The State of Cybersecurity Priorities and Strategies 2017

SCALE
Venture Partners

For cybersecurity, 2016 was an unprecedented year. Data breaches, phishing attacks, online snooping and digital intrigue involving the presidential candidates and foreign powers dominated the global news.

Against this highly charged geopolitical scene, companies continued to be targeted by cyber criminals seeking to steal their sensitive data, hijack customer accounts and exploit security vulnerabilities in networks and systems. Scale Venture Partners asked top security professionals from the CISO office to outline what ‘s on their minds and where they plan to take their company’s security strategy in 2017.

“The State of Cybersecurity Priorities and Strategies 2017” examines the top CISO concerns and proposed approaches for addressing them; solutions include shifts in security spending, adoption of new technologies and a reevaluation of how accountability is viewed within the organization.

Key Findings

CLOUD, NETWORK, AND DATA CENTER SECURITY WERE THE AREAS MOST WIDELY INVESTED IN LAST YEAR, AND CONTINUE TO BE TOP 3 FOR INCREASING INVESTMENT IN 2017.

THE PREVALENCE OF IN-HOUSE SOLUTIONS SUGGESTS THERE ARE OPPORTUNITIES FOR SECURITY VENDORS TO GAIN TRACTION WITHIN THIS GROWING MARKET.

ORGANIZATIONS PLAN TO INVEST MORE DOLLARS IN CYBERSECURITY AND MAKE CHANGES TO HOW THEY ARE ALLOCATING RESOURCES, PARTICULARLY IN RESPONSE TO THE TRUMP PRESIDENCY.

MALICIOUS HACKERS ARE THE NO. 1 THREAT KEEPING SECURITY LEADERS UP AT NIGHT. EVEN SECURITY LEADERS WHO ARE WELL EQUIPPED TO HANDLE CYBERSECURITY RISK ARE HIGHLY ANXIOUS.

WHILE AI FUNCTIONALITY IS JUST STARTING TO BE ADOPTED WITHIN THE SECURITY MARKET THE MAJORITY OF SECURITY LEADERS SEE REASONS TO INVEST IN AI NEXT YEAR.

