Raising the Bar on Communications Security

The good news: Cybersecurity professionals recognize the need to secure communications security effectively.
The challenge: Doing it right.

Johna Till Johnson
CEO
Nemertes Research

Q1 2019

Table of Contents

Executive Summary **3**

Communications Security: The Missing Link........ **4**

Common Vulnerabilities **5**

SIP Hacking (Data Exfiltration via RTP)........ 5

SIP Interception: MTM........ 6

Other Vulnerabilities........ 6

Logging, Auditing, and Fraud Prevention 7

The Communications Architecture........ **7**

SBC as Security “Master Control Point” **8**

Encryption and Data Protection........ 9

Authentication 9

Logging, Auditing, Compliance, and Fraud Prevention........ 9

Availability 9

APIs for Security Integration........ 10

Next Steps: Action Items for Securing Communications Infrastructure........10

Executive Summary

When it comes to securing communications infrastructure, there’s good news and bad news. The good news is that awareness of the need to secure communications infrastructure has skyrocketed over the past few years. Communications security didn’t even crack the top 10 concerns cited by cybersecurity professionals back in 2016. Today it’s among the top six.

The bad news is that granularity is still lacking. Many cybersecurity professionals are unaware of many of the most common vulnerabilities, including the potential for SIP hacking, man-in-the-middle attacks, TLS/SSL vulnerabilities, and the like. And even among those who are aware, these vulnerabilities comprise an unsolved problem: Roughly 70% say they’re “somewhat concerned” or “very concerned” about them.

The solution? Cybersecurity professionals should start by implementing a focus on communications security. That means putting in place a budget, staffing, and an architecture and roadmap for addressing known and future vulnerabilities.

Beyond that, they should require security as a key selection criterion when choosing communications products. Key features include the ability to deliver on key functions including encryption, authentication, logging, auditing, and high availability. It’s also important that prospective solutions be extensible and able to integrate with other products via APIs.

Communications Security: The Missing Link

Over the past few years, the risk of cybersecurity vulnerabilities in communications infrastructure has begun to percolate into the minds of information security professionals.

In Nemertes' 2018 Cybersecurity Research Study, nearly 60% of participants said that securing Unified Communications and Collaboration (UCC) is a "high" or "critical" priority—making it one of the most prominent concerns for information security.

Top Concerns of Information Security Professionals

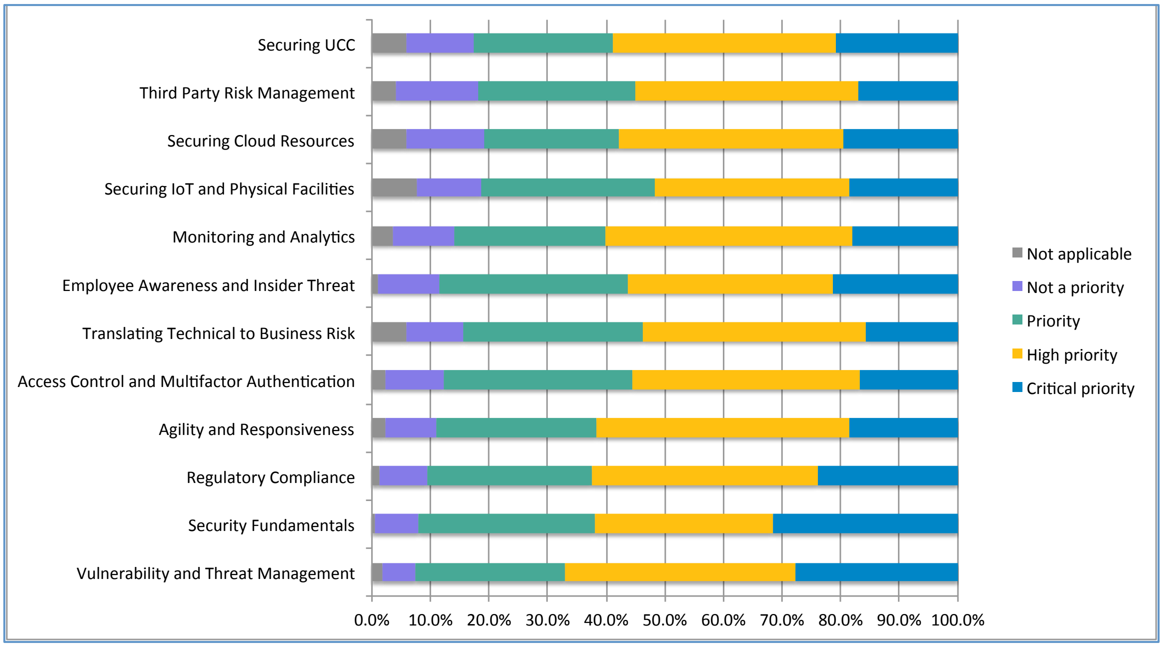

Figure 1: Top Security Priorities (Infosec Professionals)

