DARKReading RESEARCH

JULY 2020

THE STATE OF

Enterprise Unified Communications & Contact Center Security

ORACLE Communications

EXECUTIVE SUMMARY

The rise in real-time communications technology such as unified communications and contact center applications has helped enterprises interact internally and with customers more efficiently and affordably than ever before. However, organizations are still struggling to strengthen and tailor appropriate security measures to real-time communications. Data from Dark Reading's *State of Enterprise Unified Communications & Contact Center Security* survey indicates they don't take real-time communications security as seriously as other applications, which leaves them unequipped to handle the latest barrage of threats targeting their communications infrastructure.

The survey, which recently queried IT practitioners and other decision-makers about the security risks they face in this arena, shows:

Real-time communications cyber-risks are on the rise:

- **25% of organizations** say the threats hitting their communications infrastructure create more than 20 security incidents per year.
- **37% of organizations** say at least one in 10 calls to their contact centers is potentially fraudulent.

Organizations must support a range of real-time communications applications:

- **35% of organizations** primarily support on-premises third-party vendor solutions.
- **24% primarily support** software-as-a-service-based third-party vendor solutions.
- **23% rely on** an outsourced managed service.
- **18% primarily support** legacy voice/PBX.

Automated attacks are prevalent:

- **Robocalls and phishing** are the top two threats to real-time communications applications.

Existing security tools and practices aren't strong enough to meet communications threats:

- **39% of organizations either** don't know what kind of communications security management system they use, admit they don't have one, or depend on a system that requires manual intervention to work.
- **41% of organizations** depend on legacy static rules-based technology or simple decision engines to search for malicious callers or fraudulent behavior.
- **Contact centers have** inadequate means of identifying callers — their No. 1 method of verifying callers is a password, cited by 53%.

Enterprises need stronger security, and users want better experiences:

- **20% of users** would like more stringent authentication security, while 44% would like an easier/quicker user experience.

Threats against unified communications and contact centers are materially impacting enterprises and, at many organizations, are on a noticeable uptick.

In order to respond to threats and support advances in real-time communications, organizations will want to invest in a fully integrated solution that can help them tie together monitoring, analysis of threats, and enforcement of security policies. Ideally, such a solution will provide end-to-end, 360-degree visibility of their entire communications infrastructure, real-time analysis of the traffic and automated caller verification, as well as control and enforcement of policies that can be customized to an organization's needs and risk tolerances.

The Rising Tide of Real-Time Communication Cyber-Risks

As real-time communications grows as an increasingly important component of enterprise business today, it's only logical that the potential for cyber-risk mirrors what's going on in the broader IT environment. Attacks are rising as cybercriminals seek to use real-time communications as yet another avenue for committing fraud.

This survey shows threats against unified communications and contact centers are materially impacting enterprises and, at many organizations, are on a noticeable uptick. Forty-one percent of organizations must contend with more than five communications-based security incidents per year, according to the research. For one in four organizations, the number of incidents exceeds 20 per year (**Figure 1**).

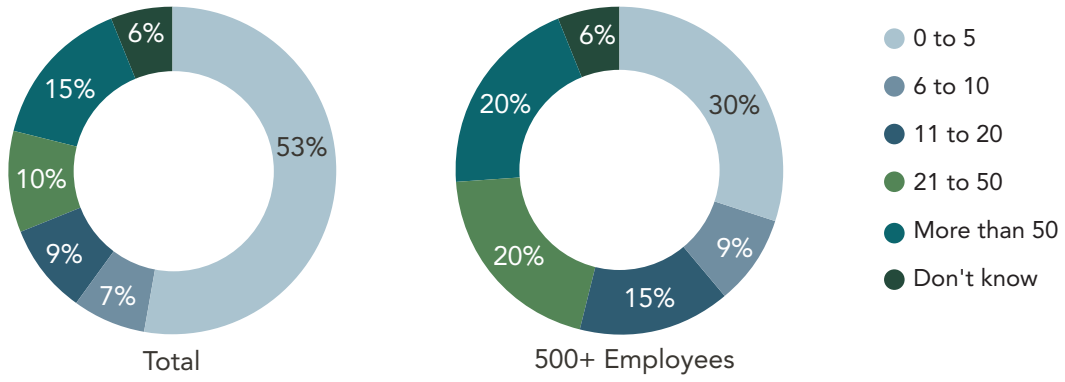
What's more, the incident pressure isn't close to letting up. In the past 12 months, 72% of organizations reported the trend of security incidents on their communication networks either stayed the same or increased (**Figure 2**).

These incidents tend to affect larger organizations and those with higher call volumes disproportionately. For

Figure 1

COMMUNICATIONS-BASED SECURITY INCIDENTS

How many communications-based security incidents did your company handle over the past 12 months?



