Success Story:

ControlScan Helps Terra Dotta Achieve Trusted-Provider Status

Terra Dotta, LLC creates software solutions that enable universities and higher-education institutions around the globe to effectively and securely manage student enrollment data while streamlining the business operations that collect that information. More than 450 educational institutions trust the company's solutions, which are primarily based on the Software-as-a-Service (SaaS) delivery model.

The progression of data and technology to the cloud has driven many CIOs and CISOs to approach software providers like Terra Dotta with a great deal of scrutiny. In fact, only recently have universities become willing to allow data to traverse the boundaries of their own IT infrastructure. Privacy and security continue to be of utmost concern.

Recognizing the opportunity to become known as a trusted provider of secure SaaS solutions for higher education, Terra Dotta invested heavily in its infrastructure. A significant portion of this investment included evaluating and solidifying its own security and compliance, as well as the security and compliance of its vendors and suppliers. ControlScan worked with Terra Dotta throughout this effort, helping them achieve a level of security and compliance that their customers can rely on.

The Challenge: "Proving Out" Privacy and Security

In recent years, educational institutions' RFPs have become increasingly detailed in their question sets. That's because today's CIO/CISO needs a lot of convincing when it comes to a prospective service provider's ability to protect their organization and its data.

"As a provider of SaaS solutions in the higher education space, we hear a lot of concern around the privacy and security of personal information," said Garrett Christian, chief technology officer and co-founder, Terra Dotta. "Educational institutions are building up their compliance framework and want to ensure that the service providers they're using are reputable businesses with good continuity plans and security practices."

Terra Dotta's hosting infrastructure is a multi-tenant, highly available, highly scaled system that also integrates with external services such as on-campus and third-party applications. Among these services is a component for processing online payments. Terra Dotta had taken a "very measured, careful approach" to the design of this component by redirecting users to external payment gateways, which reduced the scope of the environment subject to Payment Card Industry (PCI) requirements.

When version 3.0 of the PCI Data Security Standard (DSS) became effective in 2015, however, applications using e-commerce redirects were brought into scope for PCI compliance and Terra Dotta's PCI-related obligations grew. At the same time, universities and other higher-ed institutions were also being made aware of their own compliance responsibilities under PCI DSS v3.0.

"Our scope of PCI compliance had suddenly increased, plus our customers began calling and saying we needed to reassure them of our compliance in order for them to demonstrate their own compliance," said Christian. "Terra Dotta has always had security as a central focus, but the need for standards compliance would bring us to a new level."

The Solution: Certification as a PCI Level 1 Service Provider

Terra Dotta made the decision to go above and beyond their PCI obligations by pursuing certification as a PCI Level 1 Service Provider. The process would entail independent validation by a PCI Qualified Security Assessor (QSA), whereby Terra Dotta's payment card data environment would be audited using a standard methodology and reporting format, resulting in a comprehensive Report on Compliance (RoC).

In its search for PCI QSA assistance, Terra Dotta reached out to several U.S.-based service providers. ControlScan became the obvious choice, due to its comprehensive in-house security and compliance expertise as well as its pricing transparency.

"I was pleased by the conversations I had with ControlScan and also the way their quote for services was assembled," said Christian. "The ControlScan quote had a lot more detail to it, whereas many of the other quotes we received were in a lump sum that was difficult to pick apart and understand. I appreciated the granularity in ControlScan's quote because it demonstrated the value received for the associated cost."

> *"Terra Dotta has always had security as a central focus, but the need for standards compliance would bring us to a new level."*
>
> *– Garrett Christian, CTO & Co-Founder, Terra Dotta*

Implementation: Establishing a Framework of Security Best Practices

A ControlScan QSA went to Chapel Hill to work with Terra Dotta on a PCI gap analysis, which provides a holistic view of the organization's current compliance state and the steps it's taking to achieve compliance with the PCI DSS. A project calendar was established, showing the milestones to be met and key deliverable dates.

