Friday Networks
Det smarteste valget

3 IT security musts for 2020

How to protect modern IT architecture from the latest threats

CISCO
Partner
Distribution Partner

New threat landscape requires a new security approach

With the risk of experiencing a breach increasing steadily throughout the 2010s, organizations will need to take action in 2020 to reverse the trend. At the same time, the way companies use IT resources has changed rapidly in recent years. This has been driven by the exponential growth of the public cloud, SaaS applications and mobile ways of working.

The employees of the 2020s need and demand far greater flexibility, speed and convenience from IT resources - and they are counting on you, the CIO, to deliver.

> Organizations were one-third more likely to suffer a breach within two years in 2019 than in 2014
>
> – 2019 "Cost of a data Breach Report" by the Ponemon Institute and IBM

This guide will show you what tools, features and practices you need to make real progress on these benchmarks and empower your organization to be more secure.

This will also make your security efforts far more efficient so that your team can spend more time on important threats and value-added activities.

Instead of saying, no, it's too risky from a security perspective, you can be the hero that implements a security solution and best practices that make it secure. Your organization shouldn't have to choose between security and flexibility. But this requires that you change your approach to security and bolster your defenses with the latest technologies.

Focus your efforts on three critical benchmarks for IT security in the 2020s to bring your security in line with the realities of today's IT infrastructure and threat landscape:

1. Extending protection to data everywhere, this means on all devices, networks, branch offices, clouds and applications.
2. Identifying threats significantly faster before they have time to do much damage.
3. Blocking more threats from the very beginning before they can cause any damage.

Contents

1. Keep your data secure everywhere

In the past, companies relied on keeping everything inside the office's physical and digital walls to ensure security. This was based on the premise that information and resources could only be secured when they are used from company-controlled stationary devices in the office on the corporate network. However, with the emergence of cloud computing, the digital workplace, and mobile devices, the ground rules have changed, as employees expect and need to be able to work anytime and from anywhere efficiently.

This requires greater flexibility, faster connections and less hassle. As a result, companies are increasingly providing direct internet access (DIA) to remote offices instead of routing all traffic through the head office. They are also ditching VPNs to ensure faster connections and a better user experience. However, this poses major security challenges.

More and more employees are working outside of the central office – and often outside its protection. To secure these remote workers and locations requires a fundamentally different approach.

A recent survey of 450 cybersecurity experts by the Enterprise Strategy Group explored the many facets of protecting a network without perimeters.

40%

of today's workers are roaming users.

88%

of organizations have 5+ remote offices.

78%

believe roaming or remote users are most vulnerable to attack.

66%

of respondents have experienced a target attack - the majority of these respondents report roaming and remote users have been compromised.

82%

have a VPN policy, but...

85%

believe roaming users violate that policy.

The workforce has never been more distributed – or more at risk. Most organizations are still using traditional methods to protect roaming and branch users –

but they just can't keep up with today's needs and expectations.

60% +

report all/most proxied roaming and remote traffic goes through the corporate network – but backhauling is expensive and slows performance for users.

To help drive better remote performance, SaaS and Direct Internet Access adoption are on the rise – and so are security concerns.

41%

worry about data breaches in shadow IT SaaS apps – which are introduced without IT oversight.

60%

expect that the majority of their organization's apps will be SaaS-based within 2 years

More and more organizations are looking for a different solution – cloud-deployed and consolidated.

79%

of organizations are making the shift to DIA.

Increasingly, organizations are introducing DIA to sattelite offices — and IT teams are struggling to secure these solutions without sacrificing performance.

> One-third of data breaches will be caused by shadow IT in 2020.
>
> – Gartner

The increased complexity of many organizations' IT infrastructure has caused more employees to turn to the dark side and use shadow IT as well as made it harder for IT to keep track of and control all the cloud applications in use. In addition, many use personal mobile devices for work regardless of the official BYOD policy.

In addition to all the different types of devices and networks, many companies are also using hybrid cloud setups. The resulting mix of on-premises servers, private clouds and different public cloud vendors is difficult to secure one at a time. This means that threats can come at your organization from many different directions. To support this highly diverse, complex and flexible IT infrastructure, you need to be able to secure the organization's data across all of it, everywhere and anywhere.

Start by implementing a security solution that can detect and report on all cloud applications used in your organization. This way, you can bring shadow IT out of the shadows and into the light of day. A solution that leverages automation and smart categorization and optimization makes it much easier to decide which apps could pose a threat and automatically block certain workflows.

You'll also want a solution with SD-wan integration so you can easily extend your security to remote offices and connect any user to any application across any cloud. Pairing this with a secure web gateway that redirects traffic from anywhere to cloud-based proxy servers will make all traffic transparent for your organization regardless of network or device.

In addition, a cloud-based firewall allows you to protect all branch offices with one firewall. This makes your defenses stronger and smarter than having separate firewalls for each office that would often result in a case of the right hand not knowing what the left is doing. If you have a firewall that can automatically apply policies and enforce them consistently everywhere, this will certainly make your life easier.

https://info.umbrella.com/esg-report-rise-of-dia.html

One in three organizations experienced a data breach that originated from a mobile device.

