ITWC The Content Experts

CanadianCIO
VIRTUAL ROUNDTABLE

It's time to get started on Zero Trust

SPONSORED BY

CYBERARK®   SailPoint

HOSTED BY

CanadianCIO

> “Perimeters are falling down now due to remote work and the cloud.
>
> *— Chris Ruetz, AVP and Country Manager, CyberArk*

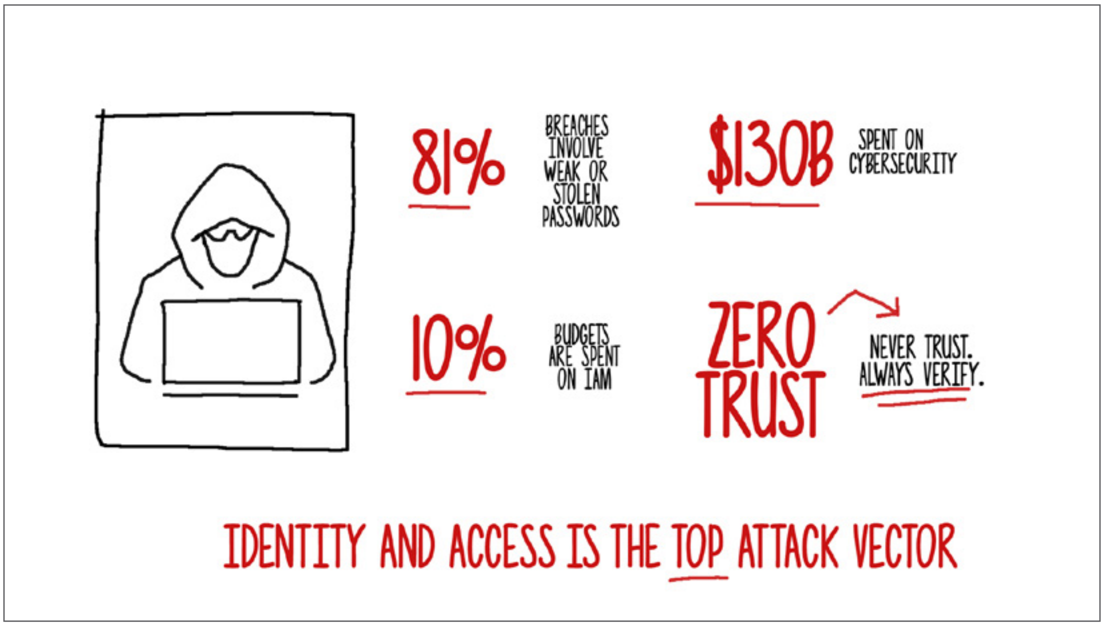
The CanadianCIO virtual roundtable *Zero Trust for the Real World: What’s Holding You Back* was held November 17, 2020. Hosted by ITWC CIO Jim Love, and sponsored by CyberArk and SailPoint, the discussion looked at why Zero Trust has become the go-to standard in security and how organizations can move forward with this approach. Expert advice was shared by Chris Ruetz, AVP and Country Manager for CyberArk, James Toomey, Country Manager, Canada for SailPoint and Ian Gritter, Manager, Sales Engineering at SailPoint.

PERIMETER SECURITY IS NO LONGER ENOUGH

Zero Trust and digital identity, together, have become one of the more important developments in security today, said Jim Love, ITWC CIO, as he opened the roundtable. “A lot of us have challenges with securing the remote work environment,” he said.

The traditional approach of protecting the perimeter isn’t working anymore, said Chris Ruetz, AVP and Country Manager for CyberArk. “Perimeters are falling down now due to remote work and the cloud,” he said.

At the same time, the number of cyber attacks has been rising sharply, especially since the pandemic began. Most of the time, the attackers are gaining access to networks by exploiting weak or stolen passwords, often obtained through phishing exercises. “Identity is the new perimeter,” said Ruetz. Organizations should press forward more urgently to protect themselves with a Zero Trust approach.


81%
BREACHES INVOLVE WEAK OR STOLEN PASSWORDS
$130B
SPENT ON CYBERSECURITY
10%
BUDGETS ARE SPENT ON IAM
ZERO TRUST
NEVER TRUST. ALWAYS VERIFY.
IDENTITY AND ACCESS IS THE TOP ATTACK VECTOR

> “You’d be surprised at the number of organizations running manual identity management processes.
>
> *— James Toomey, Country Manager, Canada, SailPoint*