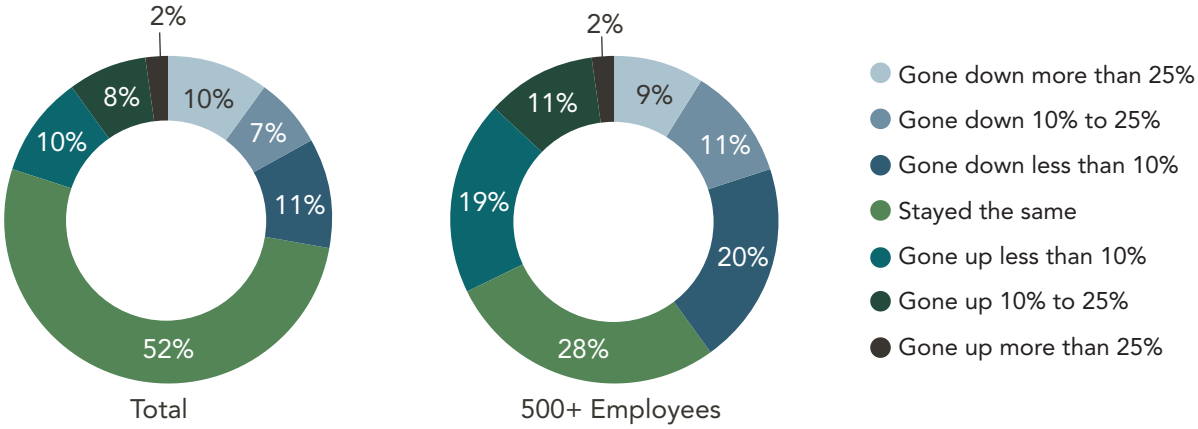
Base: 136 total respondents; 74 respondents at companies with 500 or more employees

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

Figure 2

CHANGE IN SECURITY INCIDENTS

How has the trend of security incidents on your communications network changed over the past 12 months?



Base: 136 total respondents; 74 respondents at companies with 500 or more employees

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

example, 41% of organizations supporting more than 100 concurrent SIP sessions say they also handle more than 20 communications-based security incidents annually. In addition, larger organizations are seeing bigger increases in incident loads: Thirty-two percent of enterprises supporting 500 or more employees note an increase in communications security incidents compared with 20% of the entire respondent base.

These incidents are driven by criminals armed with readily available tools that make it trivial to spoof phone numbers, IP addresses, and caller IDs. Many of these tools are so prevalent they can be found on the Apple App Store or Google Play platforms. More sophisticated tools found online and on the Dark Web help the bad actors carry their scams further with capabilities to synthesize someone's voice, carry out telephony denial-of-service (TDoS) attacks, harass employees with automated robocalls, and even gain a foothold inside an enterprise network to hijack it or steal communications services.

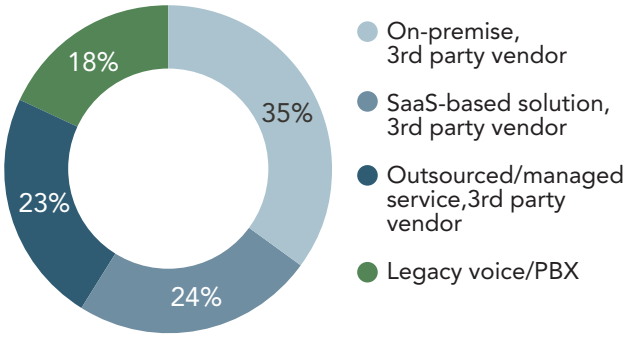
As we'll explain, the study suggests that many organizations are not yet well-equipped to rebuff these attacks. They still depend on static rules-based security solutions that require a lot of manual effort to maintain and are ill-suited to defend against the latest cybercriminal tools and techniques.

At the end of the day, this discrepancy in how organizations respond to communications-based security incidents increases operational risks and could cost them millions of dollars in the process. According to recent insurance industry figures, the average large firm loses $385,000 for every security incident it experiences.For organizations hit by 20

Figure 3

PRIMARY TYPE OF UC&C SOLUTION

What is the primary type of UC&C solution that you support?



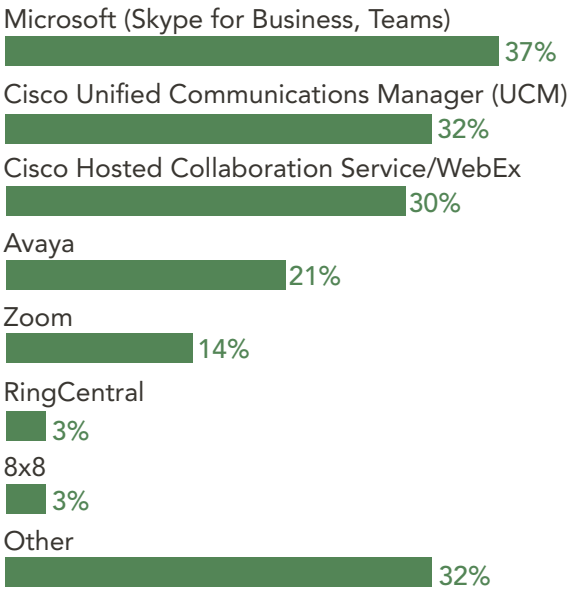
Base: 120 respondents with knowledge of their organization's contact center solution

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

Figure 4

UC&C THIRD-PARTY VENDORS

Who are your UC&C 3rd party vendors?



Base: 120 respondents with knowledge of their organization's contact center solution

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

real-time communications security incidents, that could add up to $7.7 million annually.

