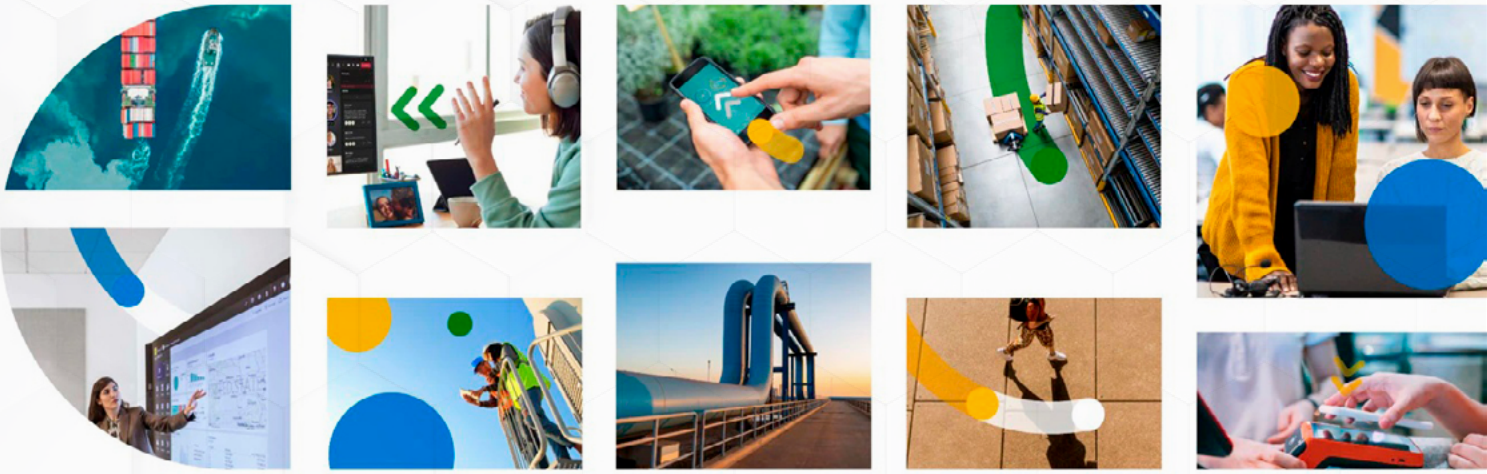
iSMG
INFORMATION SECURITY
MEDIA GROUP

Microsoft

Benefits of Automated XDR Platforms

Microsoft's Scott Woodgate on Improving Security Posture Using XDR



Microsoft

Scott Woodgate

Woodgate's team drives SIEM + XDR security marketing for Microsoft. For over 20 years at Microsoft, he has served in a number of roles including driving Azure Virtual Desktop, Windows, BizTalk Server and field marketing.

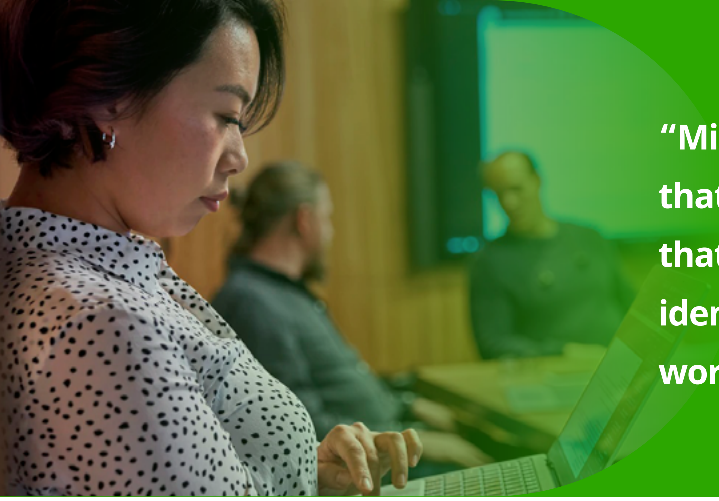
Automated XDR platforms are increasingly sought after as organizations grapple with tool sprawl and the complexity of their security stack. But is there a risk of XDR platforms becoming a single point of failure? Microsoft Senior Director **Scott Woodgate** emphasized building "resiliency" for XDR.