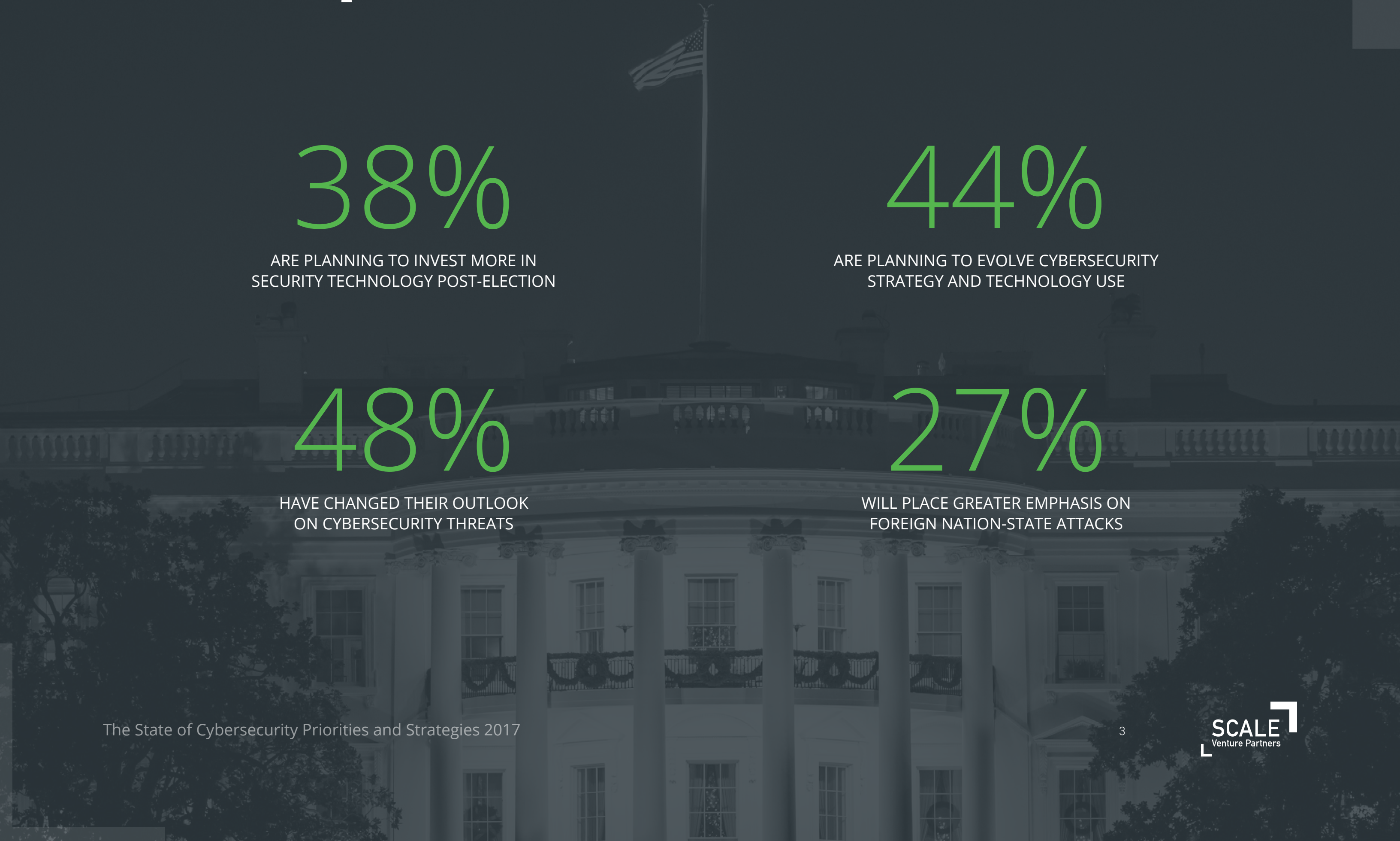
SECURITY IS NO LONGER SILOED — IT IS INCREASINGLY A BUSINESS ISSUE, WITH THE ONUS FOR ACCOUNTABILITY FALLING INSIDE AND OUTSIDE OF THE SECURITY ORGANIZATION.

Security Spending is On the Rise

Security Investment Priorities for 2017 are moving towards Political Impact on Spending, Protecting the Infrastructure Layer, Rise in Automation and AI and Building In-House Solutions.

Seventy-six percent said they invested more money in security technologies in 2016 than they did the year prior. Eighty-nine percent of respondents are planning to increase their investment in security resources in the next 12 months. The biggest increases will be seen among mid-sized companies (21 percent of mid-sized companies vs. 14 percent of large enterprises).

The Impact of the Current Presidential Administration



38%

ARE PLANNING TO INVEST MORE IN SECURITY TECHNOLOGY POST-ELECTION

44%

ARE PLANNING TO EVOLVE CYBERSECURITY STRATEGY AND TECHNOLOGY USE

48%

HAVE CHANGED THEIR OUTLOOK ON CYBERSECURITY THREATS

27%

WILL PLACE GREATER EMPHASIS ON FOREIGN NATION-STATE ATTACKS

Leaders Prioritize Cloud, Data Center and Network as Top Security Concerns

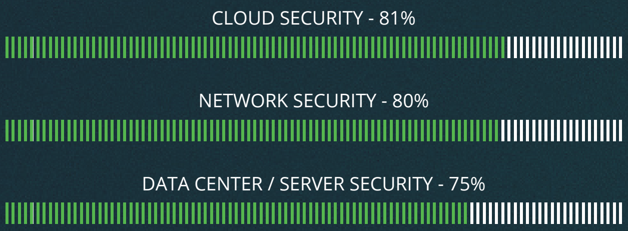
Despite the proliferation of mobile phones and connected devices, the majority of corporate secrets still reside inside the corporate network and major corporate-sanctioned cloud applications and cloud databases.

Cloud, network, and data center security were the areas most widely invested in last year, and continue to be top three for increasing investment in 2017. Security leaders are focusing on protecting data, whether it is in the cloud, data center or on the network.

