ExtraHop

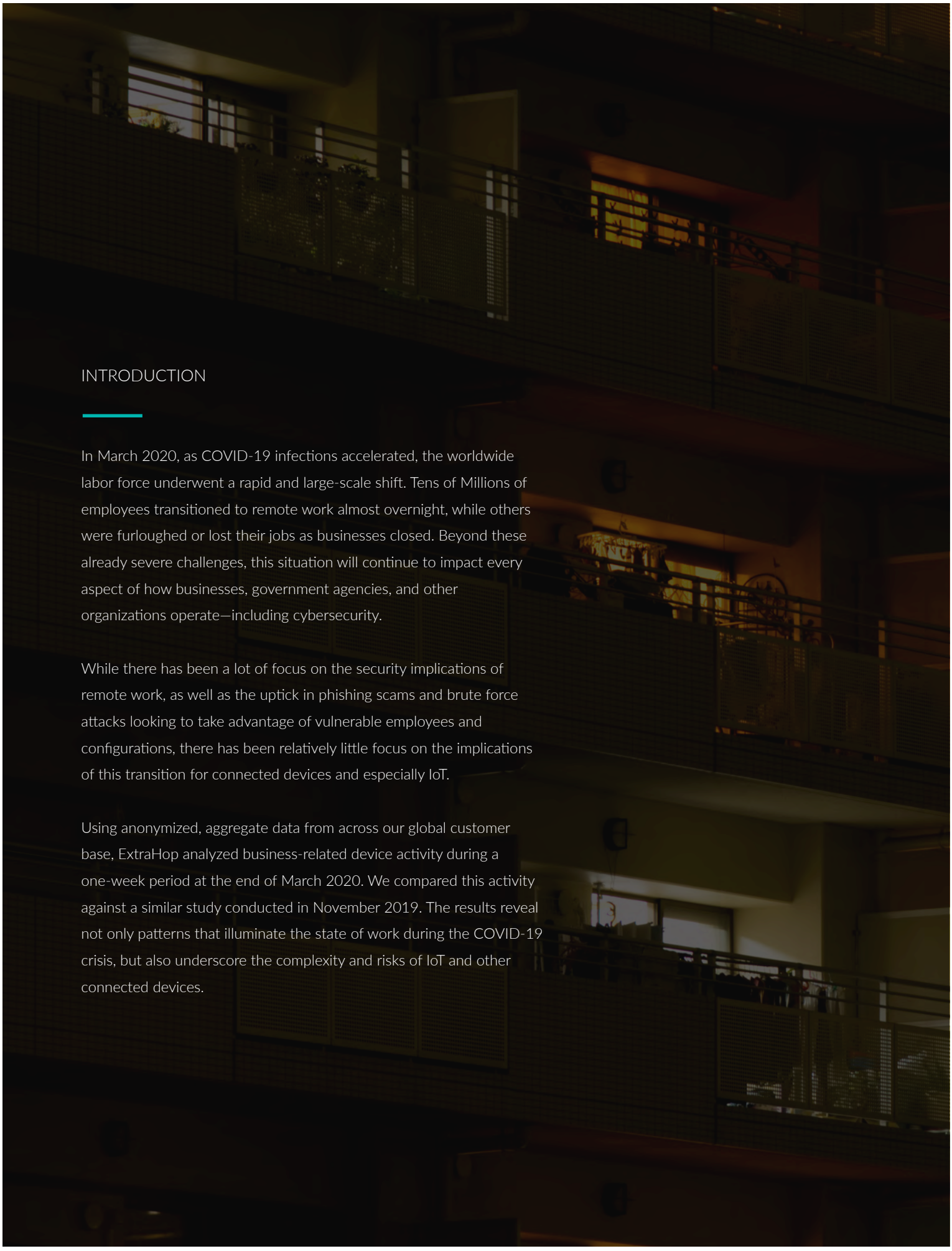
SECURITY REPORT

Connected Devices in the Time of COVID-19

What trends in IoT and other device communications reveal about the state of work during the pandemic—and the future of IT security.