Industrywide, the costs are adding up significantly. Recent studies estimate that telephony fraud costs enterprises $31 billion per year.

What's at Risk

The State of Enterprise Unified Communications & Contact Center Security survey results show that organizations are tasked to secure a broad range of real-time communications technologies, platforms, and communications channels.

Less than 20% of organizations say they still depend on legacy voice or PBX as their primary type of real-time communications technology. Instead, the business world now seems to depend on a mix of solutions offered by third-party vendors, including on-premises unified communications technology, unified communications as a service (UCaaS) or contact center as a service (CCaaS) technology, and outsourced or managed service communications (**Figure 3**).

When asked about the third-party vendors they do business with, respondents could choose as many as applied. The distribution across numerous vendors indicates many organizations take a heterogenous approach. Some of the most common deployments include solutions from Microsoft, Cisco, Avaya, and Zoom (**Figure 4**).

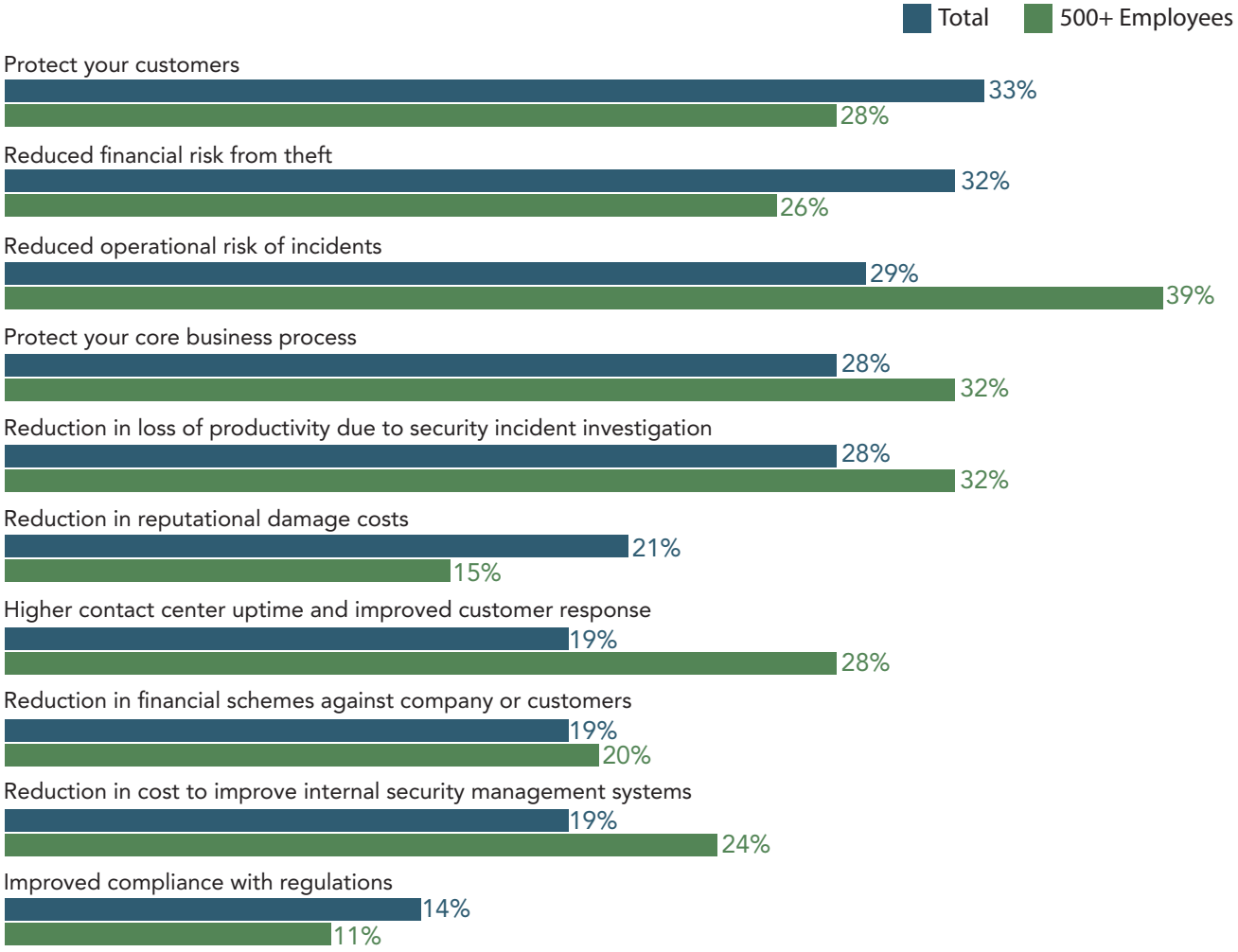
These real-time communications technologies are supporting a variety of traffic types though voice still dominates. On average, approximately 69% of respondents' SIP-based traffic comes from voice calls, another 21% supports multimedia capabilities, and 13% run automated chatbots.

Volume-wise, many organizations are handling a significant amount of traffic. Nearly half of organizations support more than 50,000 SIP-based voice calls per month, according to the survey, with 11% supporting more than 1 million calls monthly. Among the respondents, 62% say they're capable of supporting more than 100 concurrent calls.

