



Accelerating Transformation with Security and Operations Collaboration Best Practices

RESEARCH BY:



Chris Kissel
Research Director, Security
& Trust Products, IDC



Stephen Elliot
Program Vice President, Management
Software and DevOps, IDC



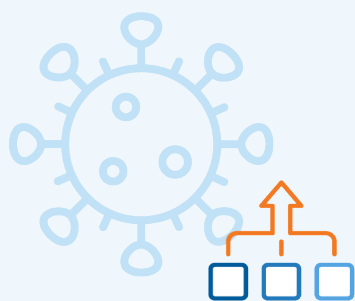
Navigating this InfoBrief

Click on titles or page numbers below to quickly navigate to each.

Executive Summary.....	3	IT Executives Are Investing in Integrated Security and Operations.....	12
Hypothesis.....	4	Best Practices to Accelerate Security and Operations Transformations.....	13
IT and Security Collaboration Is a High Priority to Enable the Delivery of Speed and Agility.....	5	Land and Expand—The Role of the Cybersecurity Solutions Provider in Securing the Transition to Multicloud Environments.....	14
Increasing Complexity Due to Multi and Hybrid Clouds Is Driving Technology Platform Adoption, Process Integration, and Team Collaboration.....	6	IT and Security Discrete and Shared Concerns.....	15
Security and Operational Challenges Are Skyrocketing.....	7	The Transitioning World: COVID-19 Makes You Rethink.....	16
Software Development Cycles Are Accelerating.....	8	Conclusions.....	17
Multicloud Disrupts Traditional Security and Operations, Creating Stress Between IT and Security.....	9	Methodology.....	18
What’s Needed to Meet These Challenges?.....	10	About the Analysts.....	19
Security and Operations Teams Need to Standardize on Better Platforms.....	11	Message from the Sponsor.....	20

Executive Summary

Multiclouds, workloads, and application environments are interrupting the way that security and operations teams need to interact.



Integration

COVID-19 has put siloed infrastructure under a microscope and increased the need for integration between operations and security teams.



Communication

Organizations with teams that communicate regularly rise to meet the challenges of multicloud environments.



Standardization & Collaboration

Standardization and team collaboration are two strategies to reduce and contain costs and complexity across IT and security teams.



Now more than ever, these teams need to align to understand how to combat complex situations and decrease fragmentation.

Hypothesis

Both SolarWinds and IDC believe there has been a call to consolidate IT and cybersecurity tools. SolarWinds made this observation from the types of tools it sells (the SolarWinds® Orion® and SolarWinds® RMM platforms are the best examples, but other solutions cross over as well). IDC believed a consolidation of tools was happening because several use cases called for this: unified compliance, IT workflow, data normalization for security and automation, and the hope to make tier one security analysts more effective.

Proving These Points

Survey data:

IDC populated the InfoBrief with existing survey data and conclusions from multiple studies. To build on the story, IDC survey data is concluded. However, often, there is a gap between perception and how tools are used in the field.

Interviews:

The project began with interviews from April–May 2020. This added an obvious level of complexity as all companies had a shared austerity—the onset of COVID-19.

Use cases:



Hospitality



Manufacturing



Finance



Government

An IT ops-specific interview was conducted, and a security ops interview was conducted for each vertical. The combined notes are presented on the following slides.

IT and Security Collaboration Is a High Priority to Enable the Delivery of Speed and Agility



Hospitality (Hotel chain)

A leading concern is the handling of credit cards. The hotel chain has built redundancies based upon Payment Card Industry Data Security Standard (PCI DSS).

- Operations teams are involved in the conversation early and often on process and tool standardization.
- Development teams are slowly adopting Dev/Sec/Ops practices, but adoption is in pockets.
- Common security conversations with development teams include vulnerability and code scanning, security APIs and libraries, and the intersection of network and security tools.
- COVID-19 has accelerated transformations in network security tools, access controls, and virtual desktops and contactless check-in technologies.



Manufacturing (Global food manufacturer)

To facilitate a global supply chain, facilitate partners, and conduct transactions, the organization hosts 6,000 web application URLs and invests heavily in domain name system (DNS) and IP reputation and WHOIS registry monitoring tools.