EXECUTIVE SUMMARY

The COVID-19 pandemic is fundamentally reshaping many aspects of business operations, including the way that organizations support and secure a large remote workforce. While there are many lenses through which to explore this transformation, connected devices—including Internet of Things (IoT) devices—and the ways in which people and organizations interact with them tell a story all their own. This report analyzes trends in device connectivity and communications in the time of COVID-19, and explores how those trends reveal not only the state of work during the COVID-19 crisis, but also the complexity and risks of connected devices.



INTRODUCTION

In March 2020, as COVID-19 infections accelerated, the worldwide labor force underwent a rapid and large-scale shift. Tens of Millions of employees transitioned to remote work almost overnight, while others were furloughed or lost their jobs as businesses closed. Beyond these already severe challenges, this situation will continue to impact every aspect of how businesses, government agencies, and other organizations operate—including cybersecurity.

While there has been a lot of focus on the security implications of remote work, as well as the uptick in phishing scams and brute force attacks looking to take advantage of vulnerable employees and configurations, there has been relatively little focus on the implications of this transition for connected devices and especially IoT.

Using anonymized, aggregate data from across our global customer base, ExtraHop analyzed business-related device activity during a one-week period at the end of March 2020. We compared this activity against a similar study conducted in November 2019. The results reveal not only patterns that illuminate the state of work during the COVID-19 crisis, but also underscore the complexity and risks of IoT and other connected devices.