Microsoft's XDR technologies are designed to protect various assets within an organization, including email identity endpoints, cloud infrastructure and cloud workload, he said. The company provides "ROI advantage" and "faster response time" to customers who adopt an integrated stack of security products.

"It's hard to stop a ransomware attack early in the process. Ransomware attacks run amok more than they should today," Woodgate said. To ensure quicker response to such incidents, Microsoft recently released Attack Disruption and Microsoft 365 Defender to automatically contain the progress of attacks and help protect organizations at "machine speed."

In this video interview with Information Security Media Group at RSA Conference 2023, Woodgate also discusses:

- Ways to address the shortage of skilled personnel in the industry by using AI;
- The benefits of integrating XDR with identity and access management;
- Microsoft's plans for further advancements in the XDR space.



“Microsoft considers the full breadth of services that you need to have protected and we enable that for the security folks. Our XDR protects email identity, endpoints, cloud infrastructure, cloud workload and so on.”

Benefits of an Automated XDR Platform

ANNA DELANEY: Organizations often talk about tool sprawl and the complexity of their security stack, and there’s a drive to automate XDR platforms. What services can these platform offer?

SCOTT WOODGATE: The customer problem in security that XDR solves is ransomware. And to protect against ransomware, you need to protect against all the places that attackers might go. You need to protect your endpoints, identities, cloud apps, cloud infrastructure and on and on. You need to protect the breadth of the assets within the organization. And frankly, that’s hard and requires a lot of investment. There are very few vendors with XDR offerings that protect against the customer problem, which is ransomware, because it’s expensive to do. But Microsoft considers the full breadth of services that you need to have protected and we enable that for the security folks. Our XDR protects email identity, endpoints, cloud infrastructure, cloud workload and so on. Anytime you build a technology, you want to make sure it’s really resilient, and our technologies are built on cloud hyperscale infrastructure that is distributed globally all over the world. It is designed for scenarios that might affect resiliency. Resiliency is super important, and we take care of it natively in the architecture of our XDR technologies.

The ROI of XDR

DELANEY: What’s the ROI of XDR?

WOODGATE: When you think about ROI from an XDR perspective, you have to think about where you started in the past. Typically, customers in the past had an individual product for protecting endpoints, another individual product for protecting email, and another one for protecting identities. There was vendor complexity and cost associated with that. There were also some TCO aspects associated with it, because instead of seeing a visualization of an attack, a security person would find some endpoint information and then have to figure out manually how it related to the email information and then figure out manually how it related to the identity information. That took a lot of time.

The technologies we have now bring all that information straight to the customer and get it all from one vendor. There are two advantages to that: You get an ROI advantage of up to 200% when you choose Microsoft’s integrated

stack as opposed to individual vendor purchases. You also get the wonderful benefit of better security. We've seen people get a 65% faster response time to security incidents and save ROI. How often do you save money and get better security at the same time?

Integration Capabilities of XDR

DELANEY: Can you integrate other products?

WOODGATE: Yes. Our XDR capabilities work for multi-cloud and multi-platforms. They support Linux, iOS and Android and all of the platforms as well as Google GCP and AWS. If you want more integrations than that, we also integrate deeply with a SIEM layer. Our SIEM product, Sentinel, adds another 278 connections to SAP, lots of competitive security products, firewalls and everything. This is definitely an open ecosystem, multi-cloud, multi-platform at the XDR layer and at the SIEM layer.

The Limits of EDR

DELANEY: What's the role that EDR can play within XDR? We know that EDR is not enough to combat ransomware attacks, and yet the majority of these attacks come via phishing emails.

WOODGATE: Endpoint protection is important, but it is not the answer to everything. Ransomware attacks do often come through an email, and 10% of phishing emails get past endpoint protection. It doesn't solve that problem. So, if all you've got is an endpoint technology and you don't have email protection, you'll miss catching ransomware earlier. The same is true for identity if you don't have identity protection. It's important to look across the system from end to end.

Tackling the Talent Shortage With AI

DELANEY: The talent shortage is a massive challenge for the industry. How does XDR use automation and AI to tackle that?