- Network segmentation is in heavy use, as is virtualization in private clouds.
- Advanced analytics are used to drive faster problem identification and resolution.
- There is growing maturity for the collaboration between security and IT; this involves deployment models and API library development.
- Compliance, audit, and security teams are increasingly sharing best practices and looking for ways to contain costs and optimize processes and workflows.
- The security and IT teams are at different stages of moving from a reactive to a proactive posture, but both teams are headed in the right direction.

Increasing Complexity Due to Multi and Hybrid Clouds Is Driving Technology Platform Adoption, Process Integration, and Team Collaboration



Finance

(Top 20 U.S. banking firm)

The firm is focused on hiring and training employees to understand risk management from the standpoint of technologies or products.

- Configurations are designed to minimize risk.
- Microsegmentation is a big issue.
- Data handling is designed to minimize exposure and micromanagement of data including data loss prevention (DLP), file integrity management (FIM), and policy and compliance enforcement.
- It is investing in planning and tools that allow risk management to be a part of service delivery.
- Risk management is a part of incenting IT and security employees to work together, with common metrics and goals to drive a single outcome.
- The firm is aiming for a blameless culture, wants to limit and eventually eliminate finger pointing, and wants to drive more standardization for its tools.



Government

(U.S. agency)

This department adapted its practices to comply with NIST 800.53 frameworks specifically. This department was highly segmented, with separate teams for hardware, software, networking, and security. These teams, too, were segmented.

- The teams are focused on device vulnerability spanning across IT and security teams.
- Each team had to consider new tools to update processes and capabilities for security and infrastructure & operations teams.
- There was heavy investment in how to manage both the private cloud and an emerging hybrid cloud strategy.
- The merger of several agencies into one provided a trigger for transforming and standardizing some security and operational processes.

Security and Operational Challenges Are Skyrocketing

Multiple clouds equals multiple silos. COVID-19 has prioritized identity and access management (IAM), encryption, remote access, and application performance while driving new demands on customer engagement. And increasing complexity with modern application stacks means increased potential for expensive application failures.

Rising complexity challenges:

Application, security, and infrastructure problems are hard to find and contain in complex, distributed environments.

Fragmented tools, processes, and teams don't work well together and increase costs.

Application failures due to this complexity result in higher business risks, security breaches, and poor customer experience.

Containers and microservices pose new security and compliance challenges.

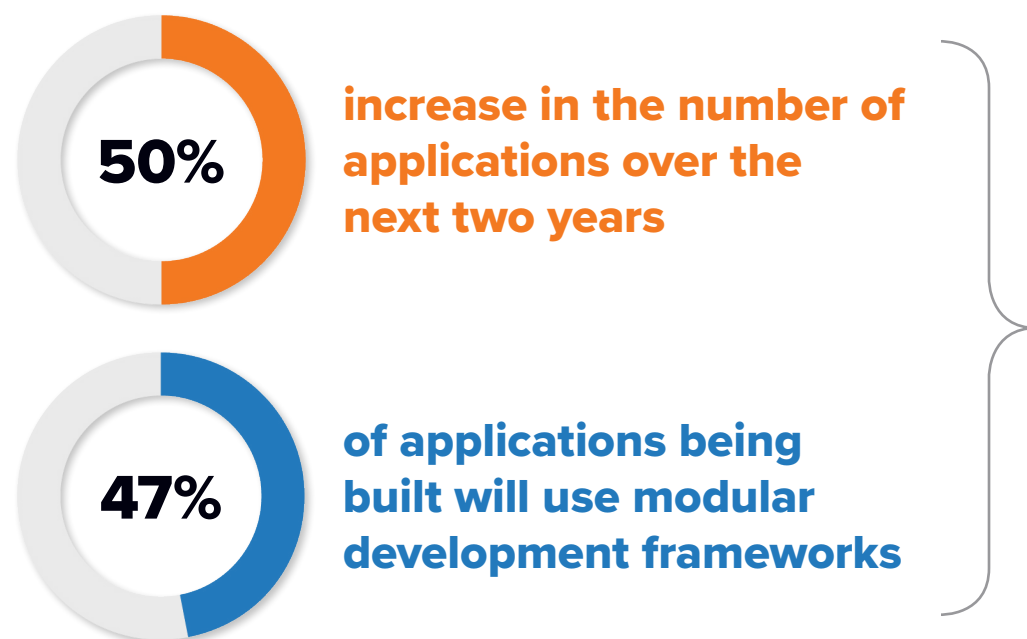
“A few years ago we went through a merger with two other agencies. During the change, we decided we had to collaborate more between security and operations teams. Now, we are adding tighter process integration with our networking team. It's been difficult, but the outcomes have helped everybody.”