Keeping in mind that we surveyed and interviewed security professionals (as opposed to communications specialists) for this study, this is welcomed news. It means concern about communications security has ratcheted up considerably since we last addressed the issue, in our 2016/2017 research study.

Back then, communications security literally didn't make the cybersecurity "top 10" list: out of the top 10 security concerns cited by information security professionals, communications security didn't even appear. Clearly, awareness has progressed over the past couple of years.

That said, cybersecurity professionals are still not fully up to speed with communications vulnerabilities. As part of the 2018 study, we asked about specific vulnerabilities. Most participants reported they were "somewhat" or "very" concerned about the specific vulnerability.

In many cases, though, the cybersecurity professional wasn't even aware of the vulnerabilities. During one interview with the CISO of a large financial services firm, we asked, "How worried are you about the following vulnerabilities…?" The response was, "Well, I wasn't be*fore* this call, but I sure am now!"

Common Vulnerabilities

One common vulnerability, for instance, is the potential for hacking the SIP session. Contrary to popular belief, SIP sessions can be hacked. This isn't hard; it can be done with freeware readily available over the internet. And hackers can exfiltrate data, particularly via the Real-Time Transport Protocol (RTP).

SIP Hacking (Data Exfiltration via RTP)

Data exfiltration refers to the unauthorized removal of data from a computer or network. One sneaky way hackers do this is via a covert channel, that is, using tunnels. Because the exfiltrated data is within a tunnel, the attack is difficult to detect. And RTP (along with ICMP, DNS, and HTTP) creates tunnels that can be hijacked by hackers.