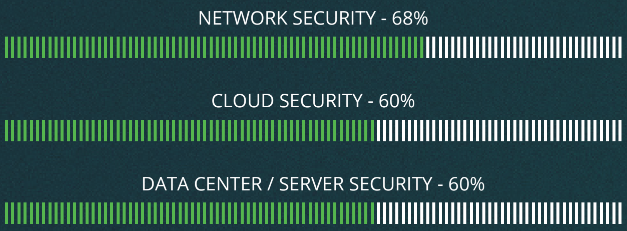
Networks and servers have traditionally been the first line of defense, and that isn't expected to change in 2017. As we've moved to a world where corporations have a perimeter-less security posture, it is still critical to secure the core IP, customer information and PII (personally identifiable information).

At the same time, the rise of SaaS, the utility consumption model and ease of use have driven companies of every size, across every industry to move in earnest to the public cloud. In fact, Gartner predicts that by 2020 the shift to the cloud will affect more than $1 trillion in IT spending. The cloud is enabling enterprises to adopt a truly digital business model, but with public cloud and hybrid cloud come new security issues. As a result, investing in cloud security to protect a more highly-distributed data center has been a top priority.

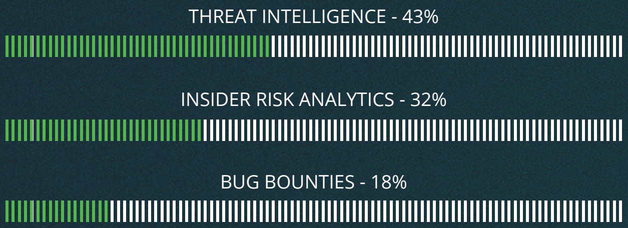
TOP CYBERSECURITY TECHNOLOGY INVESTMENTS IN 2016



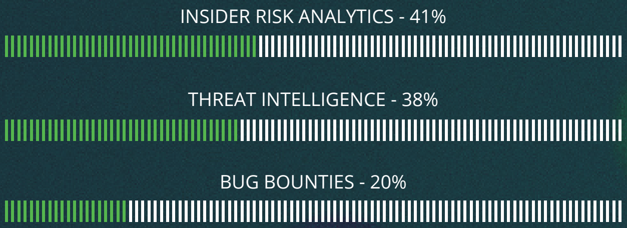
TOP CYBERSECURITY TECHNOLOGY INVESTMENTS IN 2017



LOWEST CYBERSECURITY TECHNOLOGY INVESTMENTS IN 2016



LOWEST CYBERSECURITY TECHNOLOGY INVESTMENTS IN 2017



Security Leaders Plan to Double Down on Automation and AI

While we are experiencing a steep rise in security technology investment (76 percent invested more in security technology), finding and hiring skilled security analysts to manage these tools isn't keeping pace.

