Sandvik Embraces Zero Trust and Empowers 35,000 Users to Work-From-Anywhere with Zscaler Private Access

Sandvik Group is a global high-tech and engineering company with a strong commitment to enhancing customer productivity, profitability and sustainability. Founded in 1862, Sandvik holds approximately 6,000 active patents in industrial tools and tooling, mining and construction equipment, and advanced stainless steel and special alloys. The company is a world leader in Manufacturing and Machining, Mining and Rock, Rock Processing, and Materials Technology.

VPN falls short for security and user productivity

Even before the COVID-19 pandemic changed everything, the traditional virtual private network (VPN) approach to connecting and securing remote workers for the Sandvik Group was becoming a significant challenge.

"At any given time we have almost 20,000 users accessing our applications, which includes our employees plus contractors, consultants, and vendors," explained Michael Alvmarken, Service Manager for Cybersecurity and Technology, at Stockholm-headquartered Sandvik Group. "Prior to the pandemic, VPN technology was increasingly insufficient for supplying secure connections that encouraged productivity. When the pandemic required sending most of our workforce remote almost overnight, we needed to modernize immediately."

Embracing zero trust with Zscaler

Although Sandvik had relied on VPNs for decades, the technology increasingly caused productivity and user experience hurdles. "VPNs are a network-centric technology that hasn't evolved much since it was introduced," said Alvmarken. "Putting up access barriers causes users to consider shortcuts. We wanted to adopt a technology that removed connectivity hurdles and reduced attack surfaces to improve our security posture."

CHALLENGE

- Establish zero-trust network access rapidly and smoothly to enable WFA transformation.

SOLUTION

- Zscaler Private Access™ (ZPA™)
- Zscaler Internet Access™ (ZIA™)
- Zscaler Zero Trust Exchange™ platform

OUTCOMES

- Transition 20,000 global employees to zero-trust WFA network access in less than five days
- Minimize attack surfaces and access barriers by reducing VPNs
- Significantly improve user experiences
- Reduce time spent configuring security connectors from over an hour to seconds
- Effectively segment network access using policy-based tools to speed performance
- Uncover and protect applications previously unknown to corporate IT
Having previously partnered with Zscaler to start implementing a zero trust strategy, Sandvik sought to expand upon its recently deployed cybersecurity innovations. This led the engineering firm to conduct a proof of value (POV) with cloud-driven Zscaler Private Access (ZPA).

Then the pandemic hit. “Fortunately, when management informed us that we needed to prepare for the COVID-19 work-from-anywhere [WFA] transformation, we already knew Zscaler Private Access provided us with a smart, safe and scalable solution for addressing our various VPN concerns,” said Alvmarken.

Alvmarken’s team quickly tested ZPA over a weekend with 30 users. “Everything went completely smoothly,” he said. “We extended our partnership with Zscaler to add ZPA and launched globally five days after that, meeting our corporate deadline for enabling all of our employees to work safely during the pandemic.”

Zero attack surfaces in a holistic WFA security environment

Using ZPA, Sandvik can provide seamless, secure, VPN-free access for private applications running on public clouds and within its data center. By adding ZPA to its existing deployment of Zscaler Internet Access (ZIA), Sandvik established a holistic WFA zero trust security environment called the Zscaler Zero Trust Exchange platform. That’s because ZIA enables remote workers to access SaaS applications and the Internet, complimenting private-access ZPA.

“In addition to creating attack surfaces, VPNs are also notorious for permitting bad actors to get inside undetected,” said Alvmarken. “Once in, threats move around at will—with many companies learning the hard way that it can take a long time before they’re found.”

What’s more, deploying ZPA ensures neither networks nor applications are ever exposed to the internet. This makes all of Sandvik’s infrastructure completely invisible to unauthorized users, while still granting authorized users least-privileged access.

Protecting any application, anywhere, on any device

ZPA’s cloud-delivered zero trust network access (ZTNA) strategy provides Sandvik with support for both managed and unmanaged devices as well as any private application, not just web apps.

