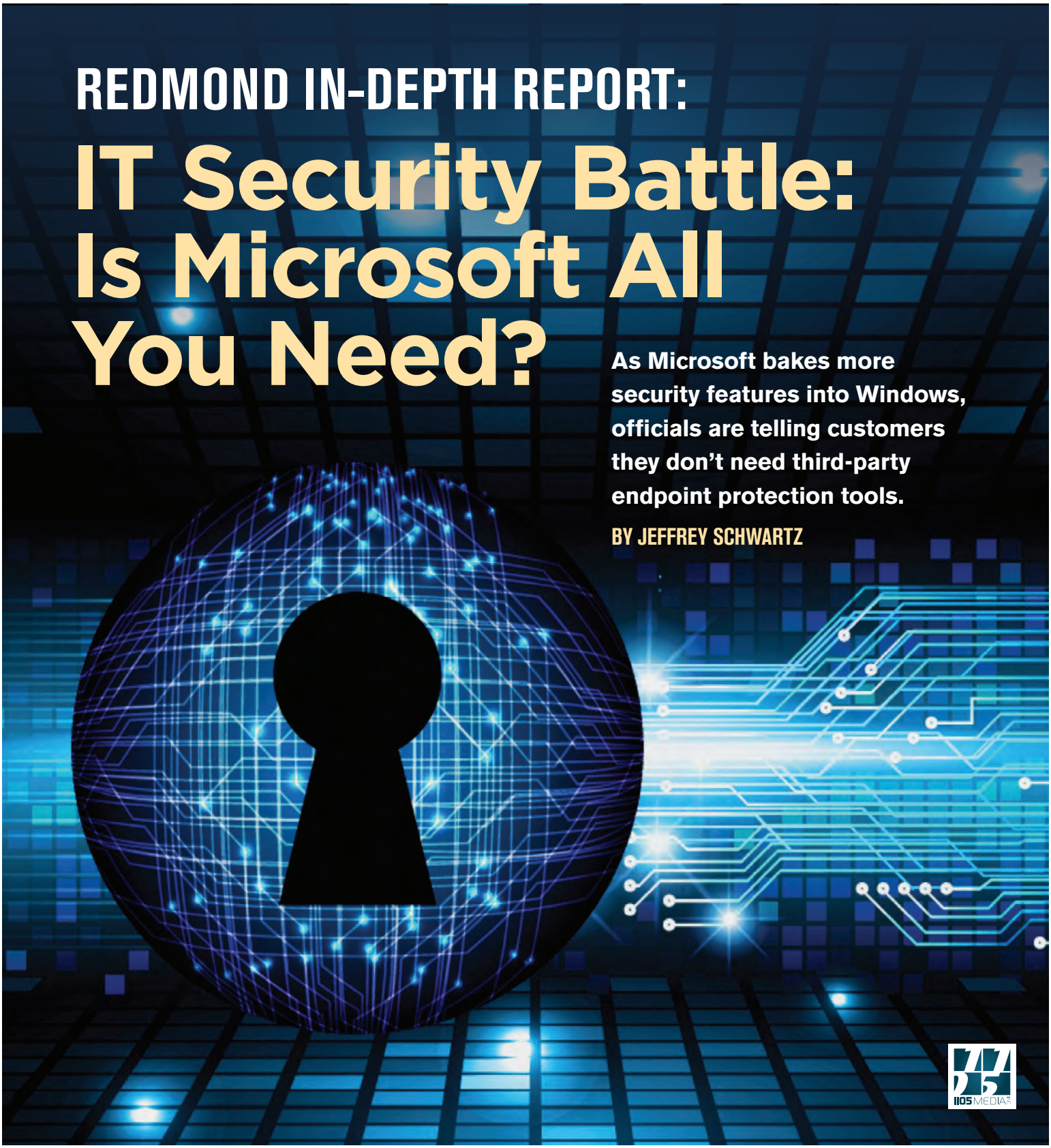
CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY



REDMOND IN-DEPTH REPORT:

IT Security Battle: Is Microsoft All You Need?

As Microsoft bakes more security features into Windows, officials are telling customers they don't need third-party endpoint protection tools.

BY JEFFREY SCHWARTZ

This year will mark the 15th anniversary of the infamous Trustworthy Computing manifesto by Microsoft Founder and then-Chairman Bill Gates. In an e-mail to all Microsoft employees on Jan. 15, 2002, Gates issued his "call-to-action" that everyone needed to make, improving the security of the company's products. Gates' message, published by Wired magazine, introduced Trustworthy Computing.

