semperis

CASE STUDY WHITBY

Whitby

For a community of 150,000, protecting identity infrastructure—a key target for attackers—requires deep insight into the AD environment's security. With Semperis Directory Services Protector, the town improves visibility into its security posture and leverages actionable information for mitigating vulnerabilities, reducing risk, and strengthening operational resilience.

> If you're not regularly looking into the health and the security of your Active Directory, I think it's imperative that you take the time to do that and do whatever you can to secure and protect that vital system.
>
> If you lose Active Directory and you rely on it, you're going to lose everything.

Rob Brodofske
Senior Manager of Infrastructure and Security Services, Town of Whitby

AUTOMATING IDENTITY PROTECTION STRENGTHENS SECURITY POSTURE FOR THE TOWN OF WHITBY

As cyberattacks against the public sector continue to increase, protecting identity infrastructure—a key target for attackers—has become a critical imperative. For most organizations, that means strengthening the resilience of Microsoft Active Directory (AD).

For the Town of Whitby in Ontario, Canada, that meant investing in a solution that could provide the town with a deeper level of insight into the security and configuration of its AD environment.

The identity system is the fabric that connects users to services, and any disruption that prevents users from accessing resources hampers town operations. Restoring those operations for the community of roughly 150,000 would incur significant costs in both time and money.

IMPROVING IDENTITY SECURITY POSTURE VISIBILITY

As in the private sector, government organizations are not immune to ransomware attacks. Attackers who exploit Active Directory misconfigurations can quickly escalate privileges and expand their foothold, often lying in wait, ready to strike whenever they want.

In 2022, St. Marys, also in the province of Ontario, experienced a ransomware attack[1] that disrupted services there. The outcome of that attack—which cost St. Marys millions—would have been much worse had the town not already been planning a cybersecurity improvement program. That experience serves as an example to other municipalities, regardless of their size.

Rob Brodofske, Senior Manager of Infrastructure and Security Services for Whitby, takes such lessons seriously. He is tasked with providing the strategic planning needed to meet the network and security requirements that Whitby's technology infrastructure needs to deliver services to the town's residents. He is in charge of the Technology Infrastructure team and part of the Technology and Innovation Services department, which has some 40 people.

"I know how important Active Directory is to my organization, and while I have many tools at my disposal, I felt there was a gap in how it may be secured," said Brodofske. "Specifically, I didn't have a method to shine a light on the potential vulnerabilities or risks within the identity aspect of my infrastructure. I wanted something that would be able to look deep into Active Directory and provide me with the confidence that I was seeking in our controls and our configuration."

Before turning to Semperis, the team was able to perform log monitoring but had no tools that could provide deep visibility into AD or quickly detect vulnerabilities and misconfigurations, he explained. One of his security architects ran Semperis' **Purple Knight** tool, and Brodofske was impressed by the information it gathered and how it was presented. He was immediately able to see a snapshot of AD vulnerabilities and misconfigurations, along with recommendations for mitigating them.

"As far as I knew," Bodofske said, "nothing like it existed at the time, so I wanted to learn more." While attending a cybersecurity event, he met with representatives from Semperis and learned more about the company's products.

REDUCING RISK WITH PROACTIVE IDENTITY PROTECTION

The IT department adopted **Directory Services Protector (DSP)**, which continuously monitors AD for indicators of exposure and compromise. The move enabled Brodofske's team to proactively hunt for potential risks and remediate them before they could be compromised.

"If you're not regularly looking into the health and the security of your Active Directory, I think it's imperative that you do take the time to do that and do whatever you can to secure and protect that vital system," he said. "I think everybody focuses a little bit more on the edge and, from time to time, we forget about Active Directory. But if you lose Active Directory—and you rely on it—you're going to lose everything."

Deploying DSP was painless, he said. When questions arose, the Semperis support team was there to lean on, he added. After a few 90-minute sessions to help his team get reporting, analytics, and Azure capabilities up and running, the implementation was running seamlessly.

One key area where the organization has benefited from DSP is its ability to capture evidence of changes—even if security logging is off—and allow organizations to roll back malicious changes to on-premises AD.

According to Brodofske, "The ability to detect and immediately undo those changes was definitely something that was very attractive to us. And it works so well that, cheekily, my staff sometimes forget that it's there. When they go to make some change, DSP catches them and undoes what they've done. They have to remember to go in and enable those changes first."

Just like unpatched vulnerabilities, unsafe configurations caused by human error or configuration drift can open the door to attackers and regulatory compliance violations. Although Whitby's AD environment consists of only one forest, he is keenly aware that organizational restructuring can challenge the ability to keep AD running smoothly, even in smaller environments. Over time, reorganization has made the town's AD environment "a little messy" from that perspective, he admitted.

CONFIDENT SECURITY POSTURE MANAGEMENT

Brodofske said he is looking to make Whitby's hybrid AD environment more resilient against risky changes, especially as more services move into the cloud. As modifications are made to the environment, using DSP has enabled Brodofske's team to mitigate risk, undo mistakes, restore certain objects, and recover services more quickly.

Importantly, leveraging Semperis' technology has given him more confidence in the town's ability to face future challenges.

"I'm in DSP several times a week just looking for new indicators of exposure, monitoring my score, and then actioning it," he said. "We're a very security-conscious team here at the Town of Whitby, and if it's something that I can action, I want it actioned. There's no reason to let it linger, right?

> "I'm significantly more confident because now I can see the things that I previously could not see."
>
> **Rob Brodofske**

ENDNOTE

[1] https://www.stratfordbeaconherald.com/news/local-news/st-marys-cyberattack-cost-town-1-3-million-including-290000-ransom