The Zscaler solution accomplishes its mission using two lightweight applications. The first, called Client Connector, is deployed on client devices. The second, App Connector, is deployed to applications, which can range from a company’s entire presence on a public cloud to only specific software systems.

“In less than five days, we smoothly, safely and cost-effectively transitioned 20,000 employees to WFA by replacing VPNs with Zscaler’s zero trust network access solution.”

– Michael Alvmarken
Service Manager for Cybersecurity and Technology
Sandvik Group
“It didn’t really matter where an application resided, whether on premise or in the cloud, ZPA adapted to our situation,” said Alvmarken. “We built out our ZPA environment really quickly and, at the same time, segmented applications appropriately.”

Segmenting access provides customers like Sandvik with the ability to automate and control user connections while simultaneously speeding application log-ins. ZPA enables this by creating TLS-based encrypted microtunnels every time a user attempts to access an application, increasing security for sensitive data while also ensuring traffic takes the fastest path.

Configuration tasks slashed from hours to seconds

According to Alvmarken, the company is also impressed with the simplicity, flexibility and scalability of ZPA.

On the application side, Sandvik rapidly adjusted the number of App Connectors to enhance user experiences. “We started with two App Connectors, giving users access to the applications they needed most,” Alvmarken said. “On our rollout’s first day we discovered we needed more App Connectors to achieve the performance and segmentation we wanted, so we added more.”

Adding connectors is so much simpler than deploying VPN gateways there’s just no comparison, he added. “Configuring a virtual VPN gateway takes over an hour,” Alvmarken said. “Deploying an App Connector takes seconds.”

As Sandvik's implementation continued, the IT team scaled out App Connectors to place them in geographic proximity to users. “For example, we deployed App Connectors to Azure by region, which ensured users were connecting over the shortest distance,” said Alvmarken. “Doing so further reduced latency and improved performance.”

Revealing undiscovered applications

Obtaining granular visibility into applications and their utilization proved another game-changer for Sandvik. “ZPA enables us to see every application in our environment, including who is accessing them,” Alvmarken said. “We also gain other valuable data for generating analytics insights.”

What’s more, the solution’s intuitive dashboard reveals previously undiscovered internal applications running on-prem or in a public cloud. “The ZPA environment displays all of the applications it discovers,” Alvmarken said. “This significantly improved our visibility into what applications we needed to protect and which users needed access to them.”

"It doesn’t really matter where an application resides, whether on premise or in the cloud, ZPA adapted to our IT environment.”

– Michael Alvmarken
Service Manager for
Cybersecurity and Technology
Sandvik Group
Combining this visibility with ZPA’s customizable policy tools enables enterprises like Sandvik to set and enforce granular policies for discovered applications to ensure least-privilege access. Such control, along with Zscaler’s other capabilities, minimizes exposure and reduces attack surfaces.

“ZPA’s visibility and control are real eye-openers as well as excellent contributors to lowering risk,” said Alvmarken.

Streamlined access delights users, enables M&A growth

Moving forward, Sandvik will consider other Zscaler options for improving zero trust network access. Meanwhile, the company intends to fully leverage ZPA’s features, including capabilities for smoothing corporate acquisitions.

No matter what new initiatives come next, Sandvik’s successful ZPA deployment eliminated access hurdles imposed by VPNs, resulting in exceptionally positive user responses.

“We received comments like ‘Wow, we don’t have to log into the VPN?! That’s amazing,” Alvmarken said. “Users repeatedly called our new approach lightning-fast.”

“It’s all a big win for our employees, our company productivity and for our security posture,” he added.

“User response to Zscaler has been overwhelmingly positive, which is a big win for our employees and our security posture.”

– Michael Alvmarken
Service Manager for Cybersecurity and Technology
Sandvik Group

Staying competitive in uncertain times

Anticipating the worldwide impacts of COVID-19, Sandvik rapidly transformed its workforce to a secure, high-performance, zero trust WFA model, enabling all global lines of business to keep running smoothly while keeping productivity and profitability high.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world’s largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.