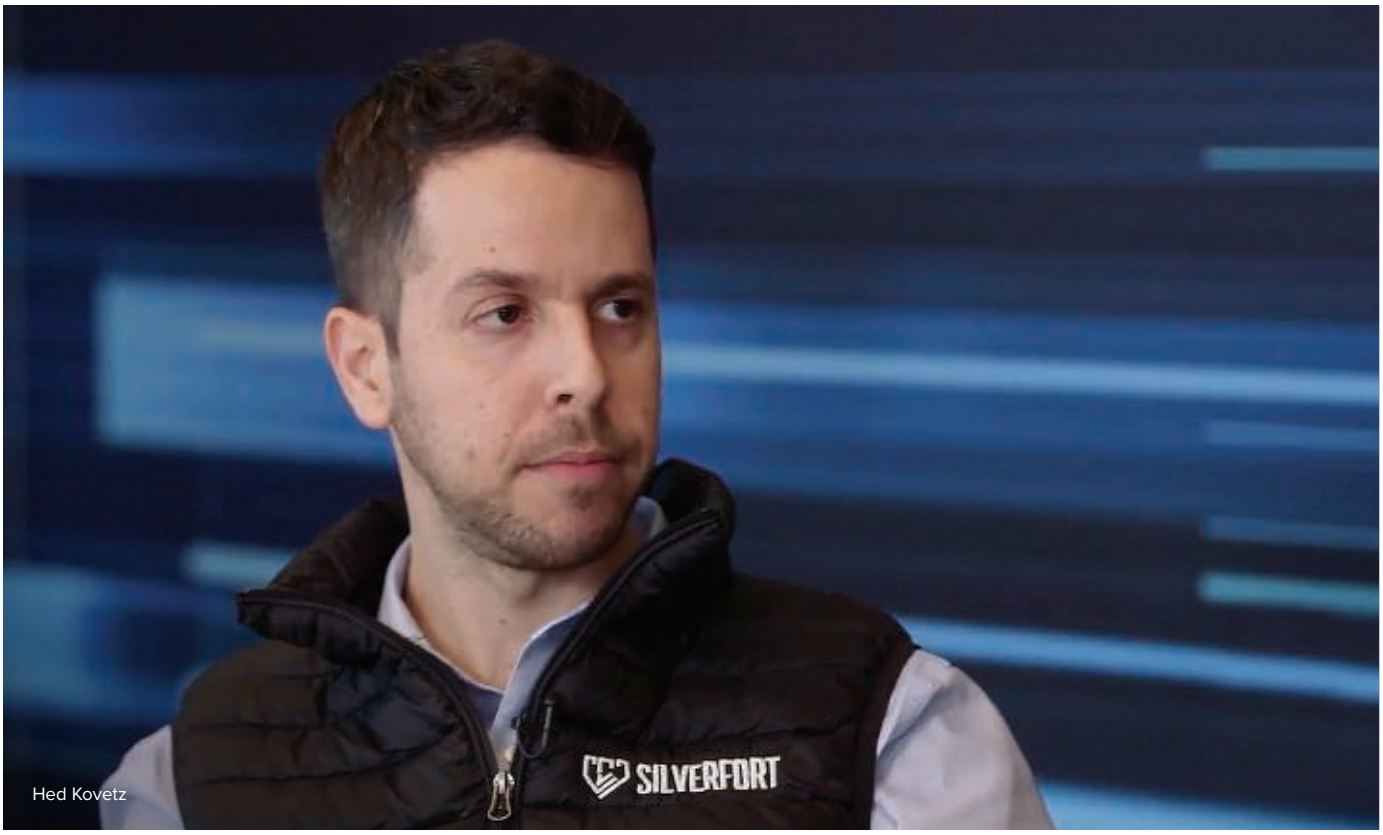
INTERVIEW TRANSCRIPT

ADDRESSING IAM PAIN POINTS AND SECURITY GAPS

Hed Kovetz of Silverfort Reviews Holistic Agentless Approach to Secure Authentication

SILVERFORT

ISMG
INFORMATION SECURITY
MEDIA GROUP



Hed Kovetz

Corporate networks have been going through dramatic changes in recent years, due to IT revolutions such as the cloud, IoT and BYOD.

In this new reality, with countless devices and services all connected to each other without clear perimeters, verifying user identities and controlling their access to sensitive resources becomes more important than ever, but also far more difficult to achieve, says Hed Kovetz of Silverfort.

In an interview with Nick Holland of Information Security Media Group, Kovetz discusses:

- The impact of trends, such as cloud, BYOD and IoT, and the growing need for secure authentication;
- The need to secure any-to-any communication and enforce true "zero trust" security policies;
- How Silverfort's unified agentless approach for IAM is helping clients to address these challenges.

Kovetz is the CEO and co-founder of Silverfort, a provider of agentless authentication and zero trust security solutions. Prior to founding Silverfort, he served in product leadership positions at Verint.

IAM Changes

NICK HOLLAND: There have been a lot of changes when it comes to identity and access management over the last few years. Can you tell me some of the changes you've come across?

