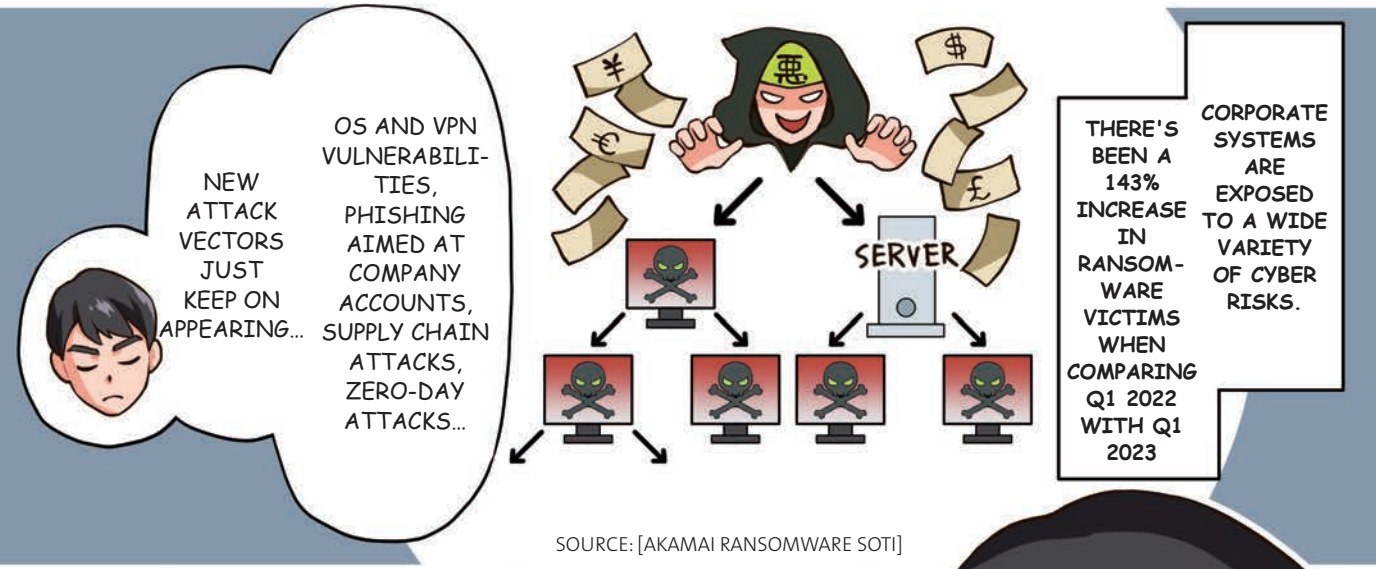
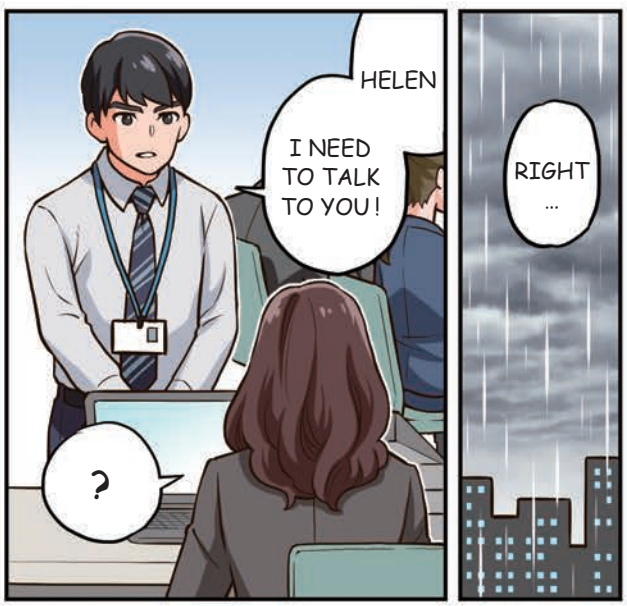