Large state agency customer

Software Development Cycles Are Accelerating

Organizations with DevOps deployed will release new code monthly or weekly, causing security and operations teams to move faster to meet rising demands. The best practice is to streamline processes between IT and security.



Agile, DevOps, and site reliability engineering (SRE) adoption and organizational practices are shaping most IT organizations.

“Just three years ago, I rarely collaborated with development. Now, it’s a requirement to enable the company to move and respond faster to business dynamics. We are finding and solving problems faster than ever before.”

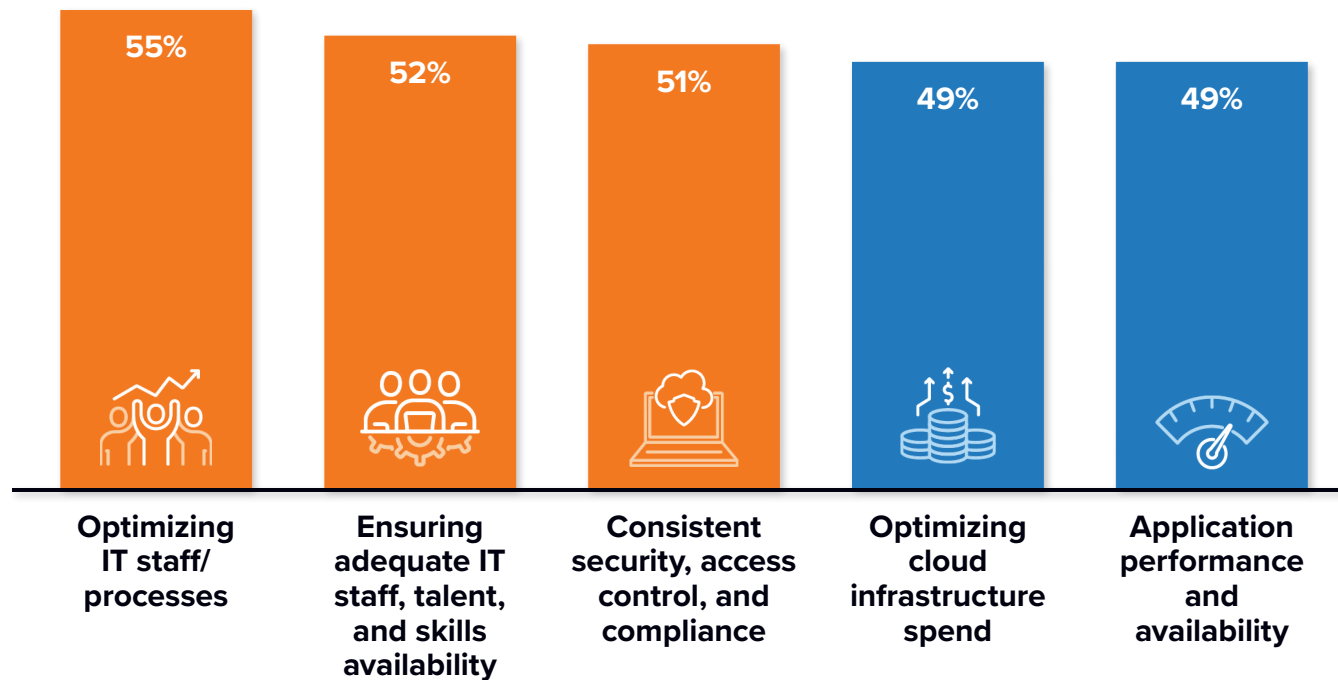


Large manufacturing customer


Source: IDC CloudPulse Q1/19, June 2019

Multicloud Disrupts Traditional Security and Operations, Creating Stress Between IT and Security


What are the most pressing operational challenges resulting from your multicloud infrastructure strategy?



“Everything is being driven to our hybrid cloud. Our old datacenter model is disappearing.”