Figure 5

BUSINESS BENEFITS OF PREVENTING COMMUNICATIONS SECURITY INCIDENTS

What business benefits will your company gain by better preventing communications-based security incidents?



Note: Maximum of three responses allowed
Base: 136 total respondents; 74 respondents at companies with 500 or more employees
Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

The stakes are high. Real-time communications provides the means to communicate and transact with customers at the contact center level and is the conduit through which collaboration and core business processes are carried out within the organization. As such, the survey shows the biggest reasons respondents would want to improve their communications-based security protections revolve around protecting the customer, reducing financial risk from theft, and reducing the operational risks of incidents (**Figure 5**).

The prioritization for reaping benefits and reducing risks through improved

No matter the specific threat mix for any given organization, the end result is IT teams are being stretched thin by the resulting problems.

real-time communications security protections shifts slightly for larger organizations. At that point, the emphasis is weighted more heavily toward mitigating operational risk, as well as maintaining productivity and contact center uptime. Nevertheless, protection of core business processes and customers and minimizing fraud remain decidedly on the radar as desired communication security benefits.

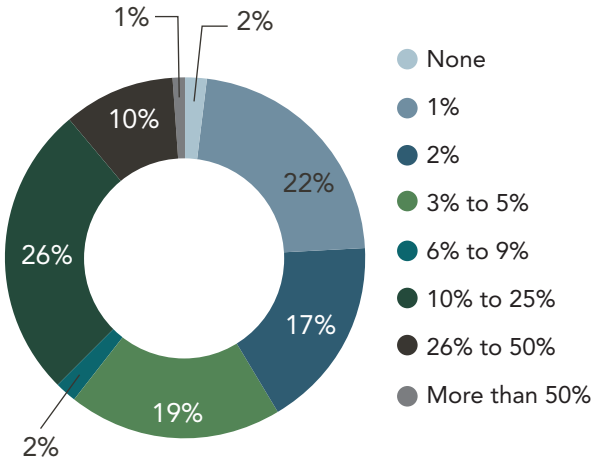
Biggest Cyber Threats To Real-Time Communications

The growing volume of communications-related security incidents has turned the screws on IT teams to find ways to reduce risks and protect their systems and users from threats. As previously mentioned, approximately one in three organizations today handle 10 or more incidents per year. In the call center, 37% of organizations say at least one in 10 calls are potentially fraudulent (**Figure 6**).

Figure 6

POTENTIAL FRAUDULENT CALLS

What percent of your inbound contact center calls are potential fraud calls?



Base: 120 respondents with knowledge of their organization's contact center solution

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

The study shows a variety of security incidents are top-of-mind for respondents. The survey asked about both the most common incidents and the major ones that are emerging. The order of highest ranked attacks is the same:

1. Robocalling
2. Phishing
3. Account takeover
4. Abuse of network or service

Similarly, for both current and emerging threats, the most mentioned breaches were:

1. Spoofing caller identities and impersonation (other than spoofing)
2. Network-device hacking (e.g., IP-PBX, voicemail)

Considering that spoofing and impersonation are key methods used in robocalling, phishing, and account takeover, this is no surprise. Network-device hacking, such as toll fraud, traffic pumping, and callback schemes, is instrumental in the abuse of networks and services (**Figure 7**).

No matter the specific threat mix for any given organization, the end result is IT teams are being stretched thin by the resulting problems. The study shows that most organizations only have a few full-time staffers working on communications security management activity, with 43% of respondents saying they have zero to two full-time employees fulfilling those obligations. And yet those people often spend a significant amount of their workweeks reactively putting out fires in

FIGURE 7

MAJOR EMERGING COMMUNICATIONS-BASED SECURITY INCIDENTS

What communications-based security incidents have been the major emerging ones over the past 12 months?

	Overall Rank	Weighted Score
Robocalls/Nuisance calls	1	200
Phishing/Pharming	2	196
Spoofing (IP or CLI/ ANI)	3	83
Voicemail hacking	4	67
IP PBX hacking	5	64
Impersonation (other than spoofing)	6	63
Account takeover	7	54
Abuse of network, device, or configuration weakness	8	54
Callback scheme	9	49
Traffic pumping to toll-free numbers	10	44
Artificially inflated traffic	11	37
Harassment (via telephony denial-of-service attack)	12	24
Extortion (via telephony denial-of-service attack)	13	9

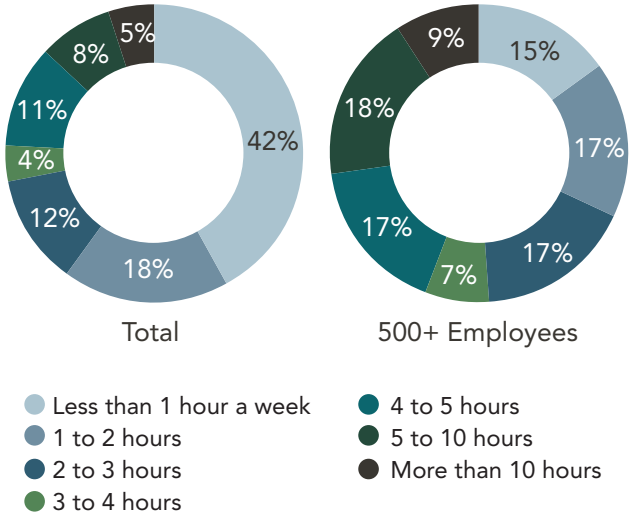
Note: Rank is based on a weighted score. Items ranked first are valued higher than subsequent items, and the score is based on the sum of all weighted counts.