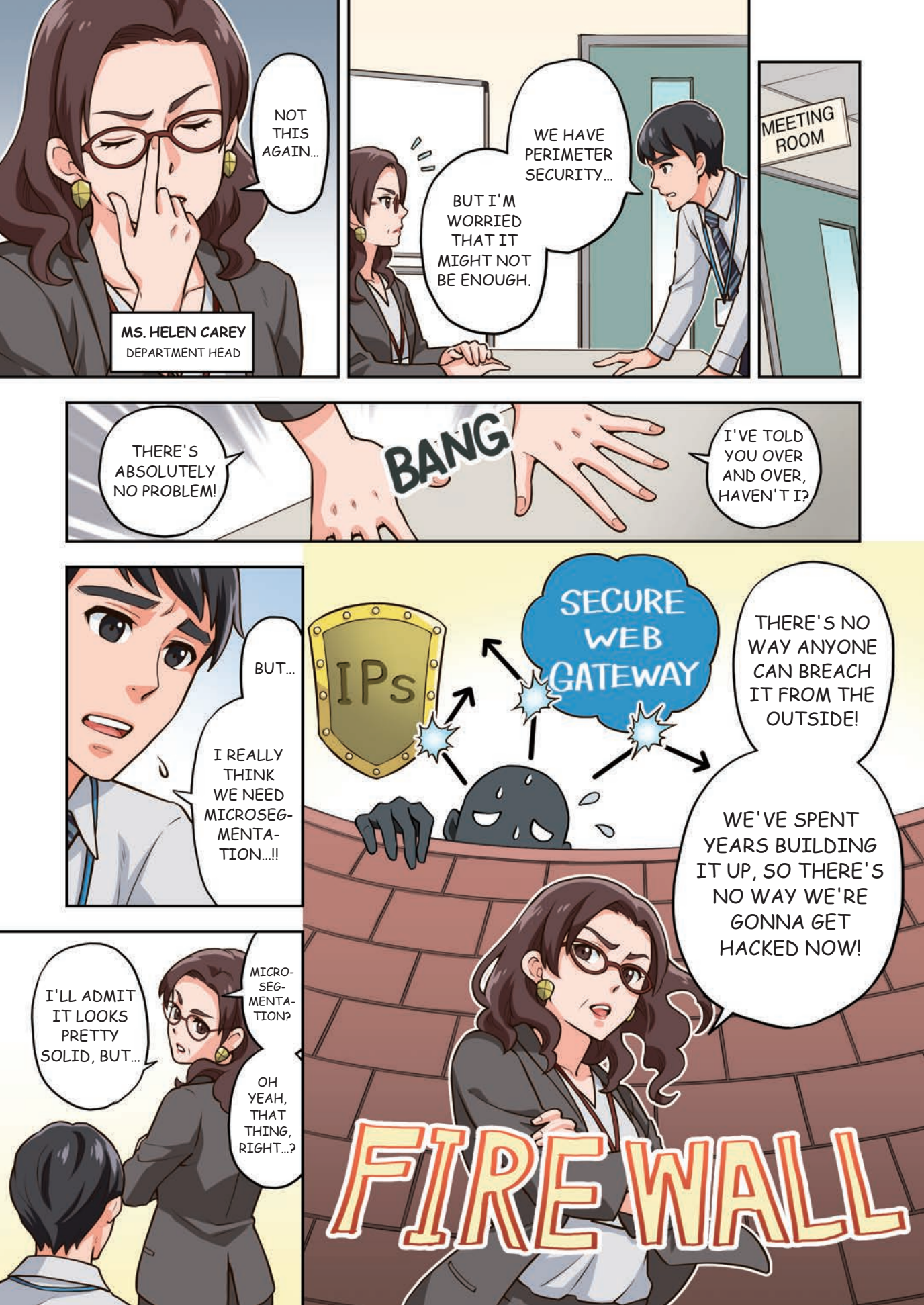