At the time, Microsoft's reputation for delivering secure software was abysmal and it was the company's reputation in a big way. Gates decided to make it a key priority to fix, aware it was an ambitious undertaking.

"Eventually, our software should be so fundamentally secure that customers never even worry about it."

Bill Gates

"Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these fixes," Gates told employees. "Eventually, our software should be so fundamentally secure that customers never even worry about it." By all accounts, Microsoft has made groundbreaking improvements in its software.

The company published its Trustworthy Computing framework six months later, which in summary focused on what would become the Software Development Lifecycle where all developers would have the tools and methodologies to "make an-order-of-magnitude improvements" in the building of secure software, the policy of distributing regular updates–including the introduction of Windows Update and Software Update Services–and in early recovery capabilities to restore systems prior to an incident.

Widening Security Portfolio

To those who weren't around at the time, it may seem incongruous that such basic functions didn't exist. Marked advances in security oddly enough debuted in the otherwise-panned Windows Vista release in 2006 with significant improvements in every new release since. The release of Windows 10 in 2015 followed by last year's "Anniversary Update" offered a doubling-down of security in a number of areas, including such features as Virtual-Based Security (VBS), Windows Information Protection, Credential Guard and Device Guard, Windows Defender Threat Analytics and, this year, the Windows Security Center that will add a

management and reporting capability to the client OS, among many new and extended features.

The most controversial of new features came with Windows 8 and the release of Windows Defender, an antivirus tool bundled into the OS. By all accounts, including a recent public proclamation by Microsoft, Windows Defender was no match for the key antivirus and anti-malware solutions, for which there are many from the likes of AVG Technologies, BitTitan Inc., Kaspersky Lab, Sophos Ltd., Trend Micro Inc. and Intel Security Group, which will soon revert back to its McAfee Inc. brand when the CPU giant spins off its controlling interest in the company it acquired several years ago.

Microsoft: Kick Out Endpoint Software

In the most recent releases of Windows, Microsoft has made no bones about the fact that it intends to obviate the need for those third-party wares. In a session at the fall Ignite conference in Atlanta, Chris Hallum, senior product manager for Windows client security, said Windows Defender has improved to the point where customers don't need additional antivirus and anti-malware software. Acknowledging it's not the best, Hallum said it's good enough and getting better.

"We are committed to be No. 1. I can't promise we will be No. 1, but I can promise you we will be within one-tenth of a point, meaning we have gracefully comparable protection," said Hallum. "This is something you should put on the roadmap, I want you to evaluate it, and I want you to start kicking out third-party antivirus because we have a great solution right now, and it's going to be even better in the months to come."

"... start kicking out third-party antivirus because we have a great solution right now, and it's going to be even better in the months to come."

Chris Hallum, Senior Product Manager, Windows Client Security, Microsoft

It wasn't an idle remark. Microsoft consistently has made that point. At a recent briefing for customers and prospects, a security architect at the company made that same point and other officials have made similar pitches. Not surprisingly, Microsoft's view on the matter has raised the ire of antivirus suppliers. Most are keeping their dissatisfaction close to the vest, but one who has spoken out is Eugene Kaspersky, founder of the antivirus supplier that bears his name, Kaspersky Lab.

"We think that Microsoft has been using its dominating position in the market of operating systems to create competitive advantages for its own product."

Eugene Kaspersky, founder Kaspersky Lab

Kaspersky has gone so far as to accuse Microsoft of anticompetitive practices, filing a claim with the EU's European Commission and the Federal Antimonopoly Service in Russia, where the company is headquartered. "We think that Microsoft has been using its dominating position in the market of operating systems to create competitive advantages for its own product," he wrote in a recent blog post. "The company is foisting its Defender on the user, which isn't beneficial from the point of view of protection of a computer against cyberattacks. The company is also creating obstacles for companies to access the market, and infringes upon the interests of independent developers of security products."

Microsoft has declined to comment on the claim but days before Kaspersky's announcement, Rob Lefferts, the company's director of program management for Windows Enterprise and Security, pointed to improvements to Windows Defender that were added to the recent Anniversary Update, particularly as it related to added detection capabilities.

"Windows Defender, which is enabled by default, can respond to new threats faster using improved cloud protection and automatic sample submission features to block malware at first sight," Lefferts said in a blog post. "We've also improved Windows Defender's behavioral heuristics to help determine if a file is performing ransomware-related activities, and then detect and take action more quickly."

