EBOOK

Protecting endpoints everywhere

Your first and last line of defense for today's threats

cisco Port53 Technologies

In this ebook

49%
of the workforce
is mobile.

82%
of corporate laptop users
bypass VPNs.

70%
increase in SaaS usage
in next 2 years.

68%
of workloads will be in
public cloud data
centers by 2020.

69%
of branch offices have
direct-to-internet access.

Security can't wait any longer; it needs to evolve now.

The world of work has changed — radically. With more unmanaged devices connecting to the network and more users working from anywhere, security gaps are widening.

IT teams have less visibility while employees have more control than ever before over the applications they use, and where they use them. Many of those applications have moved to the cloud, letting remote and roaming employees bypass the VPN. Those same cloud apps make it easy to collaborate and share information, not just within your company but with outside collaborators, too.

With critical infrastructure, applications, and sensitive data now stored in the cloud, attackers have even more incentive to target endpoints as their easiest point of entry. With ransomware on the rise, and more branch offices having direct-to-internet access, the question remains: Why are we treating today's new challenges with yesterday's approach to security? Security can't wait. It's time to take action.

"By 2018, Gartner estimates that 25% of corporate data traffic will bypass perimeter security and flow directly from mobile devices to the cloud."

– Predicts 2017: Network and Gateway Security

The threat on endpoints is massive.

The way we work isn't the only thing that has evolved. Security threats have changed, too. Today, an estimated 70% of breaches originate on endpoint devices.6 Why are endpoints the primary point of entry for attacks?

- Gaps in protection. When users and endpoints are off-network, antivirus is often the only protection available. But signature detection and preventive measures aren't enough to handle today's advanced threats, including zero-day exploits.

  65% of organizations say attacks evaded preventive tools.

- Lack of visibility. Organizations have limited visibility into user and endpoint activity, and they lack the context to see malware — where it came from, where it's been, and what it's doing — once it lands on an endpoint. You can't detect what you can't see.

  55% of companies are unable to determine the cause of a breach.
  100 days is the industry average for time to detection.

- User error. An attacker sends out a phishing email with a malicious attachment or link. Despite training and/or countless warnings, users inevitably click on things that they shouldn't.

  48% of attackers bypass endpoint defenses due to user error.

Visibility, context, and control for users, files, and internet.

It's time for effective security that's simple, open, and automated.

Attackers are getting smarter, faster, and harder to catch. Ransomware in particular has grown into a billion-dollar industry as targeted attacks become more frequent. And according to Gartner, through 2020, more than 50% of ransomware will focus on the disruption of business rather than the encryption of data.

The evolution of how we work and the evolution of internet threats together add up to a new reality for IT. You can no longer rely on network-level protections alone to keep your data secure. Traditional security can't extend protection to mobile users or handle the exponential increase in internet traffic. Secure web gateways, firewalls, and sandboxing are important tools — but they provide help only after an attack occurs.

Today, you need deep visibility into what users are doing on their endpoints, what's happening with the files located there, and where that endpoint is trying to connect to on the internet. And you need the control to stop malicious behavior as soon as it's detected. Fortunately, security has evolved to meet these challenges with solutions that are simple, open, automated, and effective.

Protect every endpoint, everywhere.

Cisco Umbrella

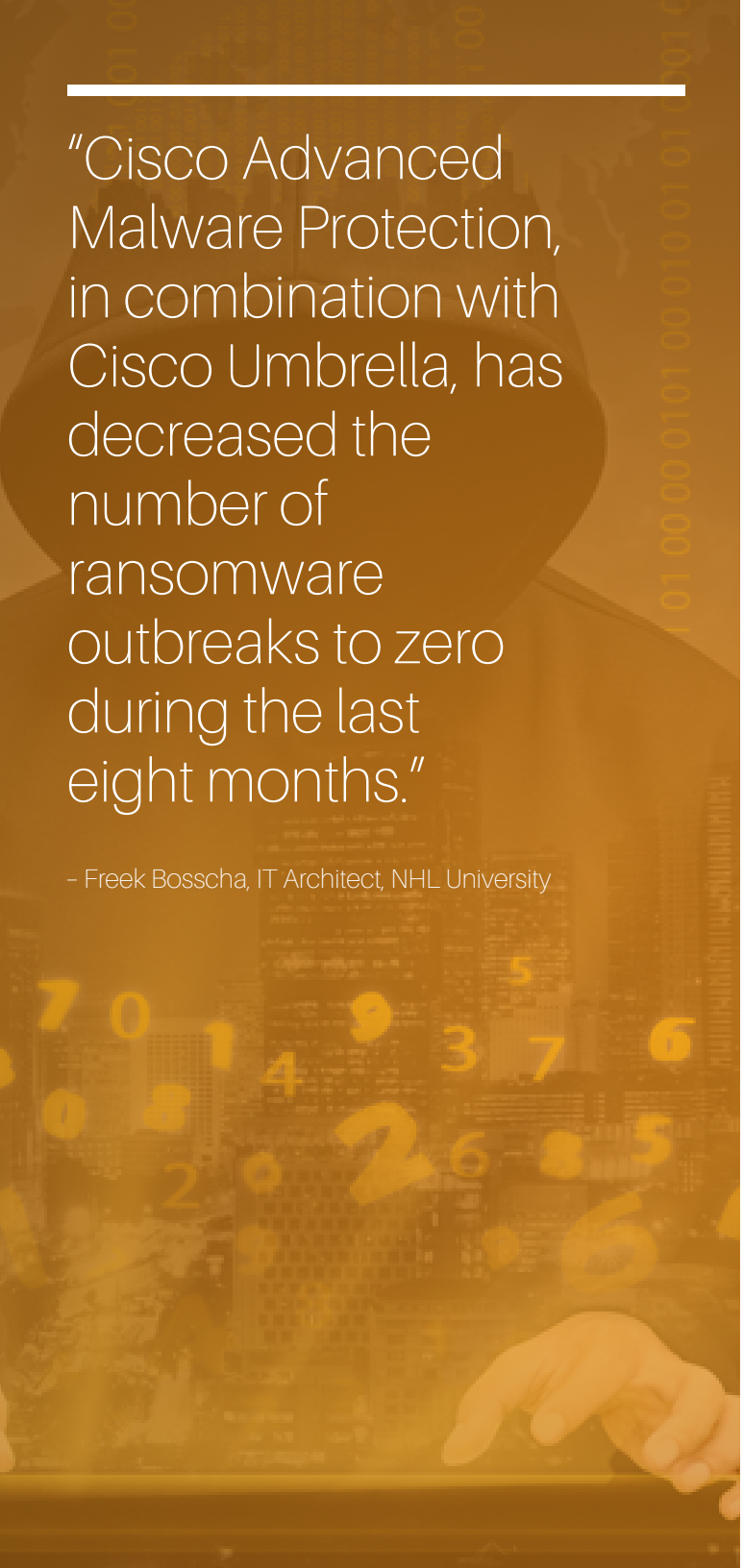
Umbrella is a cloud security platform that provides your first line of defense against threats hosted on the internet, whether your users are on or off the corporate network. Umbrella gives you complete visibility into internet activity across all locations and endpoints. Plus, it monitors and analyzes attacker infrastructure to identify and proactively block malicious requests before a connection is even established. With a massive global DNS network and intelligent proxy, Umbrella helps you stop attacks earlier, identify already infected devices faster, and prevent data exfiltration.