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

Figure 8

TIME SPENT ON COMMUNICATIONS SECURITY INCIDENTS

How many hours per week on average does your company spend on communications security incidents, including investigations?



Base: 136 total respondents; 74 respondents at companies with 500 or more employees

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

response to security incidents. Some 24% of all organizations and 44% of large organizations (those with 500 or more employees) say they spend more than four hours a week dealing with communications security incidents (**Figure 8**).

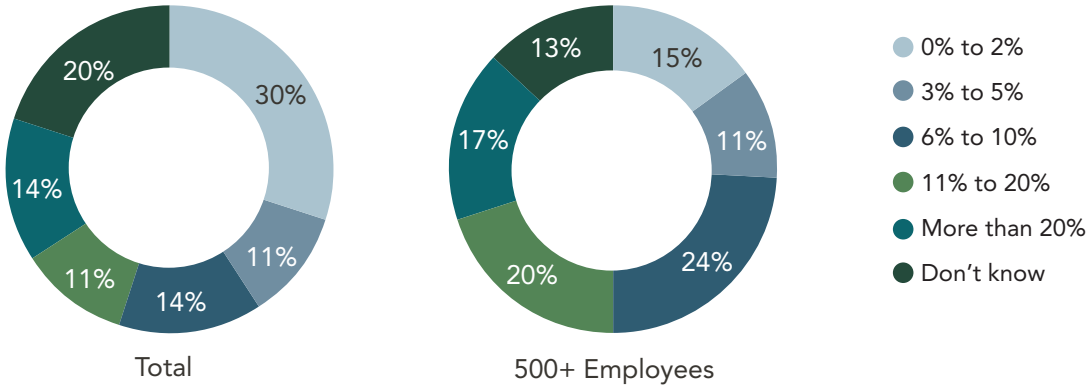
To make matters worse, many of the real-time communications security incidents flagged by legacy systems prove to be nonexistent due to very high false-positive rates from these systems. This only further exacerbates the problems stemming from overworked IT and cybersecurity staff. At larger organizations (500 or more employees), 37% of organizations say more than one of every 10 communications security investigations end up being a false positive (**Figure 9**).

The threat volume and high workload may actually be distorting organizations' perceptions of the risks. The survey shows toll fraud and TDoS attacks appear to be of less concern to respondents than the other threats mentioned. But the challenges in communications security tooling that

Figure 9

FALSE-POSITIVE COMMUNICATIONS SECURITY INCIDENTS

What percentage of your communications security incidents are false positives?



Base: 136 total respondents; 74 respondents at companies with 500 or more employees

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

Too many enterprises attempt to apply standard application security measures to real-time communications technologies such as unified communications and contact center applications.

we'll dive into in a moment and the high false-positive rate may actually indicate that organizations are not yet aware of the true levels of exposure they're subject to.

Challenges in Securing Unified Communications and Contact Center Technology

Security managers and architects generally understand standard web applications but not all of the nuances of real-time communications, whereas real-time communications managers and architects often lack sophisticated security knowledge. As a result, too many enterprises attempt to apply standard application security measures to real-time communications technologies such as unified communications and contact center applications. The study shows some 38% of organizations either don't know what kind of communications security management system they use, they admit they don't have one, or they depend on a system that requires manual management, such as maintaining lists, and intervention to work (**Figure 10**).

This means the only cybersecurity backstop for these organizations' real-time security communications technology is what the IT security has in place for the network at large. According to the survey, the top forms of general cybersecurity detection and mitigation capabilities tend to be firewalls, intrusion detection and prevention systems, and next-generation firewalls.

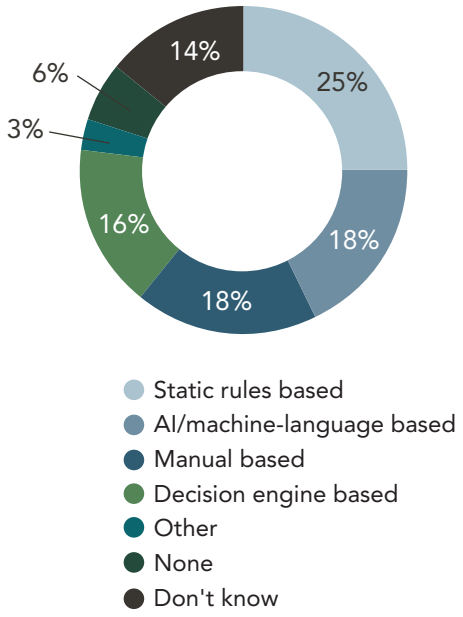
This limits user flexibility and still leaves enterprises exposed to complex security challenges. Unlike standard web-based applications that are transaction-based, real-time communications involve interactions that are stateful and session-based.

Conventional IP security products like the ones above were not designed with these kinds of real-time communications in mind

Figure 10

TYPE OF COMMUNICATIONS SECURITY MANAGEMENT SYSTEM

What type of communications security management system do you currently use?



Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

— leaving organizations vulnerable to threats specific to such communications.

Meanwhile, even when organizations do put in systems tailored to managing real-time communications security, they often rely on legacy technology that has not evolved at the same pace as attack tools.

For example, according to the study, 41% of organizations depend on static rules-based technology or simple decision engines to search for malicious callers or fraudulent behavior. Among the current top five measures that organizations take to prevent communications-based security breaches, four rely on a defined set of activities, alerts, and signature-based detection:

- SIP firewall and session border controller
- Traffic management
- Calling-number verification, which verifies caller ID through techniques such as automatic number information check, porting status and history, and harassment blacklist lookup
- Caller identity verification, which includes verification techniques such as passwords and knowledge-based authenticators (**Figure 11**)

The defined rulesets that power these methods require constant tuning in order to allow legitimate transactions while preventing evolving threats. This requires qualified security analysts to commit hours to query the system, sort and filter the data, confirm their suspicions, and identify the nature of the threat.

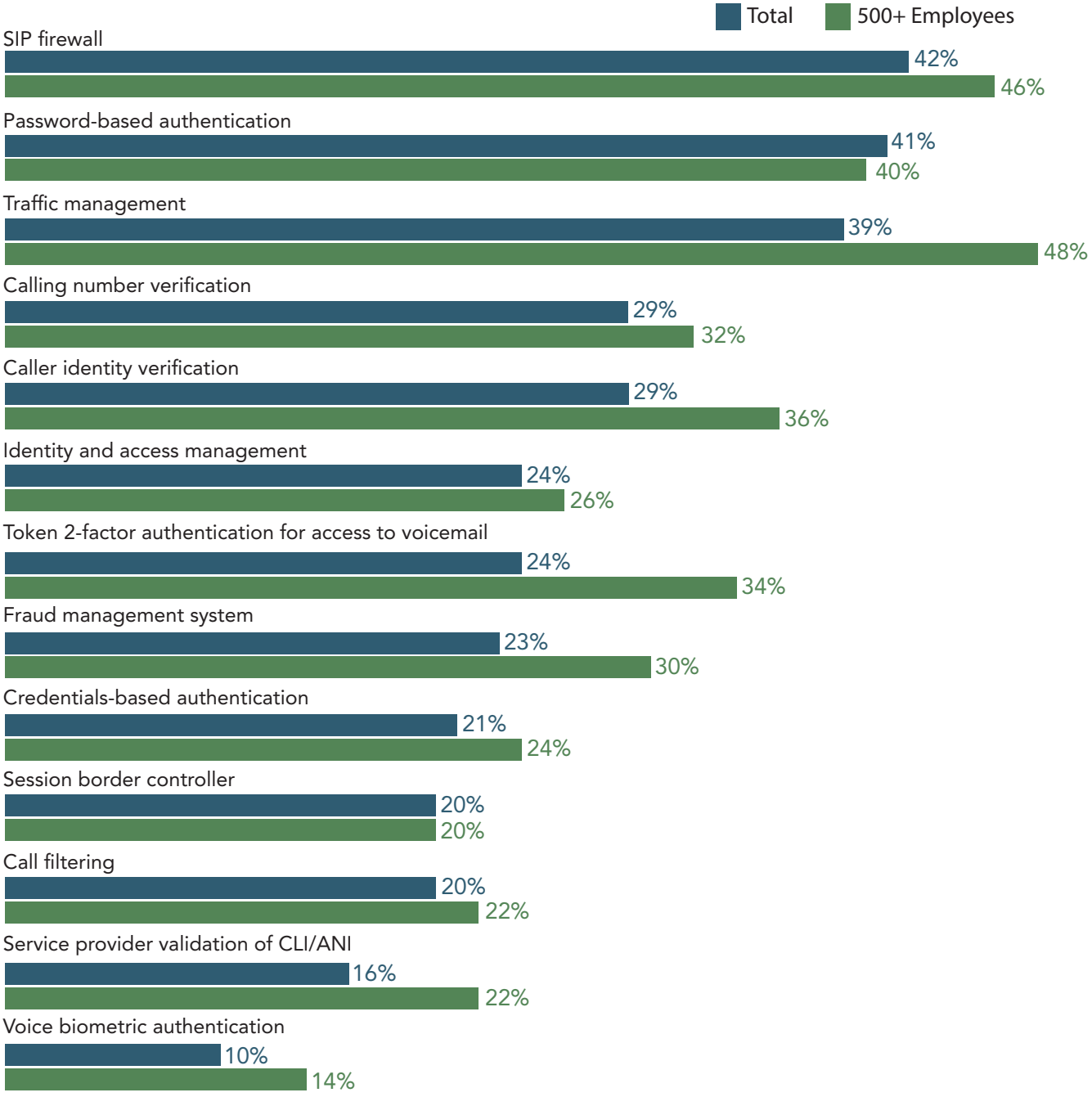
For the most part, these tools are primarily focused on on-premises-based communications infrastructure. The security state for cloud-based infrastructure like UCaaS and CCaaS is likely even more precarious. According to the *Oracle and KPMG Cloud Threat Report 2020*, cloud services and applications are consumed by business units outside the scope of centralized IT and security teams. As security pros try to help secure these assets, their efforts are often perceived as slowing down the business.