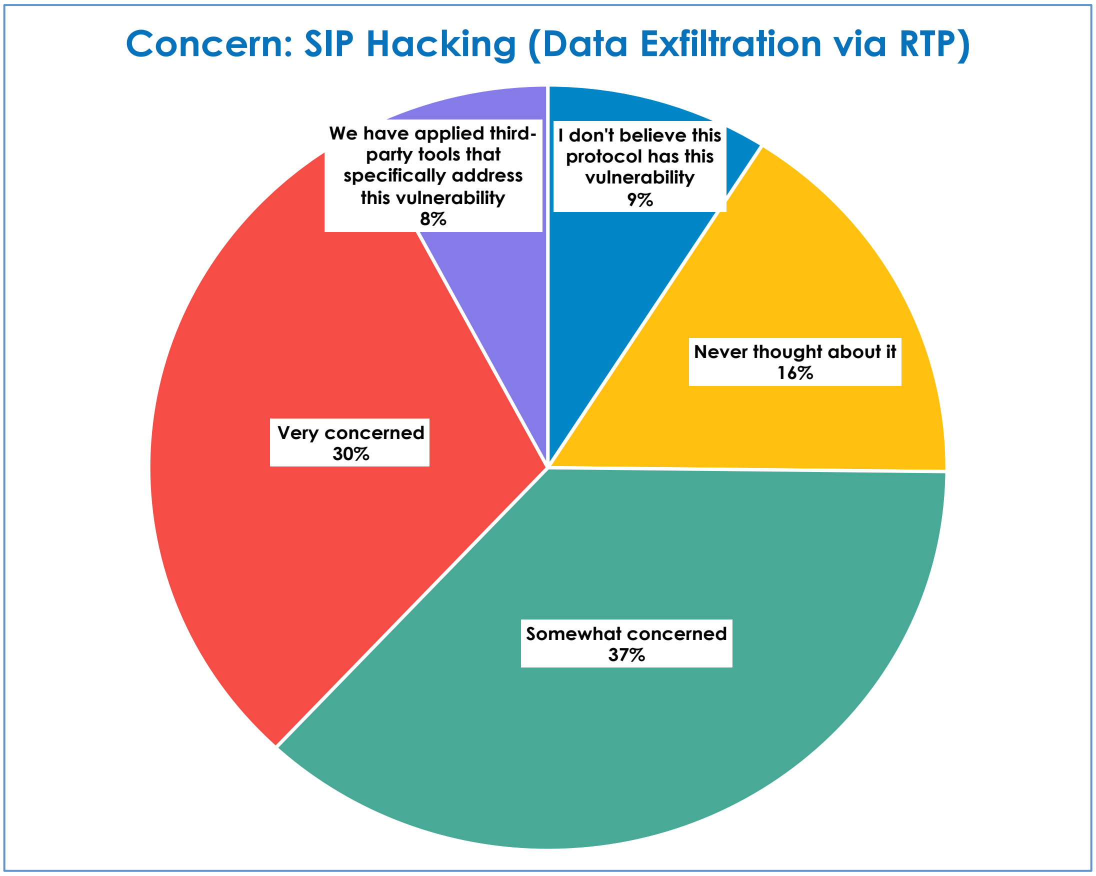

Figure 2: Concerns About SIP Hacking (RTP Data Exfiltration)

Yet 16% of the 2018 research participants "never thought about" the possibility of SIP hacking via RTP. (And remember, participants comprised cybersecurity professionals—the folks paid to think about such things!). The encouraging news is that 67% of participants are "somewhat" or "very" concerned about the potential for SIP hacking.