Also, new in the Windows 10 Anniversary Update is Windows Information Protection, which brings separation technology to address data leakage and is designed to work with the Azure Rights Management feature in the Enterprise Mobility Service.

Disputing Windows Defender "Hype"

Most providers of antivirus software haven't complained about Microsoft's increased emphasis on Windows Defender, though most scoff at the idea. "To some degree, it may sound harsh, but there's a little bit of arrogance in their claims and I think it's a little bit of living in an echo chamber," says Dan Schiappa, senior VP and general manager of end user and network security business at Sophos. "They get in their bold little worlds and start to believe their own hype."

Schiappa argues most experts and customers he deals with aren't buying Microsoft's claims. "What we see as outside vendors in the real world [is that] there's a much different picture than the platform guys seem to be seeing. If you pick any CSO in the world and say, 'Hey, just run on Windows Defender and you don't need anything else,' and see how long they'd keep their job, I just don't think anyone would be willing to bet their job on that." Using the company's recently released new Intercept X threat detection tool focused on protecting organizations against ransomware, Schiappa insists Windows Defender doesn't come close.

"We can't keep up with the demand," Schiappa says. "Anybody who even catches wind of it is beating our door down. That's an indication that free Defender is not a solution that's viable to any logical customer. It's just not." Of course, any vendor is going to have a counter-claim. In his Ignite presentation, Hallum said the tide is turning in favor of Windows Defender and the cadre of other protection capabilities built into Windows 10.

Hallum pointed to one customer, whom he didn't identify, that's doing away with third-party antivirus software and relying on Windows Defender. Other large organizations, including two of the largest financial services firms, a major automotive company and one of the largest manufacturers in the country, were in the midst of conducting proof-of-concept evaluations, he claimed "We are going to see it ramp," Hallum said. "We have finally gotten to the point where people are investigating it."

"There's really only a handful of software out there that results in the vast majority of infections, after all. Enterprises that either haven't realized this, or are heavily dependent on the software that gets hit the hardest are still using third-party solutions that are complementary to Defender."

Adrian Sanabria,
a 451 Research Inc.

Adrian Sanabria, a 451 Research Inc. analyst focused on endpoint security, is seeing more enterprises set up Windows Defender on users' PCs to mitigate the threat of infection from commodity malware. But that doesn't mean it's better, Sanabria says. "It's mitigating or avoiding altogether the software that gets hacked most often," he says. "There's really only a handful of software out there that results in the vast majority of infections, after all. Enterprises that either haven't realized this, or are heavily dependent on the software that gets hit the hardest are still using third-party solutions that are complementary to Defender."

New Windows 10 Threat Analytics

Microsoft has added another component to Defender called Defender Advanced Threat Protection (ATP), introduced in the

Windows 10 Anniversary Update. The new tool shouldn't be confused as an add-on to Windows Defender. Rather, it's a separate offering that shares the name, which Microsoft is looking at branding as a family of security protection tools. Windows Defender ATP is a post-breach service running in the Microsoft Azure cloud that performs analysis and machine learning to "help detect threats that have made it past other defenses, provide enterprises with information to investigate the breach across endpoints, and offer response recommendations," according to Microsoft's description.

Sanabria says it will be interesting to see if Defender ATP is good enough to curb the need for third parties altogether. "Anti-malware products are the biggest revenue producer in the cybersecurity market, and malware is only a significant problem on Windows, so a more resilient OS could have an even bigger impact on this market," he says. "We've already seen a lot of businesses ditching third-party offerings for Defender, so this will be a continuation of that trend, not an entirely new one."

Indeed, just as Microsoft argues against the need for antivirus software, Microsoft is betting it can now also take on the entrenched players who provide advanced analytics solutions.

Indeed, just as Microsoft argues against the need for antivirus software, Microsoft is betting it can now also take on the entrenched players who provide advanced analytics solutions. "This is an advanced, sophisticated product designed to compete with FireEye and a long list of other people in the threat intelligence space," he says.

Guarding Credentials with Intel TPM

Just as critical, the newest Windows 10 release adds improvements to virtualization-based security (VBS) within the OS, including Credential Guard, which uses Intel's latest Trusted Platform Module -- embedded on a growing number of PC motherboards -- to provide hardware-based protection of credential theft. The hardware-based VBS sandboxes aim to protect systems from pass-the-hash or pass-the ticket credential breaches by isolating key information and ensuring that only a privileged system can gain access. It also protects against NTLM password hashes and Kerberos Ticket Granting Tickets, as outlined in the Windows IT Center post.