Akamai
アカマイ
MI-SEG
マイセグ
HOW TO PROTECT YOUR DATA IN THE ZERO TRUST AGE

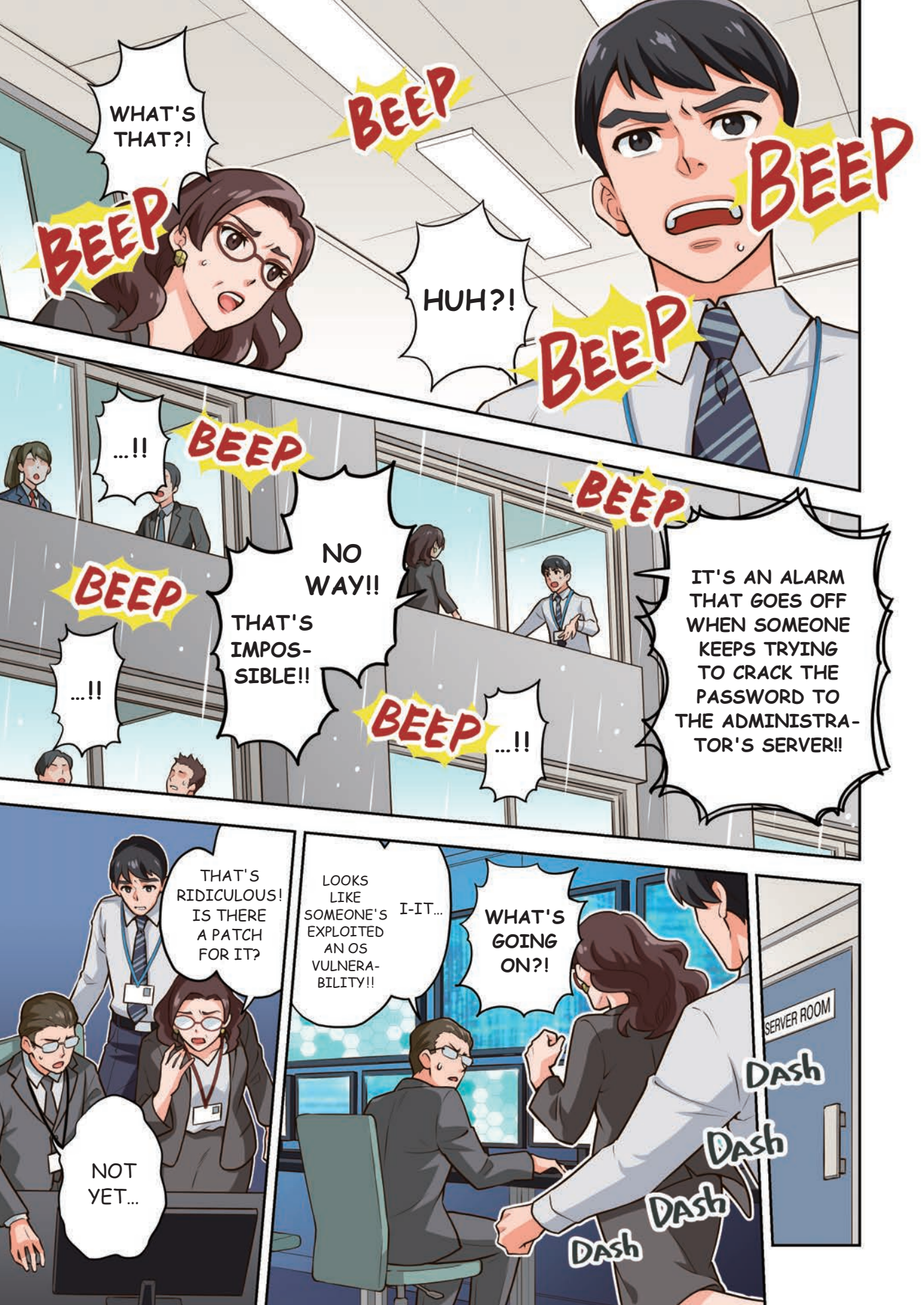


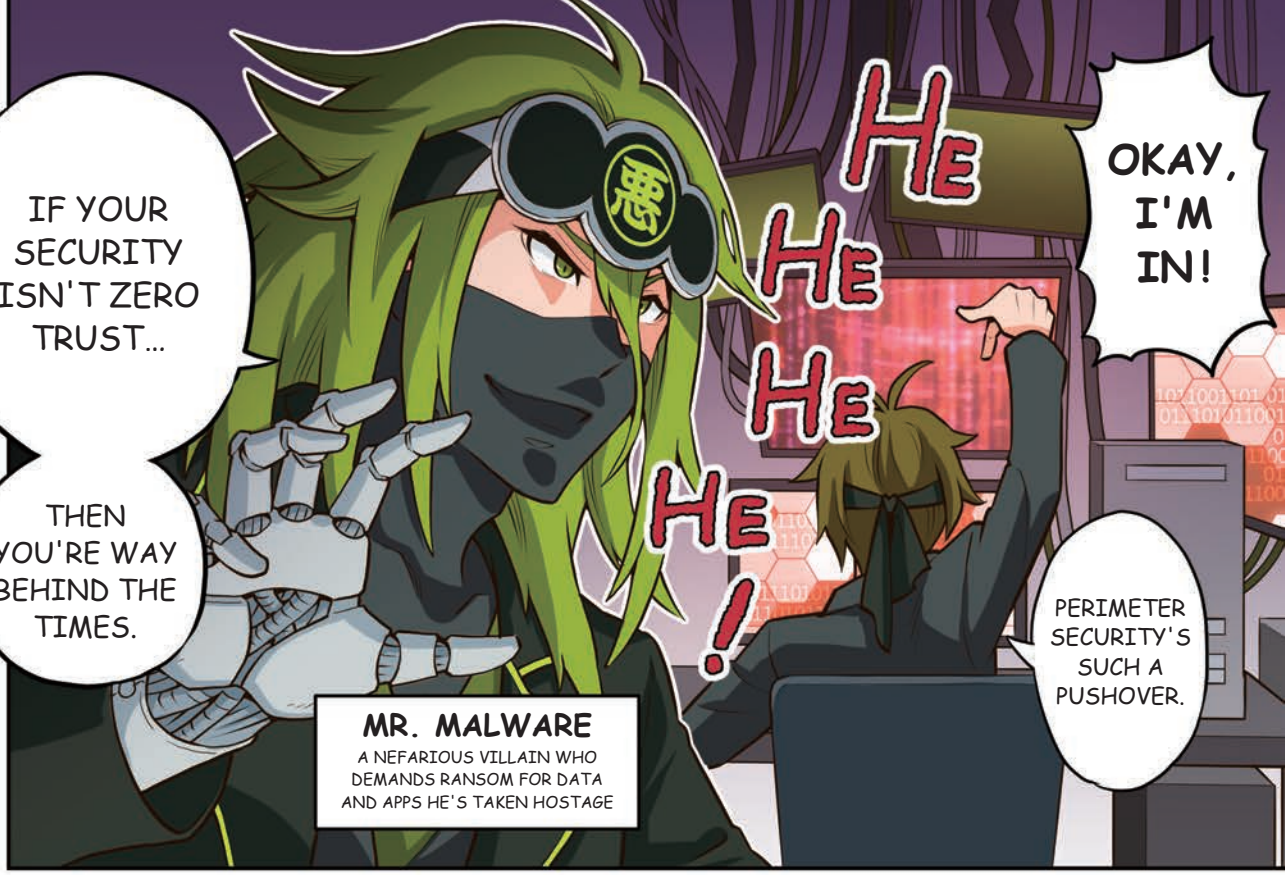
SOURCE: [AKAMAI RANSOMWARE SOTI]