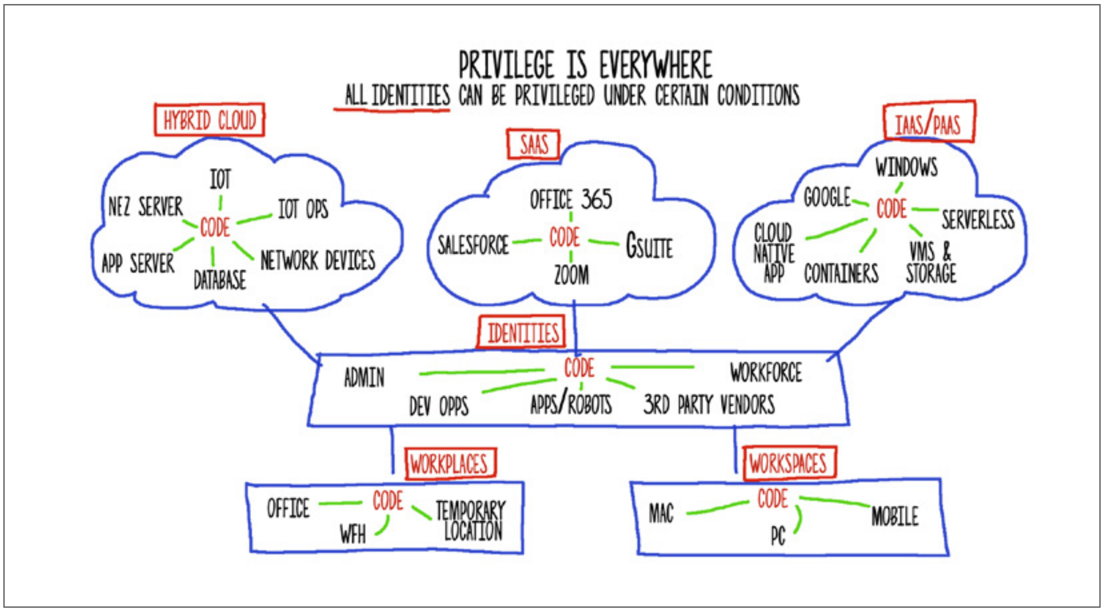
ZERO TRUST IS NOT A PRODUCT

The concept of Zero Trust was coined by an analyst at Forrester Research ten years ago, said Ruetz. It has become more mainstream as organizations make the transition from a traditional infrastructure to a more modern one.

Zero Trust is a strategy based on the idea that the identity of anyone (or anything) trying to connect to an organization’s systems must be verified to gain access. With the traditional “castle and moat” approach, once someone was allowed inside the network, they were presumed to be trusted to move around to access applications. With Zero Trust, “it is not whether they are from the outside or inside but you need to prove you are who you say you are,” said Ian Gritter, Manager, Sales Engineering at SailPoint. “It’s a philosophy that you should always assume something is risky unless proven otherwise,” added James Toomey, Country Manager, Canada for SailPoint.

This means placing identity at the centre of the security architecture and truly understanding who should have access to what and how that access is used, he said. “Identity is the currency for validation,” said Gritter. It is not a single product, he said, and IT leaders should be skeptical of any vendor that tries to sell it that way.

"It's a desire to prove that every step along the way has the appropriate security," said Gritter. Organizations should no longer assume that those on the network are just employees. What's more, the number of privileges has been multiplying with the growth of the cloud. Most organizations have four times the number of access privileges than they have employees. "At every access from one section of the network to another, you have to implement a risk-based approach with continuous multi-step authentication."



> "Perimeters are falling down now due to remote work and the cloud.
>
> *— Chris Ruetz, AVP and Country Manager, CyberArk*

MAKING IDENTITY GOVERNANCE EASIER

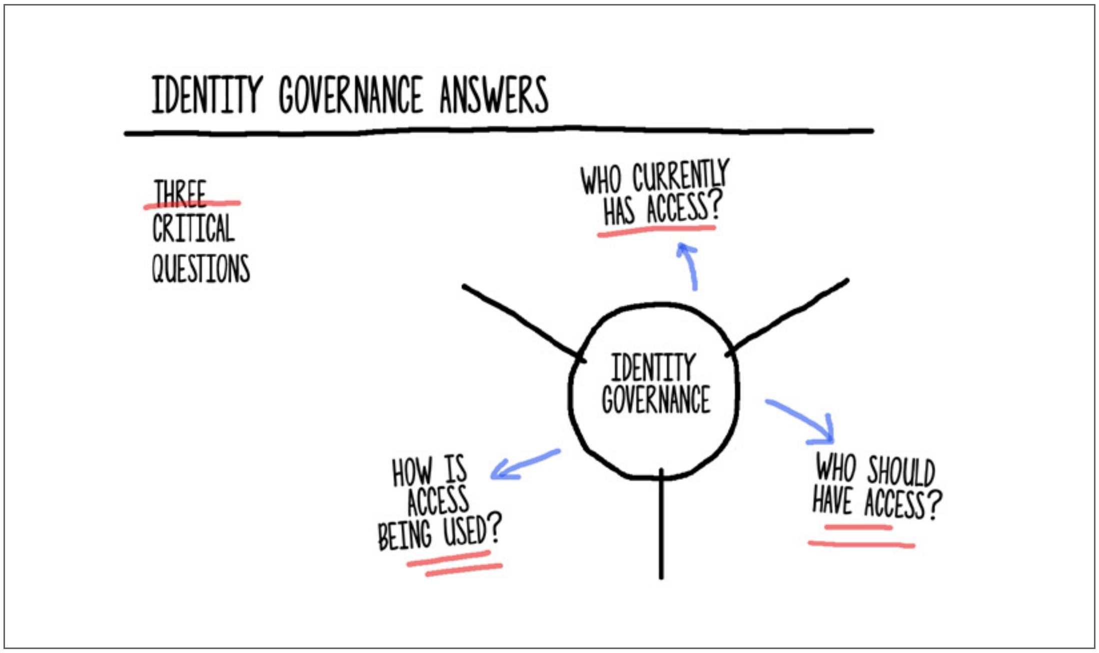
During the roundtable, participants were asked how they're managing their identity governance process today. Most, at 57 per cent said they have limited automation or a legacy solution for identity management. Thirty-six per cent said they rely on identity management as a strategic foundation for security, while 7 per cent said they're using manual processes.