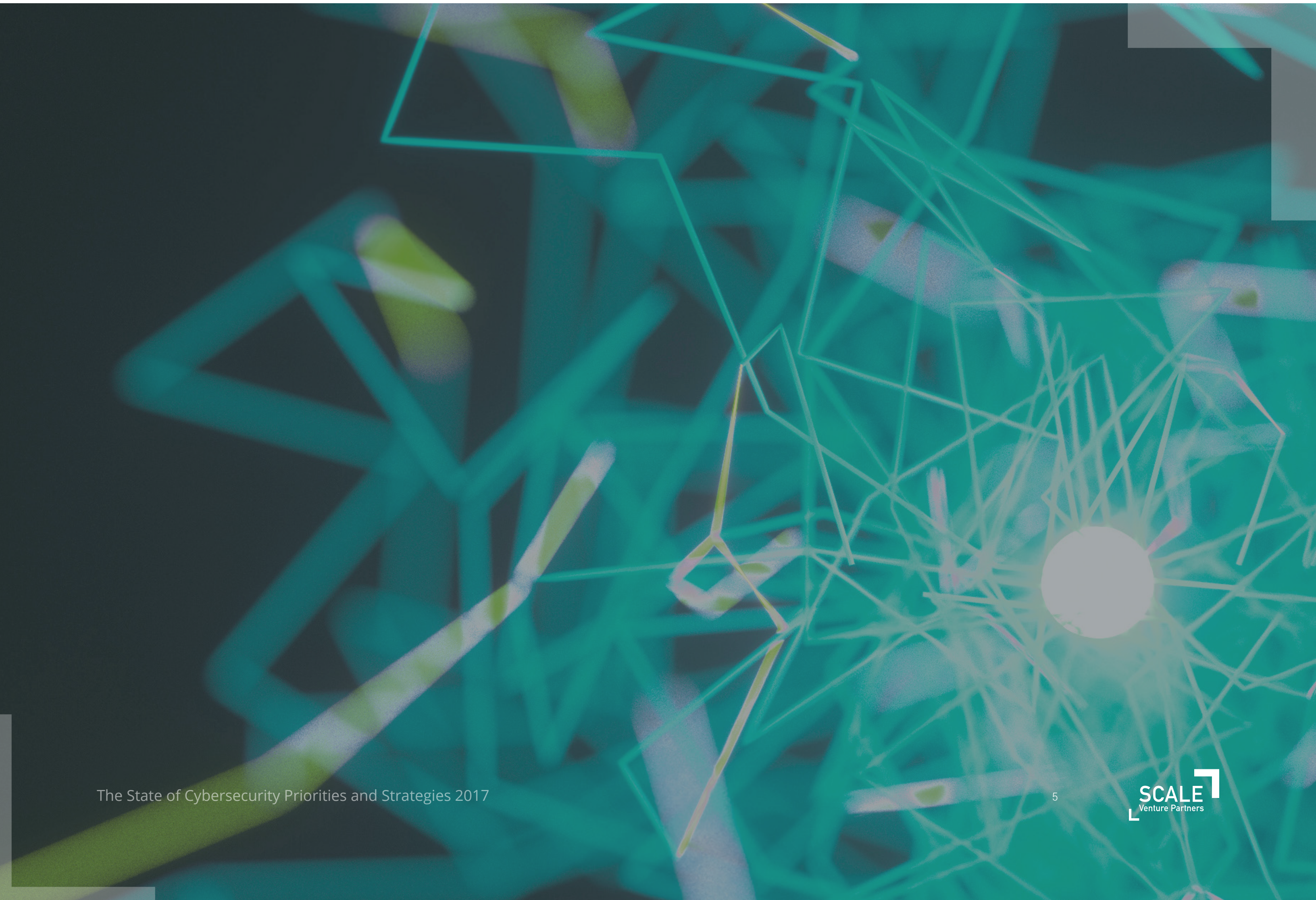
The result? Alert fatigue and a reevaluation of the security operations center and network operations center. One area where security leaders have looked to solve these challenges is automation. In the past two years, 75 percent have purchased cybersecurity automation tools and 47 percent plan to invest more money in security automation tools in the next year.

Looking beyond basic automation, there is strong interest in how artificial intelligence will shape new security tools. In that past two years, 47 percent have introduced AI-powered security solutions and 75 percent of those using AI agree that it has significantly or somewhat increased their ability to address security threats. As a result, 93 percent plan to invest in AI and machine learning-powered security solutions in 2017. Large enterprises are more readily adopting AI solutions, as compared to mid-sized companies (53 percent vs. 36 percent), which is not surprising since operating these products typically requires more resources.

Home Grown Solutions Make Way for New Opportunity for Vendors

Companies are using a combination of vendor and home-grown solutions, with more than half (53 percent) of respondents building in-house tools due to lack of a viable commercial alternative. In-house solutions are addressing the top three issues: data breaches (60 percent), malware / advanced persistent threats (56 percent), and employee use / employee negligence (53 percent). This suggests there is still room for improvement for existing vendors and a potential for innovation by new vendors.

Furthermore, once a company has adopted a security vendor, they're more likely to stay with them. Of the 62 percent that changed the allocation of security resources, only 17 percent report changing vendors year over year.