 Area IT manager, top 3 hotel chain

“Our multicloud success requires IT and security teamwork, or we will fail.”

 Large insurance company

n = 200 enterprise I&O decision makers using multiple infrastructure clouds, multiple selections permitted | Source: IDC Multicloud Management Survey, March 2019

What's Needed to Meet These Challenges?

Capabilities that:



Offer integrated visibility across security and operations teams, which also includes DevOps and ITOps



Operate in a self-service way for team collaboration



Use context-aware predictive indicators for problem identification and containment across teams



Automate workflows that include compliance, security, and audit to ensure the integrity of cloud services deployment



Take a combined risk-based approach for operations and security



Enable process integration that drives automation across security, operations, and networking teams



Correlate security events with operational events to present a holistic picture

“Most Ops team get it—they try to balance daily work with how security and compliance fit in.”



Corporate VP,
leading insurance company

“The first thing I look for in a job applicant is: Do they understand risk?”



Certified Information Security Manager (CISM)
for a top 20 U.S. financial institution

Security and Operations Teams Need to Standardize on Better Platforms

Fragmented processes between security and operations teams are rampant, while fragmented tools and processes are slowing IT operations and make cross-team collaboration difficult. Integration is required for efficient and secure operational agility.

Tool silos:

 Application	→	Fragmented data pools
 Network	→	Ineffective root cause analytics
 Cloud ops	→	Disconnected processes
 DevOps	→	No service views
 Security	→	Poor communication

Leads to:

Process and tool integrations drive collaboration and reduce business risks.

“Some of our security and operational processes are fragmented; COVID-19 is accelerating their integration and automation.”



Corporate VP, Ops, leading aerospace company

“The networking and Ops teams collaborate today; compliance and risk objectives transcend both teams.”



Corporate VP, Ops, large insurance company


“The question facing Ops is: How far can we extend our existing tools to the cloud?”



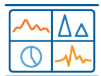
Corporate VP, Ops, leading insurance company

IT Executives Are Investing in Integrated Security and Operations

Top reasons:

 **Create concise and deep visibility**, which will provide correlated security data with network maps and related performance data to understand the threat footprint.


 **Ensure security and compliance policies are enforced**, because the fear of compliance-based fines is especially acute for midsize businesses

 **Wrap security context to business services** by analyzing data at scale, detecting potential vulnerabilities, and making proactive recommendations via root cause analytics.


 **Optimize the security of services** through integrated processes and dashboards.

 **Maintain fidelity and compliance** by using data sources only once.

“Our org structure has made security everyone’s responsibility.”

 Area manager, operations,
leading aerospace company

“We are not JW Marriott—I can’t afford a \$5 million fine for a data breach.”

 IT manager with responsibilities over several
properties of a midsize U.S. hotel chain

Best Practices to Accelerate Security and Operations Transformations

- ✓ **Identify critical processes** that overlap between security and operations teams; **collaborate** to identify areas to automate.
- ✓ **Collaborate and share** security libraries, APIs, compliance requirements, and reporting needs with operations teams to embed capabilities where possible.
- ✓ **Use DevOps principles** such as automation and the use of KPIs to measure progress and success across security and operations teams.
- ✓ **Recognize that the adoption of SaaS** as a result of work-from-home accelerates the growth of pervasive data defense and response solutions, with particular attention paid to cloud security gateways.

- ✓ **Both IT and security should adapt architectures** for VPNs and new firewall/IPS/UTM support and **ensure that the network remains impeccable** for employees, contractors, and customers alike.