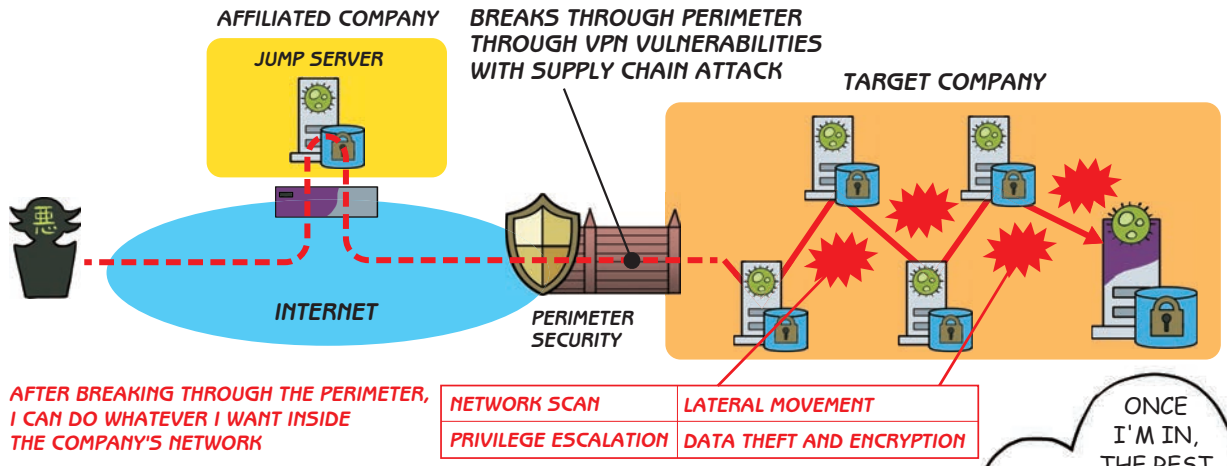



NOT THIS AGAIN...
MS. HELEN CAREY
DEPARTMENT HEAD
WE HAVE PERIMETER SECURITY...
BUT I'M WORRIED THAT IT MIGHT NOT BE ENOUGH.
MEETING ROOM
THERE'S ABSOLUTELY NO PROBLEM!
BANG
I'VE TOLD YOU OVER AND OVER, HAVEN'T I?
BUT...
I REALLY THINK WE NEED MICROSEG-MENTA-TION...!!
IPs
SECURE WEB GATEWAY
THERE'S NO WAY ANYONE CAN BREACH IT FROM THE OUTSIDE!
WE'VE SPENT YEARS BUILDING IT UP, SO THERE'S NO WAY WE'RE GONNA GET HACKED NOW!
I'LL ADMIT IT LOOKS PRETTY SOLID, BUT...
MICRO-SEG-MENTA-TION?
OH YEAH, THAT THING, RIGHT...?
FIREWALL


STARE
...ARE YOU SAYING EVERYTHING I'VE DONE SO FAR ISN'T GOOD ENOUGH?
UMM...
BOSS...!
O-OF COURSE NOT!
BUT OUR SYSTEMS ARE MOVING TO THE CLOUD, AND OUR PEOPLE ARE WORKING ALL OVER
THE PLACE WHAT WITH REMOTE WORK AND SO ON, SO OUR APPS
AND OUR STAFF ARE ALL WIDELY SCATTERED ABOUT OUTSIDE OUR PERIMETER
CLATTER...
YEAH, YEAH. THIS CONVER-SATION'S OVER!
"SO YOU ALREADY KNOW ABOUT MICROSEGMENTATION, HUH...?"
HUH?!
WH-WHO'S THERE?