Unpacking the CISO’s Top Concerns

Hackers are the No. 1 Threat Keeping CISOs Up at Night

Fifty-nine percent believe that the threat level for data breaches will increase over the next 12 months, more so than any other threat. Hackers have managed to gain access to confidential company information from startups and Fortune 500 companies across many industries, leading only to more fear, uncertainty and doubt.

72%

ARE INVESTING THE MOST RESOURCES IN DATA BREACH PROTECTION

40%

DATA BREACHES ARE THE TOP IT SECURITY RISK IN THE ORGANIZATION

46%

DATA BREACHES ARE A TOP 3 THREAT KEEPING THEM UP AT NIGHT

49%

DATA BREACHES ARE THE NO.1 RISK WHERE THEY ARE PLANNING TO DEDICATE MORE RESOURCES IN 2017

60%

BUILT AN IN-HOUSE SOLUTION DUE TO A LACK OF COMMERCIAL ALTERNATIVES

70%

ARE STILL VERY ANXIOUS ABOUT THE RISK OF A BREACH (RANKED ANXIETY 7, 8, 9 OR 10 ON A SCALE OF 1-10)

Visibility Into Cybersecurity Risk Doesn’t Guarantee Peace of Mind

Even security leaders who are well equipped to handle cybersecurity risk feel high levels of anxiety about their exposure to potential breaches.

Given how uncertain the risk landscape is, preparedness doesn’t necessarily equal peace of mind. Although many companies perform risk assessments, they remain anxious about cybersecurity risks. Eighty percent feel well equipped to handle cybersecurity risks, but still seventy-nine percent have a high level of anxiety around a potential threat to their organization.

Those assessing risk more often, on a daily or weekly basis, report feeling the most anxiety, compared to those who assess risk less than weekly (59 percent vs. 44 percent), but also feel more equipped to handle cybersecurity risk (60 percent vs. 40 percent).

SECURITY LEADERS REMAIN ANXIOUS DESPITE PREVENTATIVE MEASURES

92%

BELIEVE THAT THEIR COMPANY’S SECURITY INVESTMENT STRATEGY IS ALIGNED WITH THE TOP THREATS

86%

APPLY A RISK-BASED APPROACH TO PURCHASING DECISIONS

71%

HAVE PURCHASED RISK-ASSESSMENT TOOLS OVER THE PAST TWO YEARS

95%

BELIEVE THEIR COMPANY HAS MADE PROGRESS IN SECURING DATA AND NETWORKS

SCALE Venture Partners

Security Has Been Elevated to Board Level

No longer is security solely an issue for the security and IT team — it has become a C-level responsibility.

This shift in mindset about security as a shared responsibility across functions turns security into a business issue, rather than being siloed. Security leaders are approaching security as an issue that the entire company plays a role in executing. This is especially true for large companies that are much more likely to apply stricter enforcement and expand accountability for security across the business than smaller companies (63 percent vs 49 percent).

Eighty-two percent of respondents have defined metrics to communicate the business impact of the security program to peers and/or management. Security has been elevated as a top business priority, and security leaders are bringing the rest of the organization into the fold.