SIP Interception: MTM

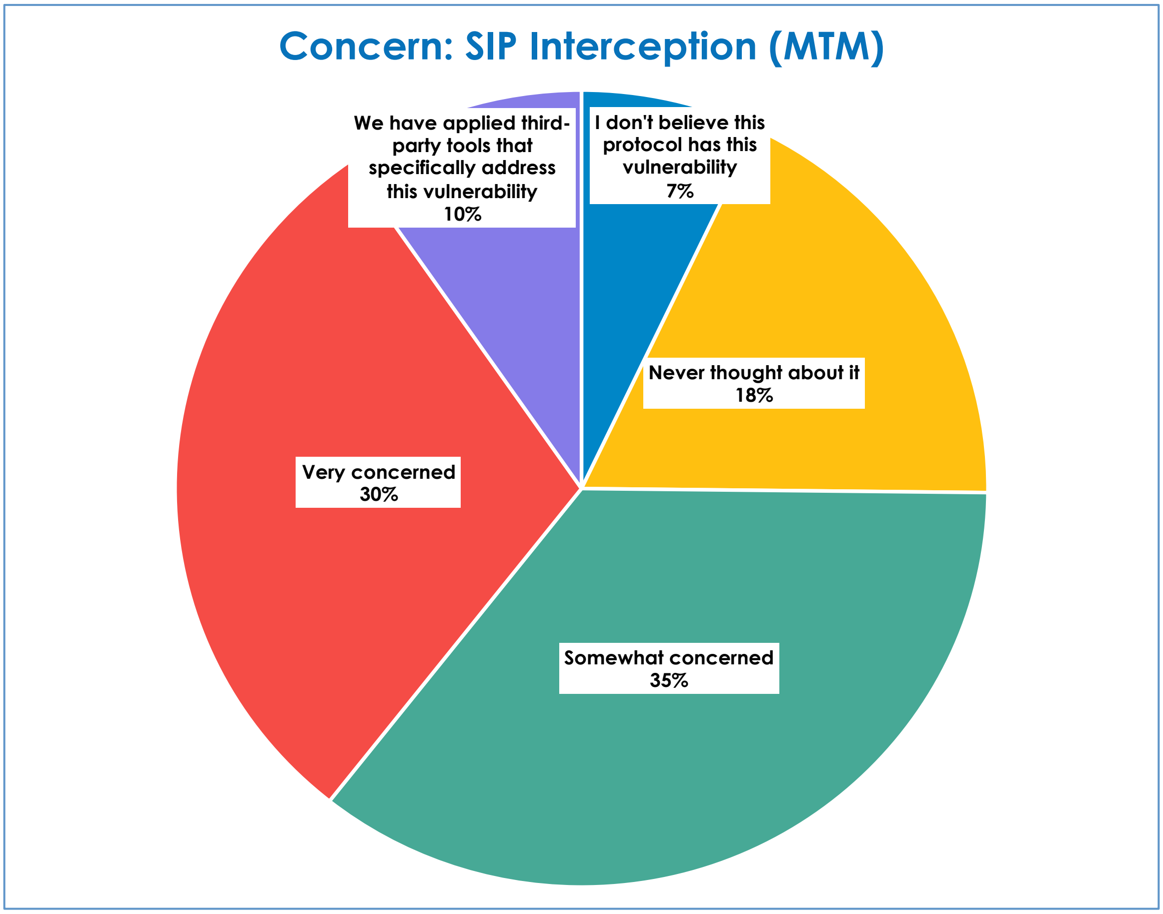

Figure 3: Concern About SIP Interception (Man-in-the-Middle Attacks)

Similarly, 18% of participants "never thought" about the possibility of Man-in-the-Middle (MTM) attacks of SIP sessions. As the name implies, MTM attacks are those in which an imposter pretends to the session source to be the session destination, and to the destination to be the source. Once again, though, 65% are "somewhat" or "very" concerned about the possibility of man-in-the-middle SIP interception attacks.

Other Vulnerabilities

Similar statistics apply to a range of other potential vulnerabilities. Roughly 70% of participants are "somewhat" or "very" concerned about the following, while 10%-20% have not even thought about them:

- TLS/SSL vulnerabilities in UCC suites
- Lack of encryption
- Data Loss Protection (DLP)
- Lack of authentication or authorization