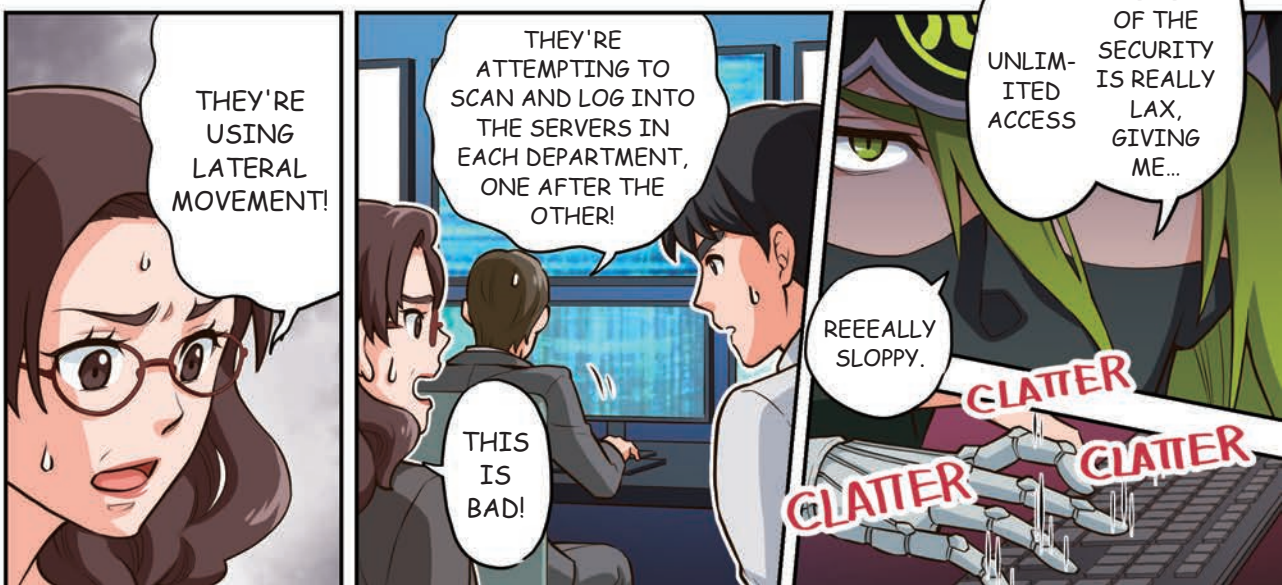

WHAT'S THAT?!
BEEP
BEEP
BEEP
HUH?!
BEEP
BEEP
...!!
BEEP
BEEP
NO WAY!!
THAT'S IMPOS-SIBLE!!
BEEP
...!!
BEEP
...!!
IT'S AN ALARM THAT GOES OFF WHEN SOMEONE KEEPS TRYING TO CRACK THE PASSWORD TO THE ADMINISTRA-TOR'S SERVER!!
THAT'S RIDICULOUS! IS THERE A PATCH FOR IT?
NOT YET...
LOOKS LIKE SOMEONE'S EXPLOITED AN OS VULNERA-BILITY!!
I-IT...
WHAT'S GOING ON?!
SERVER ROOM
Dash
Dash
Dash
Dash



