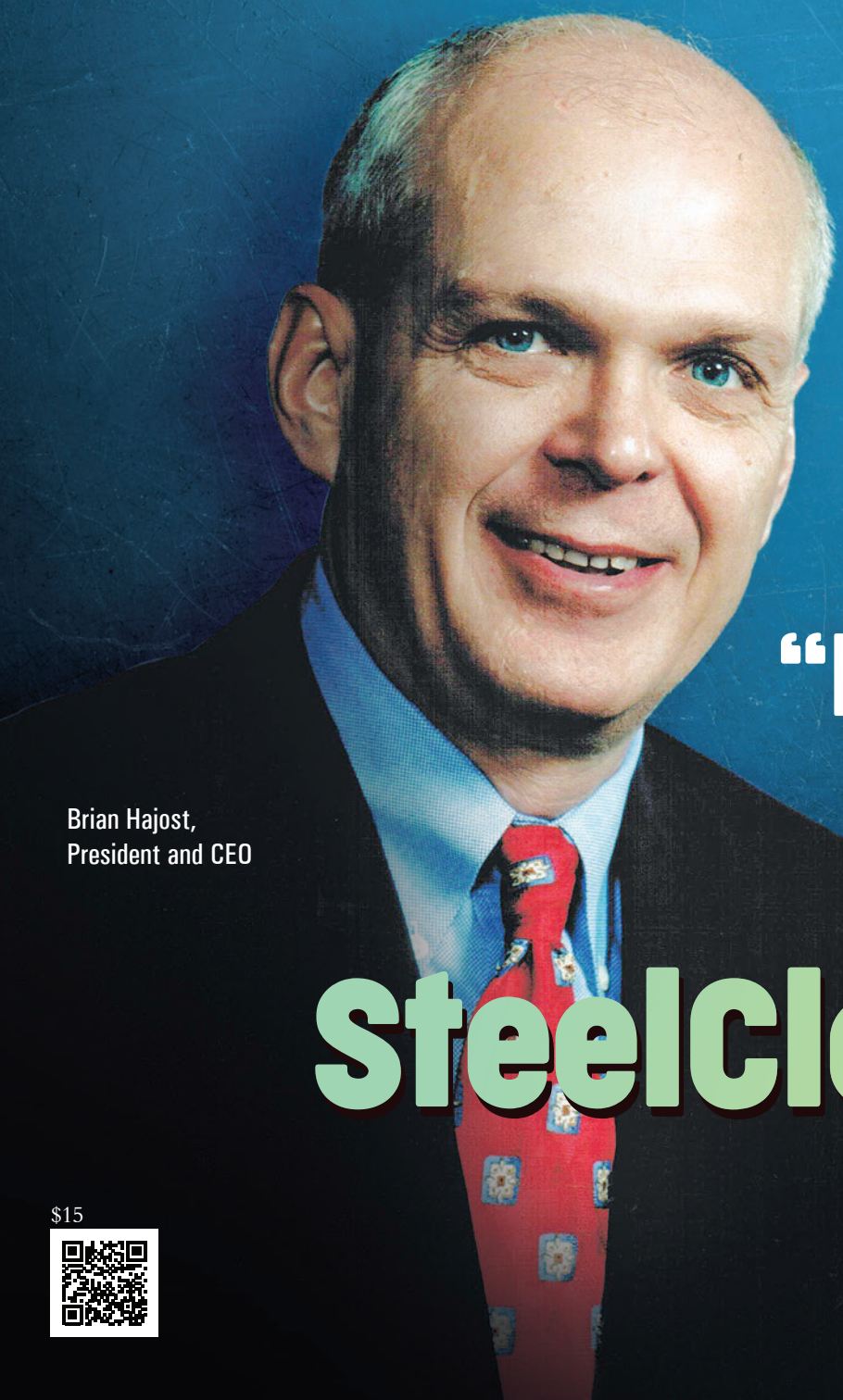
ENTERPRISE SECURITY

WWW.ENTERPRISESECURITYMAG.COM ISSN 2691-4034 SEPTEMBER - 21 - 2020



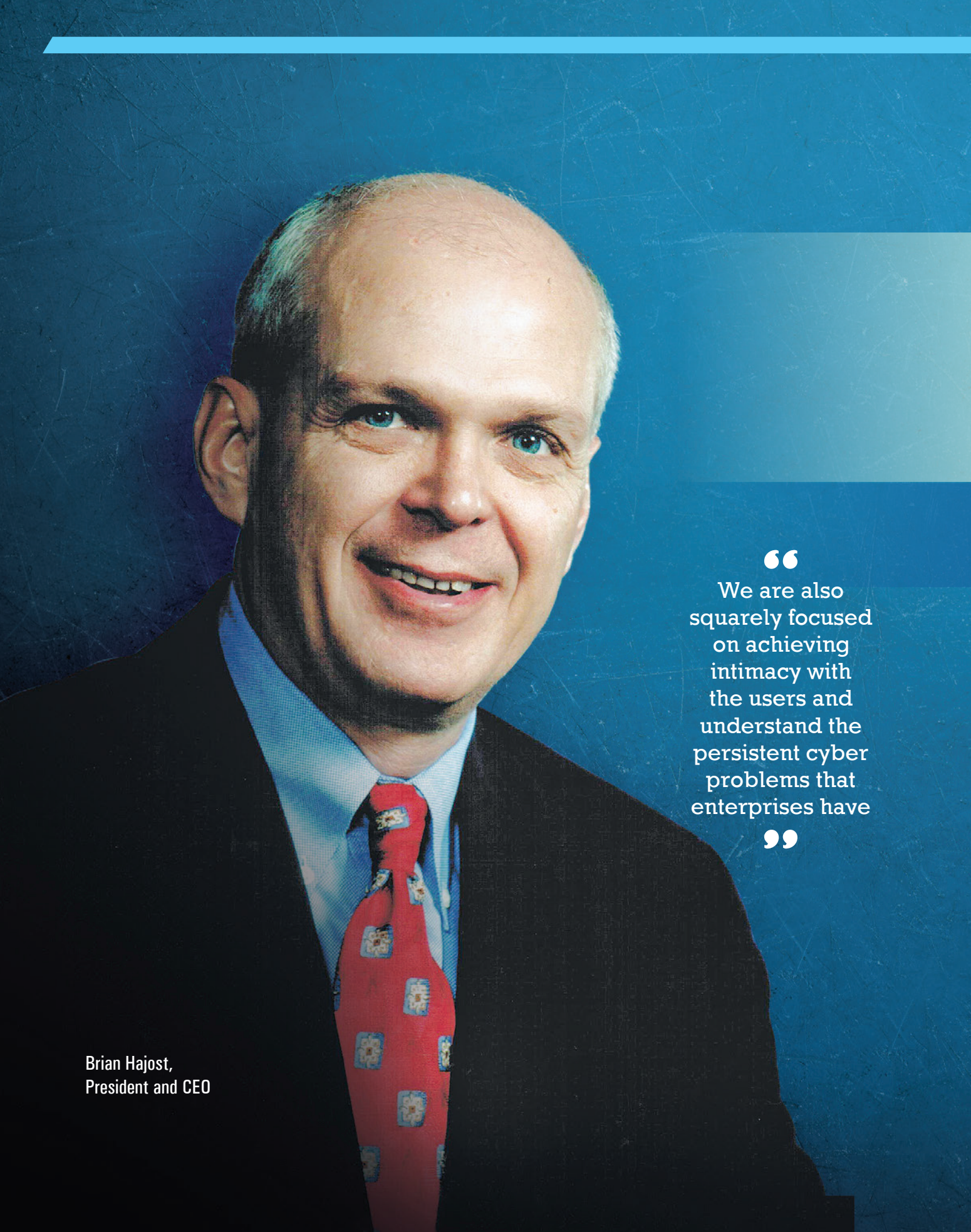
ENDPOINT SECURITY EDITION

"Hardening" Security

Brian Hajost,
President and CEO

SteelCloud LLC

$15



Brian Hajost,
President and CEO

ENTERPRISE SECURITY
TOP 10
ENDPOINT SECURITY
SOLUTION PROVIDERS - 2020

SteelCloud LLC

"Hardening" Security

When American author Robert Jordan wrote, "The oak fought the wind and was broken, the willow bent when it must and survived" he could have been penning an epigram about the importance of cultivating resilience in enterprises. Modern business environments are now a labyrinth of highly complex and ever-changing, interconnected systems, devices, infrastructures, and applications, and the security factors underpinning such environments are equally complicated. The endpoint upsurge in businesses—both inside and outside of the traditional perimeter—coupled with the threats turning craftier and more insidious demands endpoint security in enterprises to broaden its focus to keep up with the changes. According to Brian Hajost—a highly experienced leader in cybersecurity and information assurance—building a resilient foundation in enterprises is essentially the first step to mitigating endpoint exploits.

