CASE STUDY_

DigitalOcean Simplifies New Acquisitions with Supply Chain Security

DigitalOcean

CHALLENGES_

- DigitalOcean needed to verify the integrity and establish trust in the infrastructure supply chain of a newly-acquired international company.
- The company relied on a highly varied fleet of roughly 350 Windows, macOS, and Linux-based devices acquired from sources outside of DigitalOcean's approved supply chain partners.
- Replacing devices would be prohibitively costly and slow due to the cost of new hardware, import tariffs, regulations, and other logistics challenges.

RESULTS_

- Using Eclypsium, the DigitalOcean team inventoried and verified that all hardware, components, and low-level code were authentic and free from threats and vulnerabilities.
- By validating the supply chain of existing devices instead of replacing them, the DigitalOcean team was able to substantially reduce hardware costs and completed the end-user technology integration earlier than originally projected.
- Additionally, DigitalOcean was able to avoid the immediate costs associated with establishing new supplier relationships.
- Following the success of the program, DigitalOcean integrated Eclypsium for supply chain security when acquiring new companies.

With 15 data centers worldwide, DigitalOcean is a leading provider of cloud services for startups and small and medium-sized businesses (SMBs). The company provides these growing organizations with everything they need to quickly, reliably, and securely build and deploy their products and services in the cloud.

DigitalOcean has acquired innovative companies that built out the company's portfolio of services. However, acquisitions can present some serious IT challenges. One of the first and most fundamental issues is establishing trust in the infrastructure supply chain used by the newly acquired organization.

CHALLENGES OF SUPPLY CHAIN SECURITY FOR NEW ACQUISITIONS

"The most important thing for us is to make sure that all the technology that we bring in from an AcquiredCo is safe for us. For DO, we don't just think of 'us' as our business. We focus on the safety of our customers, our business, and the entire Internet. When integrating an acquired company, we have to know that each device can be trusted before we can even begin to deploy our images and code on new end-points."

Tim Lisko
Senior Director of Security Engineering, DigitalOcean

The DigitalOcean team recently faced this challenge after acquiring an innovative startup with a number of employees in a location they hadn't previously had operations (AcquiredCo). And like many startups, the AcquiredCo's focus was on developing new innovative services and not necessarily on internal IT. The company had a fleet of over 500 end-user computers (e.g. laptops). The DigitalOcean team needed to quickly decide whether to bring the existing hardware under the DigitalOcean umbrella or to replace it with new hardware.

Both options had challenges. The AcquiredCo had a highly varied fleet of Windows, macOS, and Linux-based devices, and DigitalOcean had no insight into the provenance of the devices or the supply chains that produced them. Additionally, the firm had leveraged outside service providers for support so there were many opportunities for the devices to be altered. DigitalOcean didn't have an easy way to assess the devices for risks such as hardware or firmware implants, integrity changes, vulnerabilities, or misconfigurations. On the other hand, replacing the devices would be costly and time-consuming. **In addition to the cost of new hardware, international import tariffs would add a substantial economic burden and finding trusted supply chains would introduce significant time delays**.

THE ECLYPSIUM SOLUTION

"Naturally, we have our own approved image for our operating systems and software. But it didn't make sense to install good software before we knew that we could trust the devices themselves. Eclypsium made this easy. We were able to gain a level of trust in the devices that enabled us to make a more informed risk-based decision, allowing us to move forward with reimaging. For any devices that alerted, we were able to pull them out of rotation and set aside for a deeper investigation."

Heather Cannon
Senior Manager of Security Engineering, DigitalOcean

Needing to find a way to bring the new company online quickly and cost-effectively, Tim Lisko, the Senior Director of Security Engineering at DigitalOcean, began looking for a solution. He came across the answer when talking to a member of the DigitalOcean SOC team. The SOC team was interested in hardware roots of trust and had been experimenting with Eclypsium as a way to audit and verify the integrity of assets delivered from the supply chain. Tim quickly realized that this technology could be used to assess the hardware in the newly-acquired startup.

"The roots of trust in your IT infrastructure are extremely important, yet are extremely difficult to inspect and not well understood. Eclypsium's supply chain security solution solves these critical problems simply," says Lisko.

Working with the team at the AcquiredCo, DigitalOcean deployed the Eclypsium agent to the various Windows, Mac, and Linux endpoints. According to Heather Cannon, Senior Manager of Security Engineering at DigitalOcean, "Even just doing the basics with Eclypsium was really powerful. We were quickly able to establish which assets we were onboarding and exactly what was inside them down to all the components and firmware."

Next, the team needed to understand the risk profile of their devices. With a simple, automated scan, Eclypsium was able to provide a detailed security audit of each asset, ensuring that every device and component was authentic and only running valid, vendor-approved code, was free of threats like backdoors and bootkits, while also surfacing any vulnerabilities or configuration problems that could put the integrity of the hardware or boot process at risk. When the scans were complete, the DigitalOcean team knew exactly which devices were clean and exactly what issues needed to be addressed.

Collectively, these capabilities allowed DigitalOcean to leverage the hardware of the new company without the need to import new replacement devices. This led to significant savings in both time and money by avoiding new hardware costs, tariffs, and slow import processes. All told, DigitalOcean was able to save almost $1M in hardware costs by using Eclypsium to establish trust in the AcquiredCo devices.

When it comes to solving hard problems, the people are often just as important as the technology, and this was the case in the working relationship between DigitalOcean and Eclypsium. The Eclypsium team was able to help get the solution installed and operational quickly while also sharing the team's experience and expertise in infrastructure supply chain security. This ensured that DigitalOcean was able to not only successfully deploy a new security solution, but also to get the most out of a truly new type of security solution. Beyond simply acting as a security vendor, the Eclypsium team was able to act as a partner to ensure that the DigitalOcean team was able to meet their immediate goals while also being ready for future acquisitions.

A PARTNERSHIP IN SUPPLY CHAIN SECURITY

"The working relationship with Eclypsium has been outstanding. We were able to get up and running quickly, and the Eclypsium team was super responsive whenever we needed help along the way. Between the working relationship and the cost savings, Eclypsium's supply chain security solution is a no-brainer addition to our playbook when onboarding new companies."

Tim Lisko
Senior Director of Security Engineering, DigitalOcean