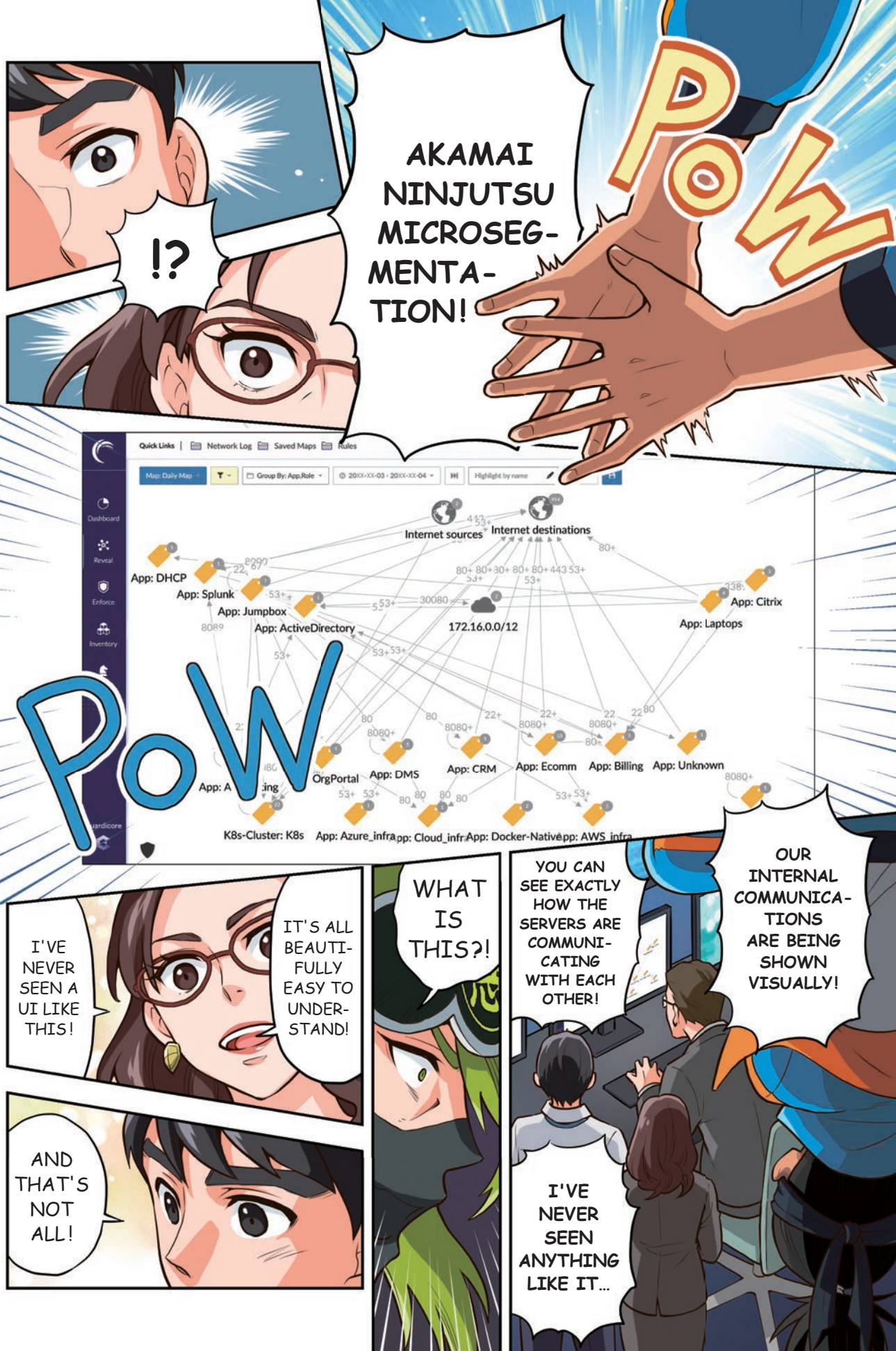


AFTER BREAKING THROUGH THE PERIMETER, I CAN DO WHATEVER I WANT INSIDE THE COMPANY'S NETWORK

NETWORK SCAN	LATERAL MOVEMENT
PRIVILEGE ESCALATION	DATA THEFT AND ENCRYPTION



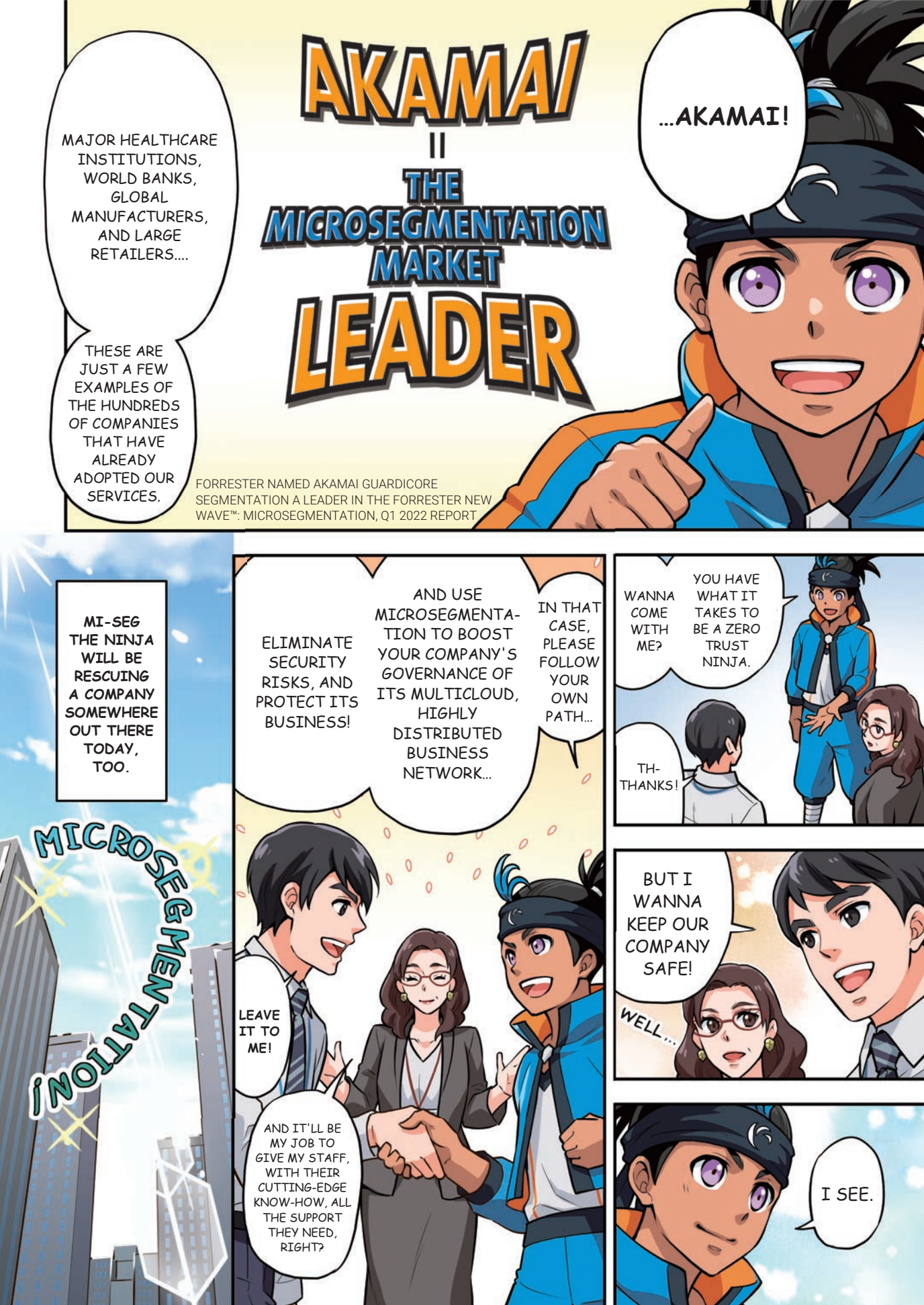

INFORMATION ON NEW PRODUCTS
INFORMATION ON CLIENTS
FINANCIAL DOCUMENTS
THE LONG-TERM BUSINESS STRATEGY
...THAT MEANS...
AT THIS RATE, THEY'LL GET ACCESS TO EVERY-THING!!
...THEY'LL LOCK UP THE INFORMATION AND DEMAND A HUGE RANSOM FOR IT...!!
THEY'RE GONNA GRAB THE DATA!!
OH NO!!
STOP!
HE HE HE HE HE!
OKAY, TIME TO GET ME A HOSTAGE.
HELEN!
WHAT SHOULD WE DO...?!
I'VE ABSOLUTELY NO IDEA WHAT THEY'RE HACKING INTO OR WHERE THEY'RE GOING...
STAGGER...
IT'S TOO LATE TO DO ANYTHING NOW...!


!?
AKAMAI NINJUTSU MICROSEG-MENTA-TION!
POW
Quick Links
Network Log
Saved Maps
Rules
Map: Daily Map
Group By: App,Role
Highlight by name
Dashboard
Reveal
Enforce
Inventory
Internet sources
Internet destinations
App: DHCP
App: Splunk
App: Jumpbox
App: ActiveDirectory
172.16.0.0/12
App: Citrix
App: Laptops