TABLE OF CONTENTS

The Data in Perspective 4

IP Phones, Printers, and Critical Vulnerabilities 4

The Lights Are On, But Nobody's Home 5

"Hey Siri, is Alexa online?" 6

A Security Catch-22 6

Um, Treadmills? 7

The Future of Security 8

A Note on Data Sourcing 9

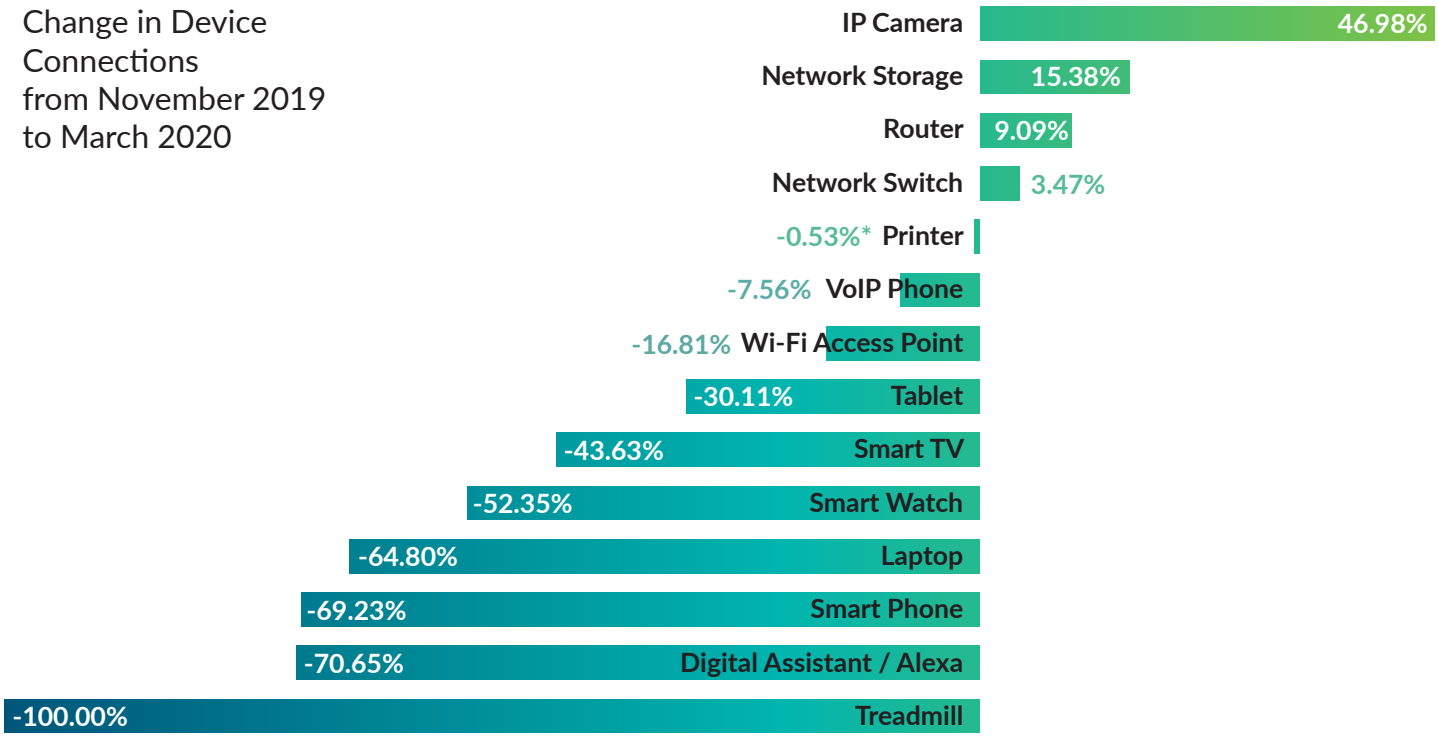
THE DATA IN PERSPECTIVE

There are a couple things worth noting regarding the data analysis below.

First, the number of ExtraHop-monitored networks reporting data increased by 89 percent between November and March. This means that many more sensors were reporting on observed devices when the new data was recorded in March. To provide a more accurate assessment of the effect of COVID-19 on device usage, unless otherwise noted below, we limited the data to device IDs present in both the November and March data.

Second, the scale of this data set is significant. ExtraHop analyzes 4 petabytes of data collected from over 15 million devices and workloads each day across cloud, data center, and remote site deployments. This intelligence is derived from that data set.

Change in Device Connections from November 2019 to March 2020



IP Phones, Printers, and Critical Vulnerabilities

In April 2020, researchers at Tenable uncovered a critical vulnerability (CVE-2020-3161) impacting the web server on specific models of Cisco IP phones that, if exploited, could enable an unauthenticated remote actor to execute code with root privileges or launch a denial-of-service (DoS) attack.

According to reporting by ThreatPost, the vulnerability ranks 9.8 out of 10 on the Common Vulnerability Scoring System (CVSS) scale. While Cisco issued a patch on April 15, it turns out that shutting down vulnerable devices or applying the patch may be easier said than done.
Looking at device counts, during March ExtraHop observed just a 7.5 percent decline in VoIP phones connected to the network. This means that, although people aren't in the workplace,

relatively few office IP phones have been disconnected. In light of the vulnerability, we also looked at how many of the observed VoIP devices were Cisco devices. As it turns out, roughly 25 percent of all phones ExtraHop identified in March were potentially impacted by the flaw.

25%
of all phones Extrahop identified were potentially impacted by the flaw

But it's not just VoIP. According to the data we observed, the vast majority of enterprise printers remain on and connected to the network, with connections between November and March declining by just 0.53 percent. Printers have long been a target for hackers, and for good reason. According to a 2019 study by NCC Group, there were 49 vulnerabilities uncovered in the drivers and software running on the top six enterprise printer brands.

The challenge here is two-fold. First, there's the fact that many of these IP phones and printers in the office are still on and connected at a time when it may not be possible for anyone to physically disconnect them. While patching devices can be done remotely, many IT teams have other priorities that may seem more pressing than applying a patch to devices in the corporate office.