Device Guard: Evolution of AppLocker

Another important security feature in Windows 10 that organizations will surely evaluate is Device Guard, which introduces a new

approach that lets organizations determine which applications can run on a device. It uses hardware- and software-based security approaches that will only allow trusted applications defined by an administrator to run on a device, allowing them to define their own code-integrity guidelines. Untrusted apps won't run.

When using hardware that meets specific requirements, Microsoft says even if an attacker penetrates the OS kernel, it will be more difficult, though not impossible, to execute malicious code. It requires Windows 10 Enterprise or Education editions and using the new VBS capabilities of the OS can isolate the Code Integrity service from the Windows kernel. Microsoft says the Code Integrity service runs in parallel with the kernel in a Windows hypervisor-protected container.

When using hardware that meets specific requirements, Microsoft says even if an attacker penetrates the OS kernel, it will be more difficult, though not impossible, to execute malicious code.

Device Guard will ultimately replace the AppLocker tool introduced with Windows 7 and Windows 2008 R2, which Microsoft says also lets administrators determine what applications can run. Mark Minasi, an MVP, speaker and author, said Device Guard offers strong protections, but it needs to evolve before it's suited for widespread use. "This is the latest version of AppLocker, although it has a different spin on it," said Minasi during a presentation on Windows security at last month's TechMentor conference, which is produced by Redmond magazine parent 1105 Media Inc. "It's a good idea. It says essentially [to] only run signed applications. But let's be very clear, I just don't want to live in a world where everything I have is signed as of yet."

Microsoft's Hallum acknowledged during his Ignite session that Device Guard will need some improvements before it's widely adopted. "We are going to see it ramp, but I don't think you will see it ramp to the highest level until later [in 2017] when we deliver more stuff," Hallum said. Nevertheless, Hallum said Microsoft internally is running Device Guard on its privileged access workstations. "If you have an IT workstation that acts as a datacenter, you should be using our privileged access workstation solution -- you should be running Device Guard on that," he said. "Because if your IT workstation gets owned for not using strong auth, it's game over for datacenter. So, that's a place where it's being adopted at Microsoft. Everyone is using Device Guard on IT workstations."

Over time, Hallum believes the combinations of Credential Guard, Device Guard and Windows Defender will eliminate the need for third-party protection. “Our belief is customers are spending way too much on antivirus. It’s not even solving the problem. It’s helping, but it’s not really a great solution. You can never fix the problem, so Device Guard is the way, but we know not everybody can get to Device Guard, so we needed to deliver something that can lower the cost of ownership of Windows” by extending the capabilities in Windows Defender.

More Security Features Coming to Windows

Microsoft clearly has more security features in the pipeline when it releases its Windows 10 “Creators Update,” which will include a new Windows Security Center portal that will let IT pros track attacks across endpoints and e-mail, added intelligence and remediation capabilities to the new Windows Defender ATP service, mobile application management, and a promised reduction in the size of updates in components by 35 percent.

As Microsoft evolves the security capabilities in Windows, Windows Server and Office 365, among other products, experts point out that organizations have to protect infrastructure beyond that based on the Microsoft platform.

As Microsoft evolves the security capabilities in Windows, Windows Server and Office 365, among other products, experts point out that organizations have to protect infrastructure beyond that based on the Microsoft platform. Critics will also point to the fact that many of the point solutions offered by third parties have deeper and often easier-to-use tools.

“I don’t think we as the endpoint market or just the general security market would see the growth we’re seeing if people thought the platforms, and the free solutions offered by platform providers, are cutting it,” says Sophos’ Schiappa, who long ago worked at Microsoft and is therefore quite familiar with its focus on security. “I used to work with Bill Gates and he would ask me, ‘Dan, when are we going to have an impenetrable operating system?’ and my answer was always: ‘Never,’” Shiappa recalls. “And he used to get very frustrated about that, but unfortunately, when you have code, there are going to be vulnerabilities in that code, particularly for products that have millions and millions of lines of code.” R

Jeffrey Schwartz is editor of Redmond magazine and also covers cloud computing for Virtualization Review’s Cloud Report. In addition, he writes the Channeling the Cloud column for Redmond Channel Partner. Follow him on Twitter @JeffreySchwartz.