POW
OrgPortal
App: DMS
App: CRM
App: Ecomm
App: Billing
App: Unknown
K8s-Cluster: K8s
App: Azure_infra
App: Cloud_infr
App: Docker-Native
App: AWS_infra
I'VE NEVER SEEN A UI LIKE THIS!
IT'S ALL BEAUTI-FULLY EASY TO UNDER-STAND!
AND THAT'S NOT ALL!
WHAT IS THIS?!
YOU CAN SEE EXACTLY HOW THE SERVERS ARE COMMUNI-CATING WITH EACH OTHER!
OUR INTERNAL COMMUNICA-TIONS ARE BEING SHOWN VISUALLY!
I'VE NEVER SEEN ANYTHING LIKE IT...


YOU MEAN YOU DID ALL THIS?!
MICRO-SEGMENTATION IS ABOUT CONTROLLING YOUR SYSTEM BY LABELING THINGS,
CREATING NETWORK RULES, AND SHOWING EVERYTHING VISUALLY
WHO ARE YOU?!
THAT'S RIGHT.
CLACK
THIS IS AMAZINGLY STRONG!
EACH ASSET HAS MULTIPLE LABELS DETAILING ITS ROLE, LOCATION, AND MORE...
MICRO
...TRANSPARENT BARRIERS HAVE been PUT UP...
SEGMENTATION
I'M MI-SEG THE NINJA.
I'M A MASTER OF AKAMAI NINJUTSU—WHICH, I MIGHT ADD, IS SAID TO BE THE STRONGEST IN THE WORLD.
FWIP
...AND THERE ARE FIXED RULES ON WHO CAN TALK TO WHOM!
GASP
SO YOU'RE THAT VOICE I HEARD EARLIER...
"SO YOU ALREADY KNOW ABOUT MICRO-SEGMENTATION, HUH...?"