In another poll question, the IT leaders were asked how they measure the importance of governance in their organization. Seventy-one per cent rated this at the moderate level, saying "we sort of know." Twenty-one per said their organizations are strategic and have a solution in place, while 7 per cent said their approach is basic.

> “It is not whether they are from the outside or inside but you need to prove you are who you say you are.
>
> *— Ian Gritter, Manager, Sales Engineering, SailPoint*

Organizations are struggling to make the shift to Zero Trust. “It requires you to rethink a lot of things,” said Ruetz. “You’d be surprised at the number of organizations running manual identity management processes,” said Toomey. It was clear from the discussion that this is not a sustainable way to prevent data breaches.

Fundamentally, organizations should be seeking to prevent credential theft, stop lateral movement within the network, and limit escalation and damage from attacks, explained Ruetz. “You need policies and rules to identify who comes in,” he said.


IDENTITY GOVERNANCE ANSWERS
THREE CRITICAL QUESTIONS
WHO CURRENTLY HAS ACCESS?
IDENTITY GOVERNANCE
HOW IS ACCESS BEING USED?
WHO SHOULD HAVE ACCESS?

“Ask who has access, how the access is used and who should have access going forward.

This is even more critical in a cloud environment, said Gritter. Security problems arise when applications that weren’t originally designed for the cloud are moved there, he said. As well, it becomes difficult to rely on manual processes to track access when applications can be spun up or down so rapidly in the cloud. Another complicating factor occurs when applications that may have both high and low security priorities are placed on the same platform. “This requires you to rethink a lot of things,” he said.

HOW TO START THE ZERO TRUST JOURNEY

Zero Trust can be implemented as a phased approach over time, said Toomey. “The first step is to define the business outcomes you want to achieve,” he said. “Look at your inventory of technology and leverage against that. Put a plan in place and stick to it. Too often, organizations get distracted and make changes, which introduces more risks.”

One of the roundtable participants asked whether adopting Zero Trust means you have to scrap your existing infrastructure. It does not replace existing technology but is added adjacent to what you have, replied Toomey.

Vendors can provide assessment tools to help organizations identify the highest priority applications to protect. These will scan the organization’s environment to identify existing risks related to privileged access. To address these risks, Zero Trust requires a mix of technologies such as multi-factor authentication, identity and access management, privileged access and network segmentation. said Ruetz. Single sign on is also important but just one piece.

> “Where we’re going is not just automating processes. With AI and machine learning, we need to get to a point where it is autonomous or we will never keep up.
>
> *— Ian Gritter, Manager, Sales Engineering, SailPoint*

Behavioural analytics and AI can help understand unusual patterns by providing context to identity management, Ruetz said. Information on what they are accessing and where the traffic is coming from can help the system make decisions in granting access, said Gritter. It also makes identity management easier by starting to automate the process. “Where we’re going is not just automating processes,” added Gritter. “With AI and machine learning, we need to get to a point where it is autonomous or we will never keep up.”

There is no one vendor that provides a complete Zero Trust solution, said Ruetz. Organizations should look for vendors that can scale across multiple areas and integrate a limited number of solutions. “Choose for vendors that work tightly together to shrink the attack surface,” he said.

Get a detailed privileged access risk assessment at no cost with CyberArk Discovery & Audit.

ABOUT CYBERARK

CyberArk is the global leader in privileged access management, a critical layer of IT security to protect data, infrastructure and assets across cloud and hybrid environments and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company has offices throughout the Americas, EMEA, Asia Pacific and Japan.

www.cyberark.com

ABOUT SAILPOINT

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive IdentityTM platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically.

www.sailpoint.com

ABOUT CANADIANCIO

CanadianCIO is an integral source of strategic insight for CIOs and senior executives. It focuses on issues related to the strategic use and management of information technology within the enterprise. It takes a hands-on, real world approach to exploring issues such as: the creation of business value through the use of IT; the evolving role of the CIO; IT-driven business transformation; innovation; information privacy and security.

www.itbusiness.ca | www.itwc.com