Logging, Auditing, and Fraud Prevention

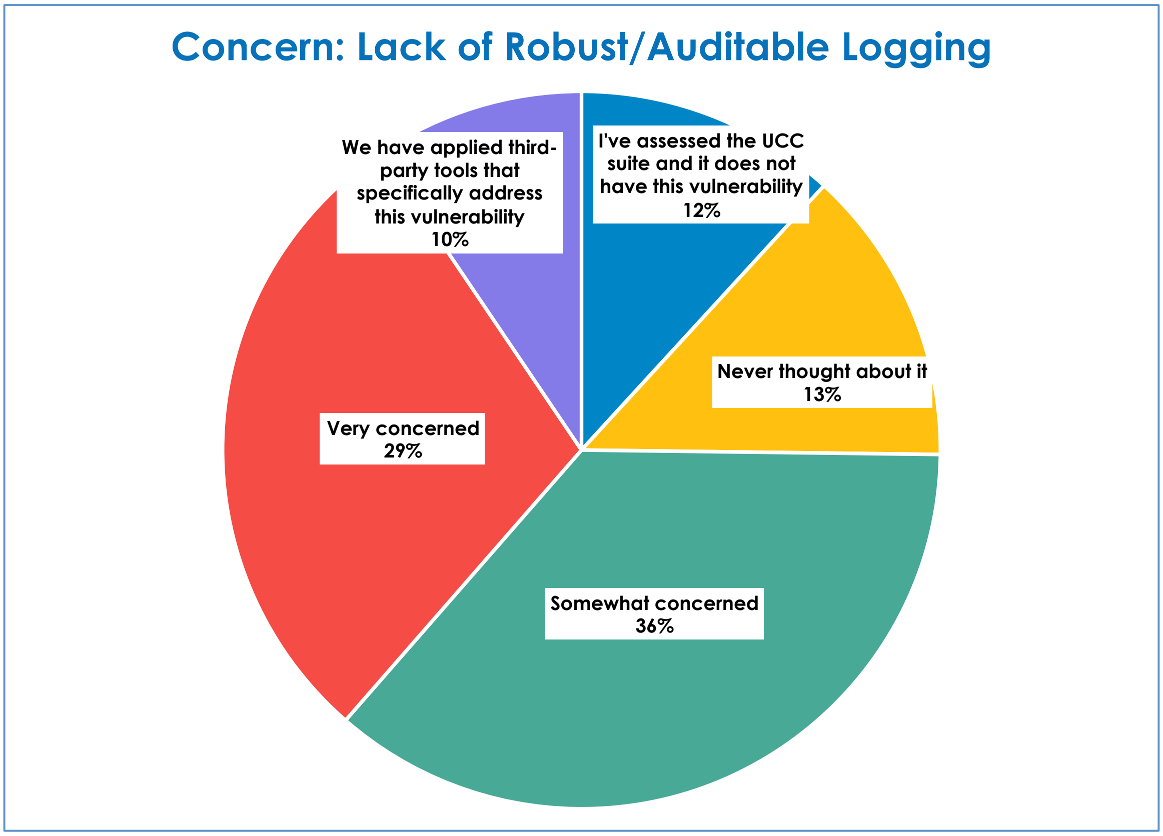

Figure 4: Concern About Robust and Auditable Logging

Finally, similar statistics apply to concerns about the lack of robust and auditable logging. This is particularly critical, as effective logging is essential in protecting against fraud. The fact that most security professionals consider this an unsolved problem indicates how critical it is to focus on this area.

The Communications Architecture

Where should a cybersecurity professional start when it comes to addressing these vulnerabilities? A good place is with a clear understanding of what “communications infrastructure” actually is. It isn’t a single technology; rather it encompasses a suite of technologies and applications including IP telephony, video, UC applications, and other communications applications. These technologies are integrated via presence federation and delivered over a range of APIs and other interfaces. WebRTC delivers voice and video to these interfaces for endpoints on the enterprise or to remote or internet-connected devices.

The interface between the UC platform and the outside world—whether the PSTN or public or private Internet—is the Session Border Controller (SBC), which provides interoperability, security, and management for SIP sessions that cross network borders, including connections between trusted and untrusted networks. Some SBCs also provide a gateway for WebRTC endpoints.

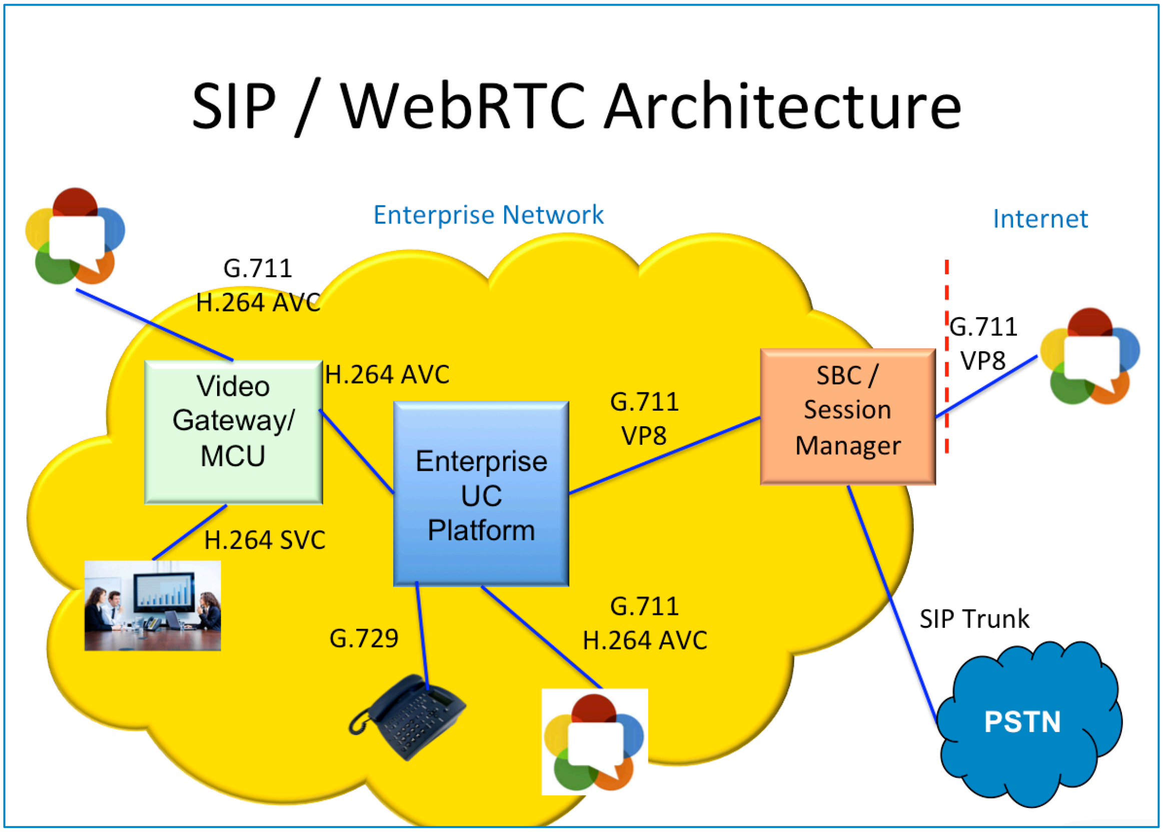

Figure 5: SIP/WebRTC Architecture

SBC as Security "Master Control Point"