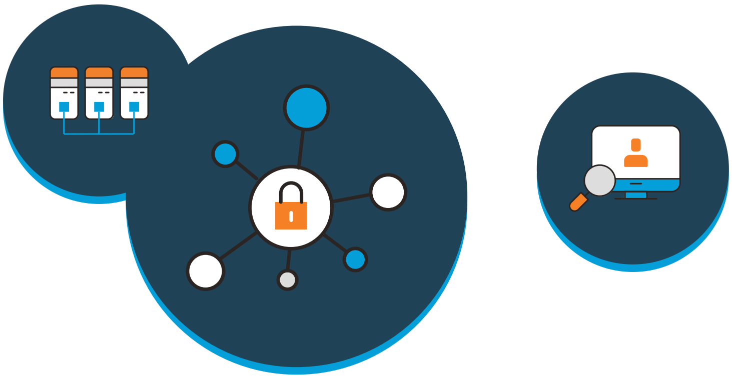
– "Verizon Mobile Security Index 2019"

2. Identify threats faster

It took Scandinavian companies an average of 225 days to identify a data breach according to data from the Ponemon Institute and IBM's 2019 "Cost of a Data Breach" report. Given that the same report shows that data breaches can cost millions of dollars and threats are becoming increasingly advanced, that's simply too long. Luckily, security best practices can help you shorten that length of time.

Leveraging more advanced security automation capabilities is an essential first step toward detecting threats faster. It's both difficult and expensive to manually monitor everything all the time, so you'll want machine learning algorithms that can flag suspicious behavior around the clock. The aforementioned report also found that:

breach costs were 95% lower for organizations with fully deployed security automation than those without automation.



In addition to cutting costs, automation was also shown to bring down the amount of time until a breach is identified from months to weeks by IAPP's analysis of data from RadarFirst. As reported in the article "How to evaluate your privacy-incident response program", this data, which comes from companies using automation best practices, showed that breach identification times in 2019 ranged from 19 to 27 days.

While you might think that detecting threats in 3 to 4 weeks instead of over half a year is good enough, the gold standard should really be within hours. Yes, you read that right -- and this has been proven more than possible with the right security solutions and practices in place. One thing that can really help is powerful investigation functionality. When powered by interactive threat intelligence, this enables you to significantly speed up investigations and detect breaches much faster with real-time threat information.

3. Block more threats from the outset

Cyber criminals have been stepping up their activities over the years, with the average number of security breaches increasing by 11% since 2018 and 67% since 2014, according to the "Ninth Annual Cost of Cybercrime Study" by Accenture and the Ponemon Institute. The Cisco Annual Cybersecurity Report also demonstrated the increasing sophistication of attack methods with the use of encryption to hide malware increasing by more than half.

> 70 to 90% of malware is unique to each organization
>
> – Cisco Security Research

The increase in both the quantity and quality of attacks challenges IT defenders to block more threats from the outset. This is where you'll want a smart security solution for both decreasing the number of threats your team has to deal with and freeing up more time to concentrate on the more complex threats that require your focus.

Cisco Security Research showed that 91.3% of malware uses DNS in attacks to gain command and control, exfiltrate data, or redirect web traffic

while 68% of organizations don't monitor recursive DNS. Therefore, deploying DNS-layer network security with DNS and IP layer enforcement can help block many threats right away before they do any damage and prevent callback to attackers from infected devices on your network. You can also leverage cloud-based proxy servers to decrypt and scan all traffic for malware and actively block it.

Cyber criminals frequently look to outsmart defenders by modifying old methods of attack and creating new approaches to avoid detection from traditional security solutions, which normally struggle to recognize a new threat until it has already had a widespread impact.

Therefore, another way you can block more threats is to make sure you have access to interactive threat intelligence that can uncover attacker infrastructure and stop attacks before they are launched. This way, you can turn the tables on cyber criminals and thus turn the hunters into the hunted. How's that for a change?

The efficiency gains of smart security

Deploying a cloud-based security solution powered by machine learning that consolidates and integrates security across your organization to give you centralized control will not only boost your security but also allow you to automate manual processes and significantly reduce the number of alerts that require your team's attention. This will make it easier to prioritize incidents that require your attention.

In addition to efficiency gains for your IT department, offering flexible and secure access to IT resources with less complexity opens the door to an outstanding employee experience and increased productivity for the entire organization.

Don't be the naysayer who held the organization back or the scapegoat of a costly data breach. Be the hero who gives everyone everything they want – without letting the bad guys in.

In summary:

To protect data everywhere, identify threats faster and block more threats from the outset, you’ll want a security solution that:

- Detects and reports on cloud applications to expose shadow IT and block apps as needed.
- Leverages SD-wan integration to securely connect any user to any application across any cloud.
- Centralizes your firewall to cover all offices from the cloud.
- Scans all traffic for malware via a secure web gateway by redirecting traffic to cloud-based proxy servers.
- Investigates threats with interactive threat intelligence to detect threats faster.
- Utilizes DNS-layer network security to block more threats and prevent infected systems from calling back.

References

Cisco 2018 Annual Cybersecurity Report. 2018. https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2018.html.

Goasduff, Laurence. Protect Your Organization From Cyber and Ransomware Attacks. 14 February 2018. Gartner https://www.gartner.com/smarterwithgartner/protect-your-organization-from-cyber-and-ransomware-attacks/.

Novakovic, Dragan. Cisco Security Research cited in Predict and Prevent Security Threats Before They Happen. 2016. https://www.cisco.com/c/dam/m/sl_si/events/2016/cisco_dan_inovativnih_resitev/pdf/new_advanced_cisco_security_solutions_-_opendns.pdf.

Oltsik, Jon. The RIse of Direct Internet Access (DIA). May 2019. Enterprise Research Strategy Group https://security.umbrella.com/esg-report-rise-of-dia.

Ponemon Institute and Accenture. Ninth Annual Cost of Cybercrime Study. 6 March 2019. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.

Ponemon Institute and IBM Security. Cost of a Data Breach Report 2019. 2019. https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.

Sher-Jan, Mahmood. How to evaluate your privacy-incident response program. 29 October 2019. IAPP https://iapp.org/news/a/how-to-evaluate-your-privacy-incident-response-program/.

Verizon. Mobile Security Index 2019. March 2019. https://enterprise.verizon.com/resources/reports/mobile-security-index/#report.