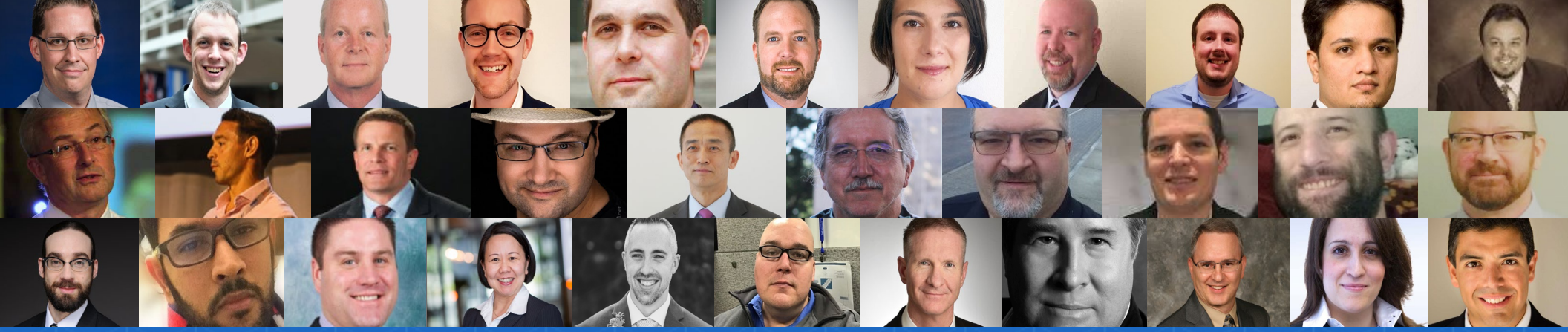


Mighty Guides

32 Security Experts

on Changing Endpoint Security

CISOs and Information Security Experts Share Their Stories Around Changing the Endpoint Security Mindset

Sponsored by Carbon Black.

INTRODUCTION: ENDPOINT SECURITY

Without a doubt, endpoint security has become an urgent priority for many organizations, and it's not hard to see why. Industry research by IDC is showing that 70 percent of successful breaches enter through an endpoint. Other research shows that more than half of companies have been hit with successful attacks, and more than three-quarters of those attacks were fileless.

For many companies, the modern business environment has become a mobile workplace in which employees work from wherever they happen to be. The fact that people continue to be the weakest security link has made mobile PCs and extended networks a sweet spot for attackers. So how are companies responding?

To find out, we drilled into the question of endpoint security with the generous support of Carbon Black. We approached 32 security experts to discuss these aspects of endpoint security:

- **Keys to shutting down attacks**
- **Rethinking your network strategy**
- **Justifying the value of endpoint security**
- **Moving to a cloud-based next-generation platform for endpoint security**

In speaking to security experts from a number of different industries, two things are clear. Endpoint security has become a critical piece of a broader security strategy, and securing the traditional network perimeter alone will not save you. One contributor observed that endpoints are in fact the new perimeter.

These essays contain useful and practical insights into evaluating endpoint security needs and implementing endpoint strategies. Regardless of how you think about the role of endpoint security in your overall strategy, I highly recommend that you read what these experts have to say.

All the best,
David Rogelberg
Publisher,
Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2017 Mighty Guides, Inc. | 62 Nassau Drive | Great Neck, NY 11021 | 516-360-2622 | www.mightyguides.com

FOREWORD: ENDPOINT SECURITY

Everyday companies put more of their assets in digital form. Healthcare records, retail purchases and personnel files are just some of the many examples of how our entire lives have moved online. While this makes our interconnected lives more convenient, it also makes them more vulnerable to attack. The monetary benefits of exploiting these vulnerabilities have created an extremely profitable underground economy; one that mimics the same one we all participate in and has led to an increase in the sophistication and frequency of attacks.

At the same time, mobility and cloud are changing the security landscape. We've moved from a centralized to a decentralized model as end users increasingly work on-the-go and access critical business applications and resources from anywhere. As such there is more emphasis on the endpoint and individual identities - from both the defender and the attacker - than ever before.

As endpoints become smarter, new challenges emerge: emerging ransomware and 0-day exploits infect all kinds of systems with ease, while many attackers use no malware at all to accomplish their malicious goals. With all this change, we spoke to 32 leading security experts to identify what's working and how they've influenced their organization to make the necessary changes before becoming the next victim.

Regards,
Mike Viscuso
CTO and Cofounder of Carbon Black

Carbon Black.

Carbon Black (NASDAQ:CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. To learn more about Carbon Black visit www.carbonblack.com.

Download the full e-book: Changing Endpoint Security

Solutions now are almost doing real-time forensics at the endpoint.