While government networks today are primarily built using commercial operating systems (Windows/Linux), database management systems, web servers, and other network devices, the organizations must comply to the hardening in the operating environment as defined in the STIG/CIS policies and should be configured in the most secure manner possible. "When organizations move from Windows Server 2012 to 2019 or from one Windows 10 version to another Windows 10, each of these versions need to be configured appropriately so that they are properly secured. Enterprises often struggle with the components in their application stack (which includes the operating system (Windows, Linux) the application is built upon as well as web browsers, databases, and other components required for the application to function) that can either provide additional security or compromise security if not configured to a policy baseline," explains Hajost, who has spent more than three decades specializing in government and federal integration, financial and the securities, and mobility markets. "Only in rare instances can applications run in generic hardened environments. Capabilities of an operating system, for instance, might be appropriate for a bookstore, but it may not be appropriate for a Fortune 100 company, wherein those capabilities are either removed or are hardened." In a nutshell, organizations have to put in a lot of effort and

time to build, test and deploy STIG-compliant environments, and the initial hardening effort can take weeks or even months. This industry narrative is precisely what SteelCloud intends to change.

Enter SteelCloud

To accelerate the accreditation of new applications and to automate the security sustainment of deployed infrastructure, Hajost and his team at SteelCloud develop technology for automated remediation of endpoints to the DISA STIGs and/or the CIS Security Benchmarks. With Hajost at the helm as the president and CEO, SteelCloud empowers large commercial enterprises, DoD/government customers, and systems integrators/consultants, with automated policy remediation solutions. "Organizations cannot foresee what they are going to get hit with tomorrow. A resilient system allows them to address problems that they are not even aware. This is where we draw years of experience in endpoint security to both recommend and work on helping organizations build a resilient foundation that can be layered with technologies as their business and security requirements dictate," adds Hajost.

To help organizations build this security foundation, SteelCloud ensures that the components of an application stack that strengthen cybersecurity are retained while the rest are eliminated. Next, the company takes charge of hardening and configuring the retained components properly, starting with the operating system. While federal IT security teams in DoD must comply with the technical testing and hardening frameworks, STIG, SteelCloud' software automates the hardening processes depending on the operating system being utilized by the client. In doing so, the company leverages industry-proven hardening techniques and capabilities, and advanced audit and security policies to reduce them to automation. This allows an organization to implement those advanced techniques and policies in their infrastructure as quickly as possible and also maintain them with minimal energy and expenses. "Security challenges are dynamic; thus, organizations need to harden their environments to respond to those challenges and requirements quickly and effectively. This is what SteelCloud software provides," says Hajost.

Automated STIG "Hardening"

For managing secure baselines and implementing/maintaining STIG-compliant environments, SteelCloud has developed ConfigOS—a patented STIG/CIS policy remediation software tool—that not only fixes/remediates STIG controls but also hardens them around an application environment in less than 60 minutes. ConfigOS can scan 10,000 to 15,000 Windows or Linux endpoints per hour and can remediation 3,000 to 5,000 endpoints per hour—per instance of ConfigOS. The tool also assists organizations with automated and comprehensive compliance reporting and XCCDF output. Putting theory into practice provides several successful examples of SteelCloud's solutions in action. A medical product vendor catering to both government and commercial sectors approached SteelCloud for mitigating security challenges and ensuring that its products operate in these highly secured environments. Backed by SteelCloud expertise and automated STIG and CIS remediation for policy compliance, the vendor has been able to operate in these secure networks successfully. In yet another impressive feat, SteelCloud assisted a Fortune 50 company that operates worldwide to automate compliance.

Besides these impressive client success stories, the uniqueness of SteelCloud also stems from the seven patents it has been awarded for its innovative solutions. For a company to stay innovative and inventive on a global scale, year after year, it stands to reason that SteelCloud's unique solutions and approach to security compliance is hard to duplicate. "Besides, we are also squarely focused on achieving intimacy with the users and understand the persistent cyber problems that enterprises have. We get to the root level of a problem, apply quality management principles to cyber, and finally attack the root problem as opposed to fixing the immediate issue. SteelCloud specializes in filling the technology gaps in an organization and keeps it secure and compliant with as little effort as possible," informs Hajost.

At a time when the COVID-19 pandemic has ushered the world into uncharted waters and organizations are struggling to maintain their configurations and security posture while having fewer resources, SteelCloud is fostering the concept of explicit compliance and security, providing clients both their capacity and their agility back to maintain their environments wherever their staff—on-site or remote. Moving ahead, with four new patents underway, SteelCloud will continue with its "magic" and solve the problems that customers didn't believe could be solved in the first place. ES

ENTERPRISE
SECURITY

WWW.ENTERPRISESECURITYMAG.COM ISSN 2691-4034 SEPTEMBER - 21 - 2020

SteelCloud LLC

TOP
ENDPOINT
SECURITY
SOLUTION PROVIDERS
2020

Recognized by
ENTERPRISE SECURITY

SteelCloud LLC

TOP
ENDPOINT
SECURITY
SOLUTION PROVIDERS
2020

Recognized by
ENTERPRISE SECURITY

The annual listing of 10 companies that are at the forefront of providing Endpoint Security solutions and impacting the marketplace