94%

AGREE THAT SECURING AND / OR PROTECTING DATA IS A HIGH PRIORITY IN THE ORGANIZATION

59%

ARE EXPANDING ACCOUNTABILITY FOR SECURITY ACROSS THE BUSINESS

82%

HAVE DEFINED METRICS TO COMMUNICATE THE BUSINESS IMPACT OF THEIR SECURITY PROGRAM

38%

ARE PROVIDING GREATER TRANSPARENCY AND VISIBILITY INTO THE STATE OF THEIR SECURITY

48%

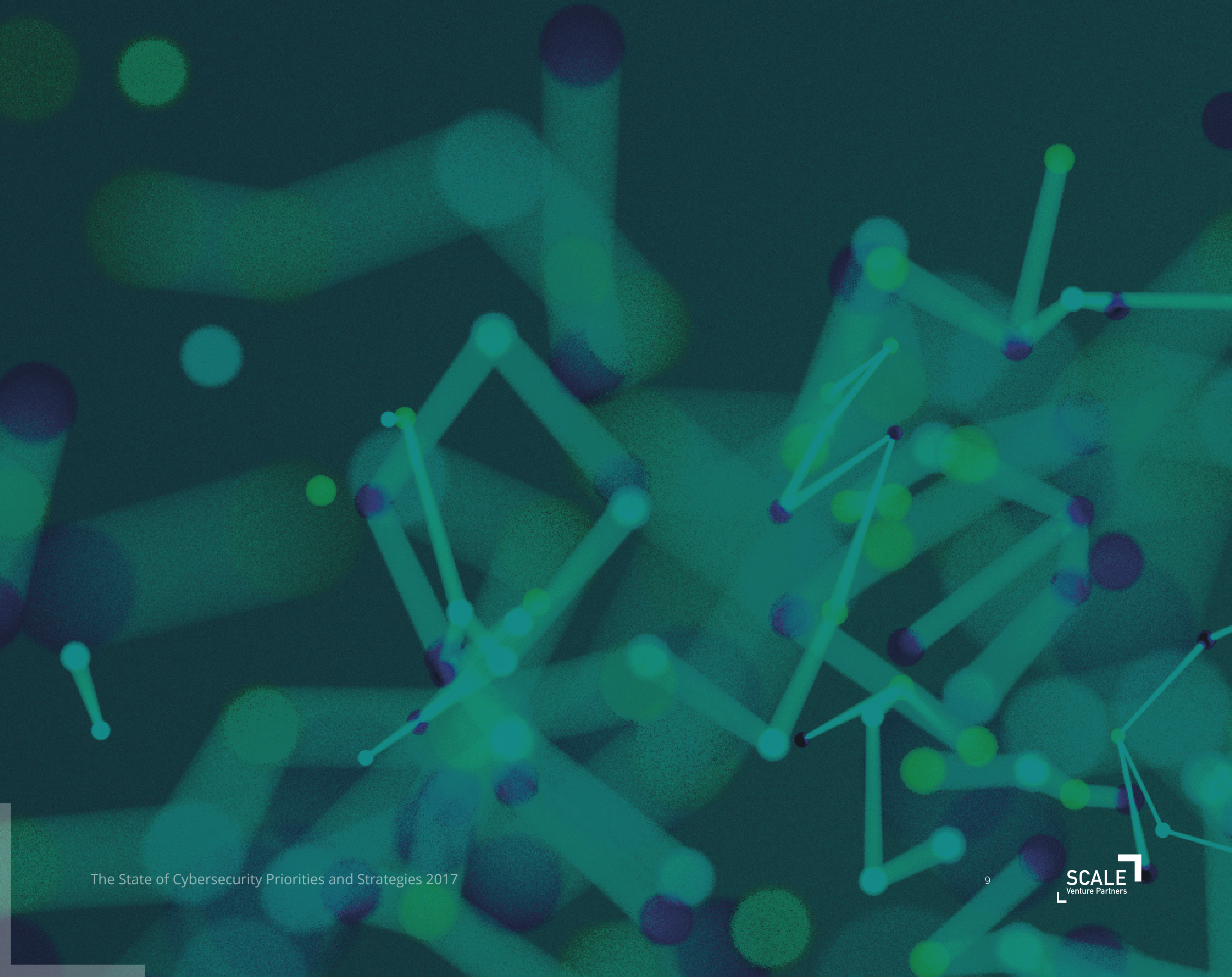
ARE INCREASING METRICS AND REPORTING AROUND CYBERSECURITY

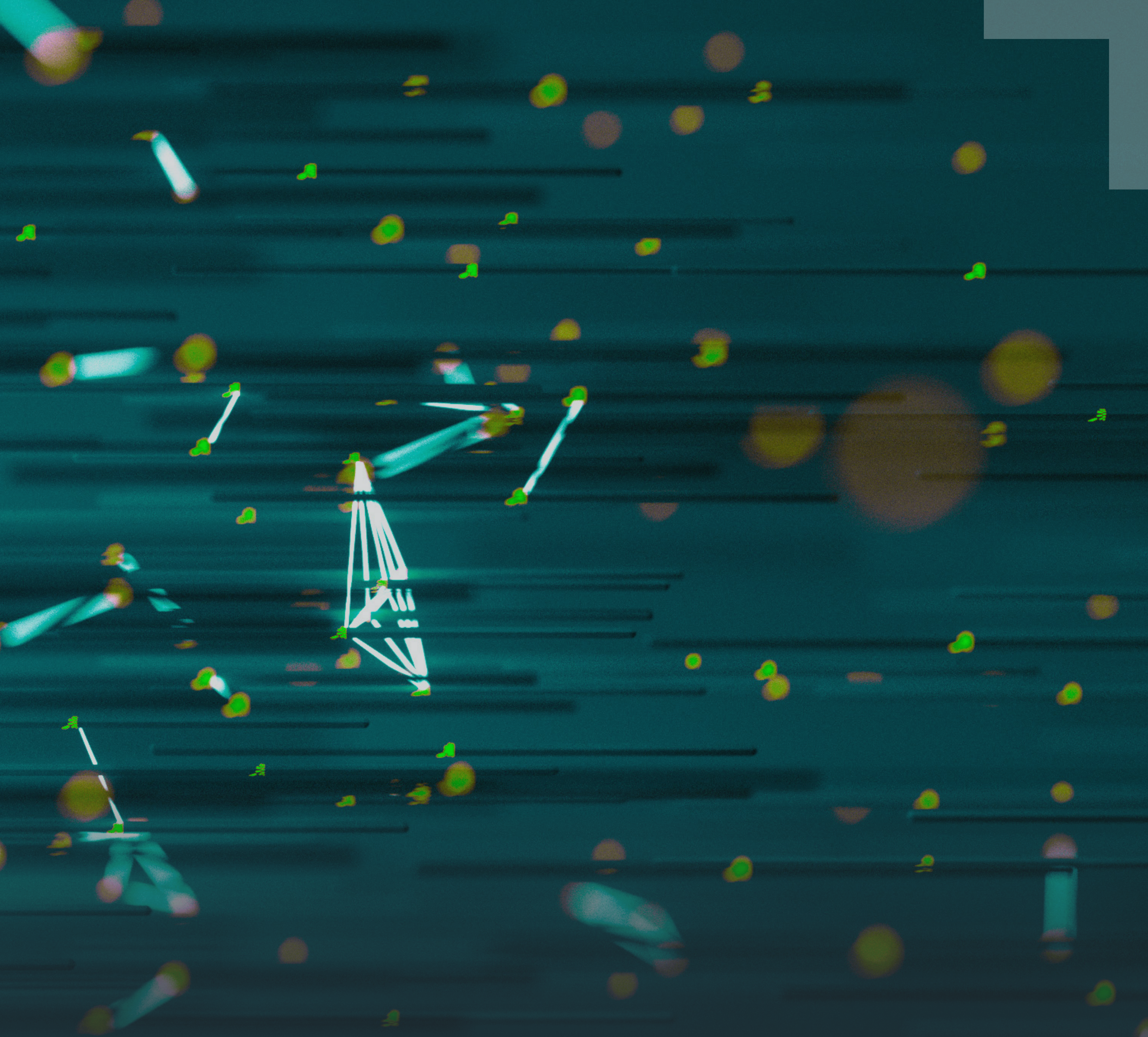
70%

ARE INCREASING INTEGRATION OF SECURITY WITH OTHER TEAMS

Conclusion

Security leaders will continue to prioritize tools and strategies to secure a highly distributed environment, and leverage automation and AI to deal with the evolving threat landscape. Companies will continue to seek (or build) security solutions that meet more complex needs and those that are not addressed by currently available solutions. Despite the high level of anxiety over the looming threat of the next data breach, security leaders remain optimistic. Ninety-five percent believe their company has made progress in securing data and networks, and many are actively taking steps to ensure that employees and business leaders — not just security leaders — are accountable for security.





Methodology

Scale Venture Partners conducted a survey of 200 security leaders in the United States who are responsible for security buying decisions, the success of security deployments, or the overall security of the company.