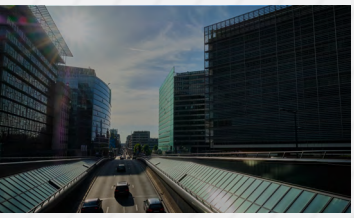
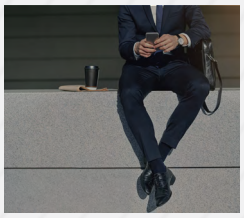
voices

CrowdStrike Customer Case Study





StepStone

CrowdStrike Helps Leading Digital Recruitment Business Protect Personal Content for Thousands of Jobseekers Worldwide

One evening at 11 p.m., Serge Groven, senior corporate IT manager at StepStone, received an urgent communication from the CrowdStrike OverWatch team alerting him to a possible threat. The company had overlooked mentioning to CrowdStrike that a routine penetration test was being conducted. "It was great to know that the CrowdStrike OverWatch service was working so effectively," Groven said. "Not only was I alerted about the incident, but I was also told that it was a test. This shows how CrowdStrike marries automation with human intelligence to deliver effective, real-time threat prevention."

Founded in 1996, StepStone is one of the world's leading digital recruitment platforms and is ideally positioned to create value in an environment with dramatically increasing talent scarcity. By combining AI-powered hiring platforms and digital recruitment services, StepStone pushes the boundaries of technology to help companies hire the right talent and help people find the right job. StepStone is active in more than 20 countries with more than 20 brands (StepStone, Totaljobs, Appcast, and others) and employs around 3,700 people. The company has its headquarters in Düsseldorf, Germany.

Endpoints Are Typical Ingress Points

StepStone is a rapidly expanding business with a growing presence in the U.S. and plans to enter new markets such as blue-collar industries. As a high-profile online business faced with increasingly sophisticated and numerous cyberattacks, security is more important than ever before.

"Security is of paramount importance to StepStone because our candidates trust us to protect their data, especially highly personal resume information," Groven said. "Among several security measures, we are heavily focused on protecting endpoints because these are typically the ingress paths."

The company has built a leading digital recruitment platform that delivers more than 100 million job applications per year to over 150,000 employers. In a typical month StepStone averages three million page views and one million site visits.

With the threat level increasing and becoming more sophisticated with phishing and malware attacks, the company realized that its existing antivirus products were no longer sufficient. To rectify the situation, StepStone carried out an extensive review of solutions and created a shortlist of three that included CrowdStrike.

INDUSTRY

Recruitment

LOCATION/HQ

Düsseldorf, Germany

CHALLENGES

- Ensuring that highly sensitive personal information is secure
- Increasing vulnerability when protecting digital-only, global business operations
- Greater risk of cyberattack due to high volume of global online traffic
- Existing antivirus and endpoint security tools no longer provided sufficient protection

SOLUTION

StepStone, one of the world's leading digital recruitment platforms, uses CrowdStrike to ensure highly sensitive candidate personally identifiable information and employer data are protected from increasingly sophisticated security threats

"CrowdStrike is a true next-generation endpoint protection solution."

Serge Groven
Senior Corporate IT Manager
StepStone

voices

CrowdStrike Customer Case Study

Each of the finalists was effective, but a couple had key drawbacks including a dependence on allowlisting (a pre-approved list of entities), needing too much micromanaging, and having multiple dashboards. StepStone chose CrowdStrike for offering the most comprehensive and easy-to-use solution set. Specifically, CrowdStrike has a single, unified dashboard, offers next-generation antivirus protection and is cloud-based, which proved to be a particularly important asset during the pandemic lockdown.

Straightforward Global Implementation

StepStone deployed the suite of CrowdStrike solutions to 3,600 client and server endpoints across the business.

"Deploying CrowdStrike was a very smooth process without any issues. It took just six weeks in total. The deployment was very quick and easy, in part because the client-side installation has such a light footprint, does not require a full endpoint scan and can be installed almost without users noticing."

In addition, because of the excellent CrowdStrike pre-sales support, StepStone was able to identify potential implementation hurdles and mitigate them. For instance, CrowdStrike enabled a smooth uninstall of the legacy client including the removal of several software bugs that StepStone had been unable to identify.