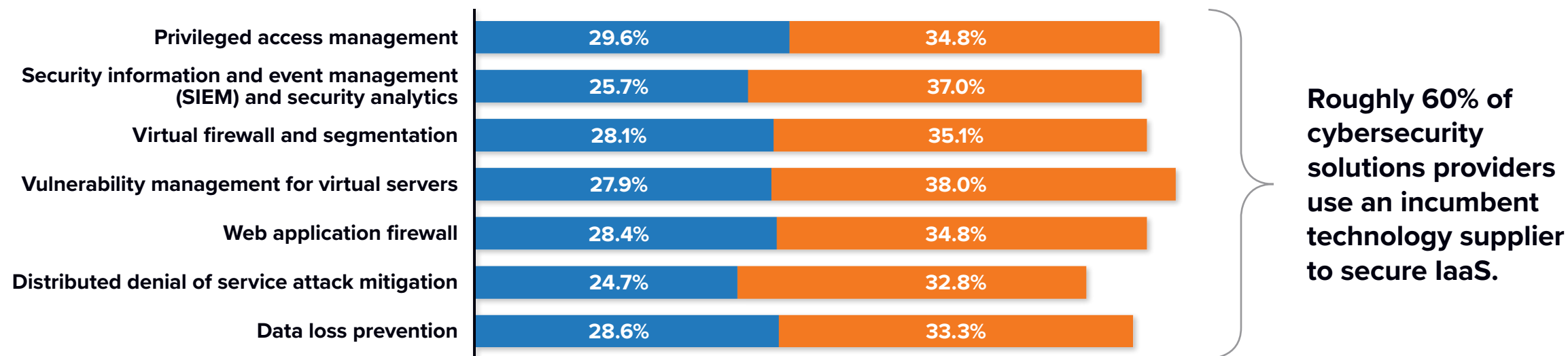
Capacity issues become a joint consideration. Most on-premises networks have a planned remote access bandwidth capacity and a surge capacity. However, the math changes, because network planning was not designed to accommodate surge capacity for individual employees.
- ✓ **Both IT and security should acquire new skills,** as the network has completely changed.

SecOps manages multiple networks ranging from hybrid and multicloud environments; requires visibility for SaaS; and needs to consider virtual private networks, IoT, mobile, and even social networks.

Land and Expand – The Role of the Cybersecurity Solutions Provider in Securing the Transition to Multicloud Environments







Thinking about security solutions for cloud architecture (IaaS), when your organization first adopted cloud architecture, how did you choose to secure it? (Answer by _____ technology.)

■ Extended on-premises solution for IaaS ■ New solution from existing on-premises vendor



n = 405 North America-based companies (223 replies = companies with 2,500–4,999 employees; 116 replies = companies with 5,000–9,999 employees; 66 replies = companies with 10,000+ employees) reflected as percentage of companies replying (unweighted) | Source: Cloud Security Survey, IDC, December 2019 | Note: Managed by IDC's Quantitative Research Group

IT and Security Discrete and Shared Concerns

	Network side of operations	Security side of operations	
 AI	Insights for automation and capacity	Statistical baselines, user and entity behavior analytics (UEBA), and predictive analysis	 Shared interests: Workflow Risk Policy Access Compliance Patching Capacity
 Tools	Continuous application and network performance monitoring	Used to determine anomalies and threat actors	
 Balance	Load balancing and application delivery	Monitor against configuration drift	
 End user experience	The network is the sum of all conversations	Make sure ingress/egress to the network is safe	
 Applications	The reasons for networks in the first place	Come from public and private clouds and are hard to manage	

The Transitioning World: COVID-19 Makes You Rethink

Don't rethink your approach to security. Instead, rethink your approach to IT and the manner in which business application and data services are provided to users. Addressing security without addressing IT produces a suboptimal, kludged, band-aid-riddled mess.

COVID-19 accelerates the movement to implement security around the four central control points of digital transformation:

Endpoints
Protection has to be applied at termination points.



Identities
Least privileged access is born from identity; identity is the new perimeter.



Applications
Increasingly disassociated from specifically defined servers, networks, and infrastructure. For security, Layer 7 is the new Layer 3.



Data
The adversary's bounty of choice. Security measures need to travel with the data and be applied to the data.

Retire network-centric IT approaches.

VPNs are a valuable security tool. First, stop to ask if a user needs to be on the corporate network at all. Least privileged access and reduced help desk calls are the upside.