The bigger cause for concern is actually what happens if and when these types of devices start connecting over employee networks. As organizations look for ways to better enable remote workforces, many are shipping IP phones to remote workers. This complicates the maintenance process substantially. While remote updates are theoretically possible, they're complicated by lack of direct access to the device on a trusted network (e.g., being able to obtain the firmware via TFTP for the install process). In many cases, individual employees will need to install updates or apply patches themselves, and many, if not most, lack the technical skills required. This means that critical updates may not be applied properly or in a timely manner, leaving network resources exposed.

The Lights Are On, But Nobody's Home

Two of the most common device types we see connecting on the network are laptops and smartphones, and that should come as no surprise. Many employees rely on these devices to do their jobs, and not just for communication. Smartphones are now broadly used as mobile point-of-sale devices in retail operations. In healthcare settings, they're used to dictate notes, review diagnostic imaging, and even act as diagnostic tools.

Of course, as businesses shift employees to remote work, retail operations shut down, and non-emergency medical visits cease, the number of devices connecting to the network has changed.

In networks where over-time comparison was possible, ExtraHop observed a 65 percent decline in the number of laptops and a nearly 70 percent decline in the number of smartphones connecting directly to customer networks from November 2019 to March 2020. Those figures align closely to data from the recent CSO Pandemic Impact Survey, which found that the number of employees working at least 60 percent of the time from home increased to more than 77 percent in late March.

That said, the fact that these devices are no longer connected to the corporate network doesn't mean they aren't connected at all. Employees working from home are still accessing corporate resources, whether via the cloud, a virtual desktop, or VPN. In many cases, these employees are connecting from questionably secure local networks that lack the safeguards of the office network and thus are more exposed to malware. Remote access technology itself also expands the potential attack surface, as VPN and other remote access infrastructure can be compromised.

And that's to say nothing of the explosion in phishing, social engineering, and other cybercrime aimed at taking advantage of vulnerable remote employees and the Help Desk staff that support them.

350%
Increase in Phishing Scams in Q1 2020

- Google

According to Google, new phishing scams increased by 350 percent between January and the end of March, with a large number using domain names that included terms like coronavirus, COVID-19, and pandemic in order to play on and exploit the public anxiety surrounding the virus. Even more concerning, the use of encryption in phishing scams continues to grow. According to PhishLabs, by the end of 2019, roughly 75 percent of all phishing sites were using SSL certificates. This practice makes it more likely that individuals will consider the site a trusted source, and makes it harder to track activity once the attacker has found their way inside.

"Hey Siri, is Alexa online?"

Another interesting data point related to smartphones and other portable devices is the sharp drop off in digital assistant devices and services. When compared against the November 2019 data, activity from digital assistants like Alexa, Siri, Google, etc. is down over 70 percent. This activity dropoff aligns closely to what we're seeing across laptops and smartphones and is what we might expect—devices that function solely based on their interaction with people ("Hey, Alexa…") should see a dropoff in activity with fewer people around.

A Security Catch-22

With offices sitting empty, many businesses seem to have bulked up their physical security measures. The March data indicates a 47 percent increase in the number of IP cameras on the network, indicating that many organizations are taking additional precautions against physical intrusion or nefarious activity.

But cameras themselves can be a weak point when it comes to cybersecurity. In a security advisory issued in 2019, ExtraHop recounted an incident involving a security camera set up by an employee at a large multinational food services company. During a data review with ExtraHop, the customer noticed that approximately every 30 minutes, a network-connected device was sending UDP traffic out to a known bad IP address. The activity was taking place during normal working hours. As it turned out, the device in question was a Chinese-manufactured security camera—likely set up independently by an employee at their office for personal security purposes. The camera was phoning home to a known malicious IP address in a foreign country.

While the camera in this particular case was purchased, configured, and connected by an employee without the knowledge or consent of IT, there are numerous examples of security cameras having critical flaws and vulnerabilities that can leave network resources and sensitive data exposed.