"CrowdStrike is a true next-generation endpoint protection solution," Groven said. "In simple terms, other solutions and antivirus products work by identifying the 'mugshot' of a known threat rather than tracking suspicious activity. As CrowdStrike is heuristic, it looks at behavior as well as at the mugshot."

StepStone tested this during its solution selection process by taking a known malicious file and adding a minor variant. Standard security products identified the file, but not the variant. CrowdStrike was able to detect the change and block the file. "The heuristic capability in CrowdStrike is critical because with today's fast-moving and changing threat levels, attacks are identified much easier and quicker," Groven explained. "CrowdStrike also looks at behaviors like lateral movement and processes to further strengthen our defenses."

StepStone is shifting its IT infrastructure almost entirely to the cloud, primarily on AWS for its job site applications, while corporate systems are on Azure. The IT environment comprises both Microsoft and Apple platforms. CrowdStrike support for both on-premises and virtual domains is key because 15% of staff use Apple devices, and Apple OS updates can often have ramifications on other applications. Every time there is a Mac OS update, it is automatically supported by CrowdStrike. This gives StepStone more scope to attract some of the most highly skilled candidates who often say they only want to work with Apple equipment.

StepStone has leveraged the ability of CrowdStrike to easily integrate with other security tools and related functions to deploy Falcon Firewall Management™ and Falcon Device Control™ to manage USB devices.

The next phase will see StepStone deploying CrowdStrike Falcon Spotlight™ to streamline vulnerability management across their enterprise. "I am excited to see what else is possible with

RESULTS

Overhead dropped to under 1% of endpoint processing power

Delivered an easy, seamless deployment to 3,600 endpoints in six weeks

Combined automated and human intelligence to deliver robust threat mitigation

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Device Control™ endpoint device control
- Falcon Firewall Management™ centralized firewall management
- Falcon Insight™ endpoint detection and response
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus

voices

CrowdStrike Customer Case Study

CrowdStrike because it has so much information and delivers incredible visibility into what is going on," Groven said. "I'm excited to see what intelligent, cost-effective solutions CrowdStrike will come up with in the future, and how they will make my life easier."

CrowdStrike Is an Invisible Enabler

StepStone views CrowdStrike as a key part of its security and threat mitigation strategy, especially for managing, monitoring and controlling endpoints.

"If you ask what CrowdStrike does, it enables me to sleep easier at night because I do not need to worry so much about security," Groven said.

"For the business, CrowdStrike has delivered comprehensive protection: This has been especially important during COVID-19 and means that we are confident that our clients are more secure."

One of the key benefits of the CrowdStrike Falcon platform is its light footprint on the business while enabling operational continuity. StepStone attributes this to two reasons. The first is low impact on device performance (e.g., demand on CPU performance is usually less than 1%). An additional key feature for the security team is the unified dashboard that is easy to read and provides a wealth of information and real-time vulnerability analysis.

Besides the solutions, StepStone's partnership with CrowdStrike has been another important benefit. "What really helps us is the monthly review with CrowdStrike," Groven said. "We have a CrowdStrike engineer assigned to us who reviews each status, flags if there is a new feature and explains whether it will be of benefit in our environment. This reduces the maintenance burden and means we spend much less time on security management."

Associated with the partnership is access to the CrowdStrike ecosystem, including third-party software integrations available in the CrowdStrike Store.

Groven noted two additional benefits StepStone has realized since deploying CrowdStrike: the team has not had to rebuild any clients because the Falcon platform has blocked attacks, and its skilled engineers, who now spend less time on mundane security maintenance tasks, can spend more time developing and improving business and customer-facing systems and services.

"The importance of CrowdStrike to StepStone and the services it provides to candidates and employers is measured by the fact our senior executives do not think about CrowdStrike, because it quietly protects behind the scenes," Groven said. "Of course, security is critical but CrowdStrike is an invisible enabler. It is about having the confidence that you have the right solution. While nothing is perfect, we can honestly say we have made a great choice in CrowdStrike."

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**