"One of the very first things [the QSA] told us was that we were going to make our lives so much better if we could just eliminate all of the various entry points to our sensitive data environment," said Christian. "So all of our mobile environments, all of our work stations—anything that could access our production environment where sensitive data is housed—we needed to get them out of the picture."

Terra Dotta responded by reconfiguring its network to restrict access to its sensitive data and thereby reduce its scope of compliance. The overall environment was thoroughly hardened to reduce the risk of unauthorized or malicious access.

“This was not a small thing to accomplish; but by doing the up-front work we eliminated what would have been a monumental effort, which would be to audit and harden every single system that could possibly access our sensitive data environment” said Christian. “A bigger challenge that went along with that, though, was making the necessary changes to our firewall.”

Hosted by a third-party data center, Terra Dotta’s firewall was not configured in a PCI compliant manner or even according to their specific business needs. “We had to establish the conditioned environment we needed to allow for the single-point-of-entry design as well as other specific requirements of the PCI DSS,” said Christian.

> “We couldn’t ask for a better ally in our process of becoming PCI compliant.”

Terra Dotta also was surprised to learn that their organization’s compliance depended upon the compliance of their hosting provider. Through its communications with the hosting data center, Terra Dotta encountered some challenges in assessing the hosting center's PCI DSS compliance.

"Our ControlScan QSA helped get us through these issues as well," said Christian. "We were ultimately able to establish the documentation to show where the hosting provider’s services were in order for us, proving we could rely on their compliance as part of our own security and compliance."

Sticking to the project timeline was difficult, given the many surprises that arose throughout the assessment process. However, ControlScan’s QSA was able to apply enough flexibility to keep Terra Dotta on schedule. In the end, ControlScan completed its assessment a day ahead of the project deadline.

"We couldn't have asked for a better ally in our process of becoming PCI compliant,” said Christian. “Our ControlScan QSA was both an advocate for the data security standard and for our ability to keep doing business while doing what we have to do to be compliant."

The Result: Peace of Mind for Terra Dotta and Their Clients

ControlScan worked side-by-side with Terra Dotta to simplify their environment in a way that will create value for years to come. By taking a consultative approach, ControlScan helped Terra Dotta fully review its processes and technologies to reduce the organization’s scope of compliance and at the same time, ensure best-practices security.

As a result of their engagement with ControlScan, Terra Dotta is confident that their own applications—as well as those used by their service providers—are safe and secure for payment acceptance. In turn, Terra Dotta’s Report on Compliance assures educational clients that their employees' and students’ sensitive data are optimally protected.

Whereas in the past, Terra Dotta would sometimes need to update its security processes “reactively” in order to meet prospective clients’ requirements, the company can now select “yes” down the line when completing security questionnaires for new business. This has led to an increase in the number of closed sales.

“Overall, we’re moving through the sales process much more rapidly,” said Christian. “We’re getting a much better uptake following initial sales inquiries. When we tell IT officers we have PCI DSS certification, there’s a big sigh of relief on the other side, because it’s going to make their job so much easier.”

With a solid framework of security best practices in place, Christian expects that future audits and compliance checks will go much more quickly and smoothly. The streamlined PCI compliance process is also likely to save on related costs down the road.

“It’s very satisfying to know that we have best practices in place to support and secure our sensitive data environments. Going through this process with ControlScan has helped Terra Dotta realize the benefits of proactive security compliance.”

About ControlScan

Headquartered in Atlanta, ControlScan delivers unified security and compliance solutions that help small and mid-sized businesses secure sensitive data and comply with information security and privacy standards. We support business owners, franchisees and merchant service providers with technology, services and expertise for PCI DSS, HIPAA and EI3PA compliance; vulnerability detection and risk mitigation; POS, e-commerce and mobile security; and more. For more information, please visit ControlScan.com or call 1-800-825-3301.