The SBC is a logical point to apply security policies, as well as any security mechanisms (such as encryption). Yet most security architectures don't even address the SBC. As with any architecture, protecting communications architecture requires embedding security in multiple ways and at multiple layers. But in a very real sense, the SBC provides a logical "master control point" for security services such as encryption, authentication, and real-time firewalling. The SBC also provides a logical control point for implementing services such as Distributed Denial of Service (DDOS) protection.

So the first place any security professional should start when assessing a communications environment is to check how solid the SBC's security capabilities are. Does the SBC support both wire-speed hardware based encryption and more traditionally at the packet layer? Does it handle certificate authentication? Does it offer real-time firewalling capabilities suitable for voice and video (which require very low latency)? And what mechanisms does it support for DDOS protection?

That said, security can and should be implemented across the communications architecture. To see where and how, it makes sense to drill down into different aspects of security.

Encryption and Data Protection

Protecting real-time data communications (voice, video, presence, IM, multimedia, etc.) from unauthorized wiretapping is as essential as protecting text. But there are multiple mechanisms and locations to provide this encryption. Which is most effective depends on the type of data the enterprise is looking to protect.

A logical point is the SBC, which, as noted, resides at the interface between the enterprise and the outside world. Ideally, the SBC will include a wire-speed, hardware encryption option so all real-time traffic is protected. This approach will work for protecting traditional video, audio, and conferencing services.

But what about applications like email, messaging and multimedia traffic? Here, IP encryption mechanisms such as Secure Socket Layer (SSL), Transport Layer Security (TLS), and SMIME make sense. This security can be embedded either in the UC suite, or in the WebRTC session controller.

Authentication

It's also critical to ensure secure authentication to communications systems. This means applications such as UC, telephony, messaging, and video should support secure authentication for users. The SBC should be able to perform challenge-response and client-certificate authentication.

Logging, Auditing, Compliance, and Fraud Prevention

As noted above, fraud prevention is increasingly critical for communications infrastructure, as is compliance. Effective logging and auditing is the cornerstone of both compliance and fraud prevention. Many times, regulations require the recording of all phone calls for transparency and auditing purposes. And accurate logs are essential when it comes to detecting potential fraud. The capabilities required for both compliance and fraud detection and prevention therefore include embedded voice-recording capability and the ability to archive, index, and search all messages (including voice recordings).

Availability

In this day and age, if enterprise landline voice services disappear, users are perfectly comfortable picking up their cell phones as a backup. So the notion of protection from attacks like DDOS may seem nonsensical; except that certain voice applications are so high-value that taking them down can stop a company's business in its tracks.

A case in point? Contact centers. Particularly in regulated industries, there's simply no easy way to recover if your contact center becomes unavailable. Therefore, when you're assessing SBCs, it's important not just to look for their intrinsic reliability, but also their capabilities at resisting threats like DDOS.

APIs for Security Integration

As with any other security architecture, the security architecture for a communications environment should feature easy integration with an ecosystem of security products and services. Look for solutions that come pre-integrated with standard anti-malware, and include industry-standard protocols and APIs such as Java Messaging Service (JMS), CalDAV, and the like for integration into external security systems.

Next Steps: Action Items for Securing Communications Infrastructure

You can't fix something until you focus on it. Therefore, it's critical for organizations to address communications cybersecurity explicitly, by having:

- A line item in the cybersecurity budget for communications security
- Staffers focused on communications cybersecurity
- A strategy and roadmap for securing communications infrastructure

Moreover, it's important to factor in security when selecting and designing systems. Think in terms of using the SBC as the "anchor device" for protecting real-time services. Make sure it has the suite of security services that you require to protect your infrastructure, including logging, auditing, and network monitoring for cybersecurity violations. To be truly effective it should incorporate real-time feedback mechanism for constantly improving the SBC's security policies. Finally, make sure your solution integrates well into your existing ecosystem of security solutions via the appropriate APIs.