When this dynamic plays out with UCaaS/CCaaS, the security problems for communications infrastructure are exacerbated by the cloud's shared responsibility model. In the cloud, the

Figure 11

PREVENTING COMMUNICATIONS-BASED SECURITY BREACHES

What capabilities are your UC&C using today to prevent communications-based security breaches?



Note: Multiple responses allowed

Base: 136 total respondents; 74 respondents at companies with 500 or more employees

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

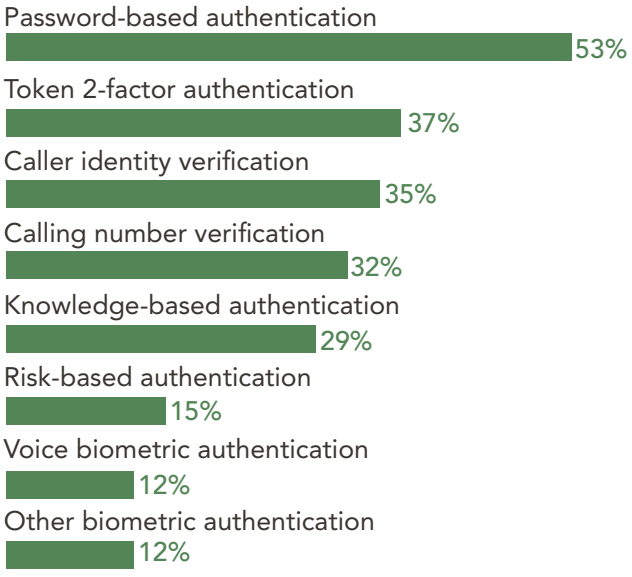
responsibility for security is shared between the enterprise and the cloud provider, and the degree of responsibility required by enterprises varies across cloud providers. For example, when one thinks of security management for Zoom, it's well-understood that it was built for enterprises with well-established and functioning security teams.

In addition to static rules-based security technology, many organizations are also relying on simplistic means of verifying users are who they claim to be. The No. 2 means of securing real-time communications — password-based authentication — is one of the easiest-to-game measures in the security world. Password-based authentication exposes a weakness felt particularly acutely in the contact center, which, as explained before, is constantly barraged with fraudulent impersonation attempts.

Figure 12

AUTHENTICATION CAPABILITIES TO PREVENT COMMUNICATIONS-BASED BREACHES

What authentication capabilities are your contact center using today to prevent communications-based security breaches?



Note: Multiple responses allowed

Base: 120 respondents with knowledge of their organization's contact center solution

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

In the call center, more than half of surveyed organizations cite passwords as the leading way to authenticate users. In contrast, only 15% of organizations utilize more sophisticated risk-based authentication (**Figure 12**). Many organizations also depend on simplistic authenticators, such as knowledge-based authentication (KBA), and simplistic verification of the calling number, using methods like automatic number identification (ANI). Like passwords, KBA such as PIN and voice authenticators are becoming obsolete as reliable verification methods. Attackers can use PIN generators to guess them, and KBA is prone to circumvention by social engineering, phishing, and stolen account information stored on the Dark Web by attackers who have perpetrated data breaches elsewhere. In addition, passwords and KBA do nothing against synthesized and fake identities used in onboarding users. And due to advances in caller ID spoofing, caller ID verification techniques such as ANI checks, porting status, and history are rendered obsolete as reliable verification methods.

The good news is that many organizations are recognizing multifactor authentication and enhanced caller verification as major steps forward to providing a reliable backstop to KBA, passwords, and other simple verifiers, the survey shows (**Figure 13**). However, the number of organizations using more complex identity verification is still in the minority, so it's clear to see much work remains ahead.

FIGURE 13

PRIME AUTHENTICATION CAPABILITIES FOR BETTER BREACH PREVENTION

What are the prime authentication capabilities you are looking at today to enable your contact center to better prevent communications-based security breaches?

	Overall Rank	Weighted Score
Token 2-factor authentication	1	112
Calling number verification	2	78
Caller Identity verification	3	70
Password-based authentication	4	63
Knowledge-based authentication	5	29
Voice biometric authentication	6	28
Other biometric authentication	7	16
Risk-based authentication	8	15

Note: Note: Maximum of three ranked responses allowed. Rank is based on a weighted score. Items ranked first are valued higher than subsequent items, and the score is based on the sum of all weighted counts.

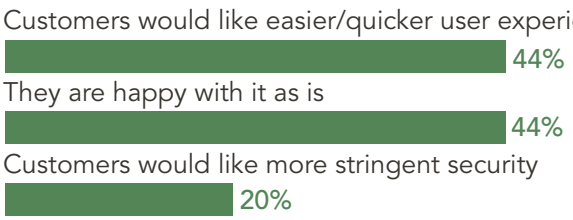
Base: 120 respondents with knowledge of their organization's Contact Center solution

Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

Figure 14

CUSTOMER SATISFACTION WITH AUTHENTICATION PROCEDURE

How satisfied do you believe your customers are with your authentication procedure?