It's not just servers and cloud instances, desktops and smartphones, printers and VoIP. It's now treadmills, coffee machines, and thermostats

Um, Treadmills?

Yes, treadmills. Increasingly, these staples of the gym connect to the network in order to allow users to sign in, track mileage, monitor their heart rate, and connect to health apps on smartphones and smart watches to see progress over time. When we saw that treadmill connections cratered in March, plummeting 100 percent, we weren't surprised. Office gyms were among the first aspects of the office to shut down as building management tried to limit access to areas of likely spread.

But the connectivity of treadmills underscores the extent to which every device is now a connected device. IT and security departments now have to worry about a much broader attack surface. It's not just servers and cloud instances, desktops and smartphones, printers and VoIP. It's now treadmills, coffee machines, and thermostats—a world of devices that make our lives so much more convenient yet leave us at much greater risk of exposure.

THE FUTURE OF SECURITY

As of the publication of this report, we are still in midst of COVID-19 and its repercussions—be they economic, political, social, or organizational. While much remains uncertain, it's increasingly clear that many of the changes in how people work—and the resources required to support remote work on a large scale—are here to stay for the foreseeable future, if not permanently. The transformation, while painful in its swiftness and scope, forced a change that many organizations have been exploring for some time.

Moving forward, what connects to the network may look very different. Already, the substantial decrease in connections from laptops and smartphones reveals the extent to which workforces have gone remote, and underscores the need for VPNs and virtual desktops to make access secure as well as scalable. It's also forcing a rapid acceleration of cloud adoption as organizations look for more ways to provide secure access to information and systems.

At the same time, a long-term transition to a more flexible workforce model will require security that can adapt to campus, branch, and remote work scenarios. Companies will have to find new ways to make services like VoIP available to employees in a secure and manageable way, without putting the burden of critical updates on individuals. According to research from The Ponemon Institute and Shared Assessments, over 80 percent of survey respondents believe that a breach or cyberattack caused by a third party's unsecured IoT device is very likely within the next two years. As more remote workers use their own devices or must maintain company-issued ones, that number may grow.

In some ways, this change, like the shift to remote work itself, has been a long time coming. During a panel discussion with WIRED during RSAC 2020, renowned security expert Mikko Hyppönnen had this to say: "More and more, things which are not traditional computers are connected to your network—things like printers, security cameras, coffee machines—and are used to enter networks. We are turning any device that has electricity into a server. In 20 years our kids will look at us and say 'What in the world were you thinking?'"

What our children think of our hyperconnected approach remains to be seen, but in the near term, just as office workers have shifted en masse to the home office, more and more of the management onus for things like IoT devices will shift to the individual as well. Enabling that management—and ensuring that it's being properly performed—may well play a critical role in the future of enterprise security.

A Note on Data Sourcing

The ExtraHop platform was engineered from the beginning for privacy and security. Our products passively monitor and analyze network traffic to understand the communications between all devices and applications. We then extract de-identified metadata and send it to the cloud where we apply advanced machine learning to surface everything from performance degradations to security threats to abnormal traffic patterns.

But while ExtraHop Reveal(x) can see every communication, device, and workload within a customer environment—from the cloud, to the data center, to the IoT device—that doesn't mean ExtraHop security researchers can. Our platform contains layers of redundancy designed to protect customers. If you've ever wondered why ExtraHop issues relatively few reports that mention our own customers' data, it's because we made it very hard for anyone but the customer to whom it belongs to access it. We firmly believe that's how it should be.

What we can extract from our platform is information aimed at making sure that our customers have the very best visibility and insight. Take the device data, for example. ExtraHop uses de-identified (anonymized) aggregate data to catalog device models, ensuring that all customer systems get smarter whenever a new model is seen by a Reveal(x) sensor. It puts data to work for everyone without compromising privacy or security—and that's a win-win.

ABOUT EXTRAHOP

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they can compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com