Tweet this Quote | Share on LinkedIn

Twitter | LinkedIn

ROBERT HOOD

Security Solutions Architect, BJ's Wholesale Warehouse Club

Download the full e-book: Changing Endpoint Security

You're judged on how you respond to an incident. Early detection and quick response are key to that.

Tweet this Quote

Share on LinkedIn

Website | LinkedIn

WAYNE PETERSON

Chief Information Security Officer, Kroll Associates, Inc

Download the full e-book: Changing Endpoint Security

Early detection and response often minimizes the damage as it reduces the time an attacker has to infiltrate the next security measure.

Tweet this Quote

Share on LinkedIn

Twitter | LinkedIn

CHAD STORM

Cloud Network Security Engineer at IBM,
Global Team Lead, IBM

Download the full e-book: Changing Endpoint Security

It's important to be on the lookout for any abnormal behavior before an attack can escalate or expand across the organization.

Tweet this Quote

Share on LinkedIn

Twitter | LinkedIn

SCOTT SAUNDERS

Cyber Security Consultant, Exelon

Download the full e-book: Changing Endpoint Security

Whether it's an attack or a phishing email, the earlier you detect and respond the less of an impact it's going to have.

Tweet this Quote | Share on LinkedIn

Twitter | Website | LinkedIn

SCOTT HARRIS

Vice President – Chief Information Security Officer, Lockton Companies

Download the full e-book: Changing Endpoint Security

Security and prevention are a very difficult sell. I have found using media reports of hacking that has destroyed companies and their top management in one fell swoop to be quite effective.

Tweet this Quote | Share on LinkedIn

Twitter | Website

OMAR TODD

Technical Director (CTO/CIO), Sea Shepherd Conservation

Download the full e-book: Changing Endpoint Security

The endpoint is kind of the perimeter for a lot of offices now.

Tweet this Quote | Share on LinkedIn

Twitter | Blog | LinkedIn

KEVIN FIELDER

CISO, Just Eat

Download the full e-book: Changing Endpoint Security

A good mix of prevention and detection is optimal.

Tweet this Quote

Share on LinkedIn

LinkedIn

AARON LENNON

Security Architect, Critical Start

Download the full e-book: Changing Endpoint Security

As more of our IT resources shift to the cloud, and more workers become mobile, the importance of endpoint security increases.

Tweet this Quote | Share on LinkedIn

Website | LinkedIn

ELLIOTT BREUKELMAN

Senior Information Security Engineer, Land O'Lakes, Inc.

Download the full e-book: Changing Endpoint Security

Early detection and response is as important as having locks on your doors and windows.

Tweet this Quote

Share on LinkedIn

LinkedIn

CLINT MENZIES

Senior Cyber Threat Engineer, Cyber Threat Detection & Response, Trustwave Managed Security Services

Download the full e-book: Changing Endpoint Security

My usual approach is to define a baseline security posture for the system.

Tweet this Quote

Share on LinkedIn

LinkedIn

ALINA SARVEY

Endpoint Security Engineer, Managed Security Services Provider

Download the full e-book: Changing Endpoint Security

There are certainly metrics that one can use to detect whether the endpoint is the root cause or is involved in some way.

Tweet this Quote | Share on LinkedIn

Twitter | LinkedIn

PAUL HEFFERNAN

CISO, Unipart Group

Download the full e-book: Changing Endpoint Security

Evaluate the current state of the endpointsecurity posture: What are the gaps and where can it be improved?

Tweet this Quote | Share on LinkedIn

Twitter | LinkedIn

CARY DAHL

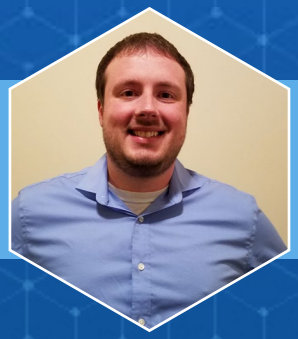
SHI, Principal Architect – Cloud & Security Solutions

Download the full e-book: Changing Endpoint Security

You need to structure your endpoint strategy so that you can leverage what it is delivering.

Tweet this Quote

Share on LinkedIn



LinkedIn

KALIN KINGSLAND

Sr. Security Architect, Global Financial Services Organization

Download the full e-book: Changing Endpoint Security

When it comes to security, a layered approach is the best way to protect.

Tweet this Quote

Share on LinkedIn

LinkedIn

CRAIG WILLIAMS

Security Design Architect, AOS

Download the full e-book: Changing Endpoint Security

With a strategic approach, you could solve an important problem that you really have, not just a threat you have identified in your program.

Tweet this Quote

Share on LinkedIn

LinkedIn

BRENT MAHER

CISO, Johnson Financial Group

Download the full e-book: Changing Endpoint Security

We now have a metric that proves my team spends less time chasing those incidents.

