that it has the ability to control how sensitive data is accessed and what actions users can take while accessing this data. "We may expand scope by segregating our internal business units so we can create the right security boundaries relevant to product lines and data. This way, we can ensure that we provide targeted service to different user groups," explains Fu. "For that, Citrix is an excellent tool to help us provide user access segregation and to deliver the customized services," says Sitaraman.

"In the future, when we are able to leverage Citrix services in Microsoft Azure, the Azure backbone will ensure that the shortest, optimum route is used for information access."

Synopsys – a continuing journey

"Over the years, Citrix has helped Synopsys consolidate data centers. We continue to grow those data centers – as well as to optimize the solutions in them. Now engineers access their apps and data through Citrix," says Sitaraman. "Of course, we will add other solutions, but Citrix will continue to be essential because it enables anyone who is authorized to connect securely from anywhere. We will keep expanding our environment with a solution that will translate well as we grow into various clouds and add Citrix Workspace technology."

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States