Conclusions

Most important conclusion	<p>An organization has to be finely attuned to “risk.” This is not a simplistic view: IT and security operations center (SOC) operations managers want their teams to think about how to mitigate exposure of critical assets, personally identifiable information (PII), suddenly accessible internet-facing assets like S3 buckets, and web servers that become exposed through poor configurations or conflicting firewall rules.</p>
Implied trade-off	<p>Minimizing risk is no small achievement. If we believe that an analyst’s time is static, that means that building and creating redundancies to enforce risk is prioritized over tracking less severe vulnerabilities, or a company is willing to live with smaller network performance issues if it is unsure how a patch or remediation will affect its risk posture.</p>
Compliance	<p>In all candor, IDC found that companies wanted to have the ability to “show” compliant practices as much as they wanted to maintain actual compliance. The hierarchy of fines is a deterrent, especially in midsize companies.</p>
Extensibility	<p>Network architecture is becoming more and more cloud-based. Digital transformation was coaxing this hand, but COVID-19 was changing the nature of security as we conducted the study. Companies had to find capability for VPNs, and endpoint protection platforms became increasingly important. However, central SIEM and network platforms remained intact, because all applications intersect with the network at some point and IT/security teams needed a central place to initiate workflow.</p>
Biggest surprise	<p>The security teams remained highly segmented. For instance, one analyst might be devoted to checking new domains for phishing; another analyst might run down an initial set of alerts; yet another would be devoted to firewalls or maintaining Active Directory and identity access management (IAM) tools. The tools may be consolidating, but in our panel, IDC found a high degree of specialization within the security team.</p>

Methodology

- In April and May of 2020, IDC conducted eight interviews with IT Operations and Security Operations teams to better understand the challenges they face in interacting, and how they have overcome those challenges.
- Four operations and four security interviews were conducted in each of the following verticals: Government (2), Finance (2), Manufacturing (2), and Hospitality (2).
- Data was also taken from IDC enterprise IT organization inquiries on the related security, IT, infrastructure, and operations topics and themes.
- There is data cited from several other IDC surveys completed independently of SolarWinds's knowledge and input, on adjacent topics and themes. These surveys are part of IDC's subscription research services.
- IT/Security interviews were matched in terms of company size and vertical so that a clear message could emerge per vertical.
- Interview analysis was combined with existing survey data to formulate a full narrative.
 - IDC Cloud Security Survey, December 2019
 - IDC Multicloud Management Survey, March 2019

About the Analysts



Chris Kissel

Research Director, Security & Trust Products, IDC

Chris is responsible for cybersecurity technology analysis, emerging trends, and market share reporting. His primary research area is Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO). The major technology groups within this practice are SIEM, device and application vulnerability management, threat analytics, and automation and orchestration platforms. Chris effectively covers the processes that security operation center (SOC) analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network within a security and vulnerability management and security analytics paradigm.

[More about Chris Kissel](#)



Stephen Elliot

Program Vice President, Management Software and DevOps, IDC

Stephen manages multiple programs spanning IT Operations, Enterprise Management, ITSM, Agile and DevOps, Application Performance, Virtualization, Multicloud Management and Automation, Log Analytics, Container Management, DaaS, and Software Defined Compute. Stephen advises senior IT, business, and investment executives globally in the creation of strategy and operational tactics that drive the execution of digital transformation and business growth.

[More about Stephen Elliot](#)

Message from the Sponsor

We are in an ultra-hybrid world with multi-everything (endpoints, devices, clouds). In order to successfully navigate this landscape, ITOps, DevOps, and SecOps teams need to more closely align.

However, resulting new complexities within the IT infrastructure have thrown a wrench into our desire to do this successfully. As this study showed us, the challenges these teams face are across all verticals. We're all trying to do more and push our IT infrastructure to its limits, and cybersecurity can't be an afterthought.

When we work together, things move more quickly and more efficiently. When we're not working together, there are issues that range from delays in code pushes to IT downtimes to security breaches.

In order to have teams work together the most effectively, we really need a three-pronged thing that ties together people, processes, and technology. If you tackle just one, it's not going to make the difference you're looking for.

We need to further invest in automation where it makes sense, the standardization of processes, and collaboration that further ties together goals and priorities. We need to take a risk-based approach that helps us better prioritize and manage. And we need to simply understand that we share a lot of the same priorities and we're not as different as we really think.

Tim Brown
Vice President of Security, SolarWinds

[Visit the SolarWinds Trust Center](#)



IDC Research, Inc.

5 Speen Street
Framingham, MA 01701
USA
508.872.8200

[idc.com](https://www.idc.com)

[@idc](https://twitter.com/idc)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Permissions: External Publication of IDC Information and Data

Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

IDC Doc. #US46790820