HED KOVETZ: There are a lot of changes, especially because corporate networks are really changing and evolving. If you look a few years back, corporate networks were pretty simple. They had a very clear perimeter surrounding them. It was really enough to protect authentication and access at the perimeter, when somebody was connecting from the outside of the network into your corporate network. That's why all these existing authentication and access solutions were designed to protect a specific point of access, which is your perimeter.

But networks don't look anything like this anymore. You have today cloud resources. You have IOT devices. You have a lot more personal devices that people are bringing in. You have a lot more people working remotely now.

In this reality, we don't have a clear perimeter anymore. We have countless different user, devices and applications everywhere that are communicating with each other without even going through any clear perimeter or gateway. The question is: In this new reality, where do you even enforce secure authentication and access? How do you do it? How do you deliver it? Because it's a very complex, dynamic, hybrid environment.

"Attackers have found ways to bypass agent-based authentication solutions and penetrate systems through unprotected interfaces, like Remote PowerShell."

Pain Points

HOLLAND: What are some of the specific pain points you've seen with organizations today?

KOVETZ: One of them is the fact that for a lot of these servers and applications that people are trying to protect now, you actually need to protect them one by one because you can't count on the perimeter anymore. They don't support anything except password-based authentication, which we all know is not good enough today. Building secure authentication into each of these applications individually is very difficult.

One of the challenges is even if you build secure authentication into one of them, it would not fully protect that specific application because it would only protect one particular way of accessing it – one of the interfaces, maybe the web interface, maybe the remote desktop.

There are countless different alternatives where you can connect into a server or into an application with all kinds of command line tools and accessing file shares. All these things allow attackers to bypass multifactor authentication, even if we build it for every system. That's one very clear pain point that we see in a lot of data breaches is how attackers actually get in.

Another pain point we have seen a lot recently is the need to protect machine-to-machine authentication. For a long time we were just dealing with human authentication, so we had things like multifactor authentication with a one-time passcode, or a smart card. That doesn't work for machines. In the cloud world, in the automated, modern, IT environment, a lot more services are automated. They're just accessing one another without any human that can actually verify its identity. How do you protect this machine-to-machine access when there's no human to prove their identity? That's another challenge that we help companies address.

Then another one has to do with cloud migration. Obviously, everyone wants to move to the cloud now. One of the challenges, when it comes to security in the cloud, is when you migrate, when you lift and shift some of these existing applications to the cloud, how do you protect them? Assuming that they don't support any cloud native identity and access framework or any kind of modern authentication, it looks like what you need to do is build secure authentication frameworks into each and every one of them. If you are a big enterprise, that's an endless task.

We are talking with some enterprises who have been spending the last couple of years trying to achieve that. They say it will ever end because they have too many of these applications. So being able to apply some kind of unified, transparent layer of secure authentication and access across these applications, without having to modify them one by one, is crucial if we want to allow enterprises to move to the cloud.

These are just a few pain points that are very common that we see in a lot of enterprises.

Silverfort's Role

HOLLAND: How does Silverfort help organizations upgrade their approach to identity and access management?

KOVETZ: We really looked at this problem from the high-level problem we described to all these specific challenges. We figured we need a new approach for delivering secure authentication and access. It cannot be done by protecting every single device and every single application one by one. That's not possible in today's dynamic perimeter-less environment.

So we invented a way of seamlessly delivering secure authentication and access across all these use cases, without having to deploy any agents or proxies or making any changes to those individual applications.

What that means on the technical level is we solve all these challenges I just mentioned. We can protect all these legacy applications, this infrastructure equipment and things that don't support secure authentication, including those interfaces that allow attackers to bypass the existing multifactor authentication. It means that we can protect anything – humans, machines, on-premises, in the cloud.

As opposed to protecting individual assets or just specific points of access like your gateways, we can actually extend an intelligent, AI-driven, authentication policy across everything you have connected to your network. Again, that means on-premises, cloud, infrastructure, applications, machines, humans – all of that – because we don't need to integrate with them one by one. Because we have a seamless way of applying them.

The way it works is we actually found a way to analyze the existing authentication protocols that your applications and servers are using. Instead of replacing them, which again we don't think is realistic, we found a way of enforcing an additional layer of protection on top of them. It's a very unique solution.

We are the only company today that can do that, which is why we are seeing amazing reaction from the market. It's just a way that makes much more sense for organizations to deliver secure authentication and access which is a holistic approach – not system-by- system; not just for a particular use case; not having a bunch of different siloed solutions – but just a way to extend it everywhere without any agents or proxies.

By doing that, we also address all of these challenges we just mentioned. We let people migrate to the cloud securely without having to change their applications at all. We protect the inside of your network and not only the perimeter. We protect machine authentication, not just humans, because we can identify that. We can learn that. We can apply a policy on that. We make sure nobody can bypass your protection.

Because no matter how you try to access something, within a corporate network or cloud, we can apply a policy on it. We don't even care what it is. That's really the beauty of this technology. We believe this is the next-generation approach for secure authentication and access in the perimeter-less cloud. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io