Tweet this Quote

Share on LinkedIn

LinkedIn

CATHARINA BUDIHARTO

Director, Information Security, CB&I

Download the full e-book: Changing Endpoint Security

A lot of the work that starts on one of our developers' laptops impacts our platform because we operate in a DevOps lifecycle.

Tweet this Quote

Share on LinkedIn

LinkedIn

HARSHIL PARIKH

Director of Security, Medallia, Inc

Download the full e-book: Changing Endpoint Security

I can't begin to stress how important early detection and response is when it comes to mitigating threats and minimizing damage.

Tweet this Quote

Share on LinkedIn

LinkedIn

AHMER BHATTY

Field Solutions Engineer - Networking and Security, SHI International Corp.

Download the full e-book: Changing Endpoint Security

It's especially helpful to present security information in the form of metrics and useful data points.

Tweet this Quote
Share on LinkedIn

Website | LinkedIn

MIKE SANTOS

Director of Security & Information Governance, Cooley LLP

Download the full e-book: Changing Endpoint Security

You've got to get those logs off the endpoint in near real time so you don't lose visibility to hackers cleaning up after themselves.

Tweet this Quote

Share on LinkedIn

LinkedIn

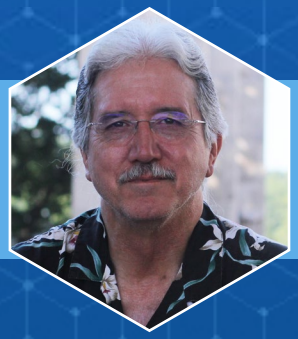
CHRIS THOMPSON

Global Director, IT Security and Controls, Bentley Systems

Download the full e-book: Changing Endpoint Security

Never waste a breach. Use the cost of recovering from a previous breach to emphasize the ROI of doing things ahead of time.

Tweet this Quote | Share on LinkedIn



Twitter | Website | Blog | LinkedIn

RANDY MARCHANY

Chief Information Security Officer, Virginia Tech

Download the full e-book: Changing Endpoint Security

Honestly, it is extremely trivial in many cases to bypass antivirus.

Tweet this Quote
Share on LinkedIn

Twitter | Website | LinkedIn

RICHARD DAVIS
Executive Director of IT Security,
Embry-Riddle Aeronautical University

Download the full e-book: Changing Endpoint Security

We're able to log event information to prove compliance, and we can also analyze how effective our controls actually are.

Tweet this Quote

Share on LinkedIn

LinkedIn

BRIAN TIMMENY

Global Head of Advanced Engineering, DevOps, Engineering Processes, BBVA

Download the full e-book: Changing Endpoint Security

Prevention is great, but detection is an absolute must.

Tweet this Quote

Share on LinkedIn

LinkedIn

CHRISTOPHER LAJINESS

Sr. Systems Engineer, Symantec

Download the full e-book: Changing Endpoint Security

Many of these technologies can help us answer a lot of questions more easily now than we could in the past.

Tweet this Quote | Share on LinkedIn

Twitter | LinkedIn

DAN BOWDEN

VP & CISO, Sentara Healthcare

Download the full e-book: Changing Endpoint Security

Business is transforming to a point where most user endpoints aren't inside the infrastructure.

Tweet this Quote | Share on LinkedIn

Twitter | Website | LinkedIn

DAVID MERRILL

Senior Director, Travelers Insurance

Download the full e-book: Changing Endpoint Security

Effectively identifying the most severe cybersecurity threat and mitigating the most impactful attacks are imperative for cyber defense.

Tweet this Quote | Share on LinkedIn

Twitter | LinkedIn

CHARLES LI

CTO, Integration and Innovation Lead,
IBM GBS Cyber Security and Biometrics

Download the full e-book: Changing Endpoint Security

You need to think about how you are going to manage whatever you deploy.

Tweet this Quote

Share on LinkedIn

LinkedIn

JOHN MEAKIN

CISO, Formerly Burberry

Download the full e-book: Changing Endpoint Security

It really falls upon the security professional to understand the business, and then understand the front landscape around it.

Tweet this Quote | Share on LinkedIn

Twitter | LinkedIn

DANIEL SCHATZ

CISO, Perform Group

Download the full e-book: Changing Endpoint Security

There will be a continued industry-wide shift from prevention only security strategies in favor of detection and response.

Tweet this Quote

Share on LinkedIn

Website | LinkedIn

BRIAN HUSSEY

VP of Cyber Threat Detection & Response, Trustwave

Download the full e-book: Changing Endpoint Security

You have to be able to trust the results. You want a company that demonstrates it can obtain information and control everything all around the world.

Tweet this Quote | Share on LinkedIn

Twitter | Website | Blog | LinkedIn

ISABEL MARIA GOMEZ

Group Information Security Manager, Bankia