WOODGATE: There are 3.6 million or so available jobs at any one point, and there's a real opportunity for AI and automation to help. We certainly don't believe in a world where AI and automation cause a reduction in security resourcing. There are lots of job opportunities for the long term and, for us, it's about how AI and automation help the security team be more effective. There is a never-ending amount of work for the security team, and AI and automation can help junior folks find more advanced use cases and help advanced folks solve more work quickly.

We have AI and automation built into our tools to fuse together events, and we can go through a use case in a minute. We've just announced our new generative AI tool, “We can protect all aspects of the identity and ensure you’re set up with best practices on posture, things like MFA and so on, all from a single provider, all in an integrated way. Other solutions are often piecemeal; customers end up with gaps and those gaps get exploited.”

Security Copilot. It is a virtual assistant, and it’s like having another member of your team working with you. The AI gives you guidance and instructions to help you in the incident, and that helps you scale your security team.

Use Case: Attack Disruption

DELANEY: Let’s go through a use case.

WOODGATE: Often, the state of the art in protecting from ransomware and similar attacks is, unfortunately, recovering from it. The first step in XDR is building a view of what ransomware looks like. Let’s say my email account was compromised and then my device was compromised and then my end user was compromised. With XDR, you can see that, and the security operations team can then take action. But it takes about 72 minutes for an attacker to move from one step to the next step in the process, and all of us take lunch breaks, so it’s hard to stop a ransomware attack early in the process.

Ransomware attacks run amok more than they should today. To respond to that, we recently released our Microsoft 365 Defender product called Attack Disruption, where we complement the security defender with machine speed. This XDR signal knows me, the human, but it also knows my email account and my identity, and yours and perhaps a couple of others, just to make sure, and when something has been compromised, it turns us off from the system. My device is isolated, and my identity is turned off. That will affect my productivity, but the 500 or 1,000 other devices that would’ve been affected from my beacon are now protected from the ransomware attack.

This product is a huge advance in terms of what defenders have today. Some may trust the AI to make decisions in real time to turn off devices and others may not, so you can exclude different assets and resources. It is a big win in terms of protecting organizations and making them safer.

Integrating XDR and IAM

DELANEY: What are the benefits of integrating XDR with identity and access management?

WOODGATE: Identity is a core part of all of this. Many companies have on-premises identities in Active Directory and Entra.

You also need to protect the identity infrastructure at Azure as well as on-premises Active Directory. You need to protect users. Workloads now have identities, and you need to protect them.

Microsoft is in a very unique position relative to the industry because it has the number one identity provider on the planet. Active Directory is so central to so many organizations, but it's also a leading XDR technology. That means we can make the gamut of protections available. On the identity provider side, conditional access is important to ensuring you have security out of the gate for your Active Directory systems. On the other end, you need identity threat protection for cloud or for on-premises and for users, workloads and identities. That's what we do in our XDR technologies.

We can protect all aspects of the identity and ensure you're set up with best practices on posture, things like MFA and so on, all from a single provider, all in an integrated way. Other solutions are often piecemeal; customers end up with gaps and those gaps get exploited.

The Future of XDR

DELANEY: What's next for XDR?

WOODGATE: XDR is an evolving market. Not every vendor that talks about XDR talks about it in the same way. Microsoft provides the most comprehensive XDR on the market in terms of the amount of signals that we put into the XDR. Lots of vendors may have endpoint protection and they've just added identity, and over time, they'll add other sources. They are still building a complete incident view of ransomware. But Microsoft has done that work, and we're taking it to the next level. We'll still add additional rich context. We just added DLP into our incident layer. But we're also continuing the journey with things like Attack Disruption. Today, it applies to a certain set of scenarios, but we'll be adding many more over time to help folks.

Once you've been attacked with something, we learn, and what we've learned is that you can implement some security best practices to prevent that attack in the future. There's a closed loop between threat protection and posture that we can fill. That will enable you to do a much better job of securing your infrastructure in the first place based on specific attacks. We're taking it to the next level in terms of AI for attacks, and we're informing posture. There's a lot more to come.

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.

(800) 944-0401 • sales@ismg.io

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

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

iSMG
INFORMATION SECURITY
MEDIA GROUP

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