Cisco AMP for Endpoints

AMP for Endpoints is cloud-managed, next-generation endpoint security that analyzes unknown files and automatically blocks malware from trying to run on endpoints. It continuously monitors and records all file activity on endpoints, regardless of file disposition, to quickly spot malicious behavior. AMP then shows the complete recorded history of the malware's behavior over time — where the malware came from, where it's been, and what it's doing, enabling you to retrospectively detect and remediate threats once thought to be benign.

"We have much greater confidence in the security of our endpoints with Cisco Umbrella combined with Cisco AMP. We have had zero malware infections since our implementation three years ago."

– Engineer, Medium Enterprise Financial Services Company



"Cisco Advanced Malware Protection, in combination with Cisco Umbrella, has decreased the number of ransomware outbreaks to zero during the last eight months."

– Freek Bosscha, IT Architect, NHL University

A one-two punch against malware.

Cisco AMP for Endpoints and Cisco Umbrella are two security solutions that work in harmony to provide the visibility, context, and control needed to prevent, detect, and respond to attacks targeting endpoints, before damage can be done.

Together, Umbrella and AMP for Endpoints provide your first and last lines of defense for today's threats, anywhere users go.

Prevent

Umbrella

Blocks malicious internet requests (domain, URL, and IP), regardless of delivery mechanism (email, web, drive-by, etc.)

AMP for Endpoints

Blocks known malware at initial inspection
Uses sandbox to analyze unknown files

Detect

Umbrella

Prevents command and control (C2) callbacks to attacker's servers to stop data exfiltration and execution of ransomware encryption

AMP for Endpoints

Continuously analyzes all file activity on endpoints to quickly detect malicious behavior and alert security teams

Respond

Umbrella

Provides up-to-the-minute threat data and historical context about domains, IPs, and file hashes for faster investigation

AMP for Endpoints

Shows the full history and context of a compromise to inform security decision-making
Can stop attacks via outbreak control capabilities and quarantining files

Avoid the aftermath with a before strategy.

To secure against ever-evolving threats across an ever-increasing attack surface, you need more than one line of defense. Backed by industry-leading Talos threat research, Cisco Umbrella and Cisco AMP for Endpoints give you seamless protection from the DNS layer to the endpoint. Together, they provide the visibility and control you need to keep users safe against malware, phishing, and command-and-control callbacks — wherever they go and whichever devices they use.

Ready to add a one-two punch to your security portfolio?

Contact a Port53 rep to learn more about Cisco AMP for Endpoints.

Or give Cisco Umbrella a try. It's free for 21 days.

START YOUR TRIAL

Sources:
1. "Secure Portable Data and Applications," SANS, 2015
2. IDG Research Services Market Pulse: "The Need for Off-Network Security," May 2016
3. "Keeping SaaS Secure," Gartner, 2016
4. Cisco Global Cloud Index: Forecast and Methodology, 2015–2020
5. "Secure Direct-to-Internet Branch Offices: Cloud-Based Security Offers Flexibility and Control," Forrester, 2015
6. Effective Incident Detection and Investigation Saves Money, IDC, 2016
7. A Year of Mega Breaches, Ponemon Institute, 2015
8. Cisco Annual Security Report, Cisco, 2016
9. Exploits at the Endpoint: SANS 2016 Threat Landscape Survey
10. "Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest," Newsweek, May 23, 2017
11. Simple Lessons You Must Learn from WannaCry, Ian McShane, Gartner, June 29, 2017