Data: Informa Tech survey of 136 IT professionals involved in the purchase of communications technologies, March 2020

Enterprises must craft new strategies and identify new security solutions to protect and control real-time communications flows — without hurting user experience or business productivity in the process.

When used individually or a few at a time, the criminal element usually finds it trivial to work around authentication methods. Online tools make it simple enough to spoof numbers, caller ID, IP addresses, and even someone's voice. Additionally, sophisticated criminals will use many different calls to gather information before they are in a position to steal the information or services they are targeting. It is challenging for contact center agents to determine a malicious behavior versus a legitimate caller trying to accomplish something. Lack of visibility makes it difficult to correlate threats, which allows the bad actors to fly under the radar.

Strengthening Real-Time Communications Security While Maintaining User Experience

Clearly, enterprises must craft new strategies and identify new security solutions to protect and control real-time communications flows — without hurting user experience or business productivity in the process. Regarding how customers perceive current authentication procedures, surveyed companies say they are less likely to be concerned about security and more likely to want to either maintain the status quo with how they are logging in or are interested in an even easier user experience (**Figure 14**).

So even as enterprises employ technology that provides better visibility and detection of malicious behavior and verifies callers based on a flexible matrix of factors, such as caller origination and reputation scoring, the protection mechanism can't introduce additional friction for the user.

Ideally, organizations should be seeking out a real-time communications security management system that can continuously inspect unified communications and contact center traffic and provide a holistic, end-to-end view of the entire environment. The system should be able to authenticate every call upfront and in real time, enforcing higher levels of authentication based on advanced artificial intelligence/machine learning (AI/ML) algorithms and customizable policies. And it should be able to automate threat detection and enforcement actions to take the burden off of security staff and communications platform administrators.

The heart of a truly effective solution will be advanced AI capabilities, which should add behavioral analytics, anomaly detection, and dynamic risk assessment to the process of detecting threats and verifying legitimate callers. With the right technology in place, enterprises can learn behaviors of certain users, such as how they dial into the call center, and have the technology automatically flag or enforce action against suspicious activity based on what the system has previously learned. These kinds of enforcement actions could range from spurring an agent to run an extra level of authentication on a user, to rerouting a call to an agent specially trained in dealing with potential fraud, to the outright blocking of calls. Similarly, a system effectively utilizing AI/ML can drastically cut down on nuisance calls while minimizing false positives.

Recommendations

With real-time communications threats and incidents on the rise, along with organizations being called on to protect a growing range of solutions in their communications application portfolios, it is clear that organizations need to refocus their security strategies. Enterprises are unable to accurately gain visibility into the threats barraging their real-time communications networks, and they are similarly unequipped to consistently verify user identities and authenticate incoming calls. Organizations need to strengthen their communications security posture without sacrificing the user experience. To do so, they need to:

Create a cross-functional team that focuses on real-time communications security:

- Include stakeholders from unified communications, contact center, network, security, and business operations departments.
- Keep in mind that each group has a different lens into the benefits, costs, and risks of associated solutions. Maintaining a balance of great security that respects privacy and minimizes customer friction requires a team effort.

Ensure the enterprise has an end-to-end view of all real-time communications:

- Gather the data from all pertinent platforms, both on-premises and in the cloud.

- Utilize tools to inspect and analyze this information against defined security policies to spot security anomalies and risks.

Invest in a next-generation real-time communications security solution:

- Seek platforms that can use AI/ML analysis methodologies, such as threat signature detection, behavioral analytics, and anomaly detection, to reduce false positives and truly provide end-to-end enterprise communications security monitoring across the enterprise.

- Look for real-time dashboards and historical analytical reporting that can then capture and quantify risk, along with subsequent automated mitigation actions.

- Ensure AI/ML can aid with caller verification and automated enforcement of customized policies.

A modern solution should help enterprises carry out these recommendations through a platform that works in a coordinated fashion to monitor, analyze, and enforce security policies for real-time communications. These solutions should provide:

- 360-degree visibility: This requires intuitive dashboards that provide a business intelligence-driven data visualization of real-time communications traffic, layered with actionable insights to mitigate risks.

- AI/ML-backed user scoring: Organizations should be able to pinpoint fraudulent calls and malicious caller behavior through a mixture of behavioral analytics, threat signature detection, and anomaly detection capabilities.

- Always-on, automated enforcement: The solution should be able to enforce policies based on risk scoring with minimal user intervention.

To learn more about how Oracle Communications Security Shield Cloud can help your organization deliver these capabilities, visit oracle.com/security-shield.

Survey Methodology

Dark Reading conducted an online survey in early 2020 to explore the trends in UC/CC security. The final data set is made up of 136 IT and cybersecurity managers at primarily North American organizations.

More than one-third (37%) of respondents hold high-level IT titles, such as CIO, CTO, or IT director. Over half (55%) work at companies with 500 or more employees, and they hail from a variety of industries such as healthcare, communications, financial services, banking, and government, among others.

Nearly half of respondents (48%) report their company supports more than 5,000 voice only (SIP-based) sessions per month, and 62% say their communications infrastructure can support more than 100 concurrent, active SIP-based voice sessions.

Informa Tech research was responsible for all survey administration, data collection, and data analysis. Informa is the parent company of Dark Reading. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.