POLICY VIOLA-TIONS!
POW
OKAY.
I'LL LEAVE THE SELF-INTRODUC-TION AT THAT...
AND PUT A STOP TO THIS HACKER!
BZZT
A NEAT WAY TO BLOCK UNAUTHO-RIZED COMMUNICA-TIONS!!
AND THEY'RE
SHOWN IN RED...
After
Before
ONLY UNAUTHORIZED COMMUNICATIONS GET ELIMINATED,
WAAAI
悪
MY ACCESS... IT'S BEEN AUTOMATI-CALLY BLOCKED...!
BOOM!!!


I'VE COME TO SPREAD THE MOST VITAL PIECE OF TECHNOLOGY FOR THE ZERO TRUST AGE... MICRO-SEGMENTATION!
...OF AKAMAI GUARDICORE SEGMENTATION
ZERO TRUST
THAT'S THE POWER OF MICRO-SEGMENTATION...
OR I SHOULD SAY...
THE HACKER...
...HAS BEEN COMPLETELY...
...ELIMINATED!!
AND FOR THAT, WE NEED MICRO-SEGMENTATION, RIGHT?
RIGHT!
AND THE MICRO-SEGMENTATION LEADER IS...
THE CRUCIAL POINT IS TO BUILD A SYSTEM THAT WON'T LET ANY DAMAGE HAPPEN EVEN IF IT DOES GET HACKED!
I WASN'T WARY ENOUGH THAT GETTING HACKED IS BASICALLY ONLY A MATTER OF TIME.
I'M REALLY SORRY FOR BRUSHING YOU OFF EARLIER.
THAT'S OKAY...

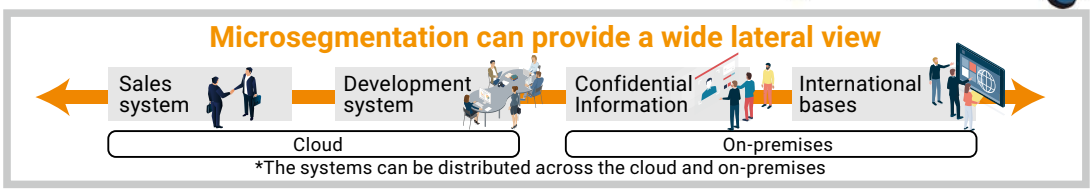

AKAMAI
=
THE MICROSEGMENTATION MARKET LEADER
MAJOR HEALTHCARE INSTITUTIONS, WORLD BANKS, GLOBAL MANUFACTURERS, AND LARGE RETAILERS....
THESE ARE JUST A FEW EXAMPLES OF THE HUNDREDS OF COMPANIES THAT HAVE ALREADY ADOPTED OUR SERVICES.
...AKAMAI!
FORRESTER NAMED AKAMAI GUARDICORE SEGMENTATION A LEADER IN THE FORRESTER NEW WAVE™: MICROSEGMENTATION, Q1 2022 REPORT
MI-SEG THE NINJA WILL BE RESCUING A COMPANY SOMEWHERE OUT THERE TODAY, TOO.
MICROSEGMENTATION!
ELIMINATE SECURITY RISKS, AND PROTECT ITS BUSINESS!
AND USE MICROSEGMENTATION TO BOOST YOUR COMPANY'S GOVERNANCE OF ITS MULTICLOUD, HIGHLY DISTRIBUTED BUSINESS NETWORK...
IN THAT CASE, PLEASE FOLLOW YOUR OWN PATH...
LEAVE IT TO ME!
AND IT'LL BE MY JOB TO GIVE MY STAFF, WITH THEIR CUTTING-EDGE KNOW-HOW, ALL THE SUPPORT THEY NEED, RIGHT?
WANNA COME WITH ME?
YOU HAVE WHAT IT TAKES TO BE A ZERO TRUST NINJA.
TH-THANKS!
BUT I WANNA KEEP OUR COMPANY SAFE!
WELL...
I SEE.

THE 3 SCROLLS OF MICROSEGMENTATION NINJUTSU

SCROLL 1

THE LATERAL CONTROL OF THE ORGANIZATION'S OVERALL SECURITY

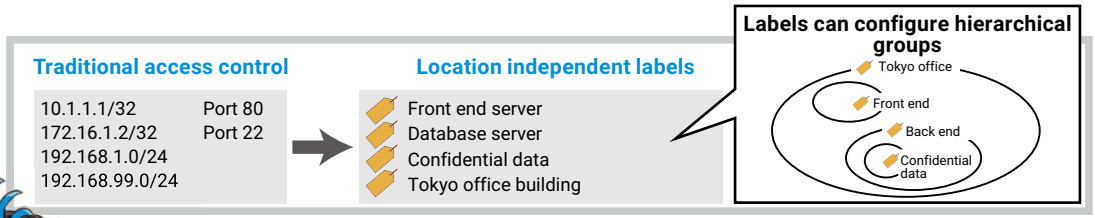
Victims of recent ransomware and APT have said, "You can't fight attackers moving laterally with organizational silos." When a company network is divided into silos, infiltrators can enter from unexpected places — such as foreign branches or supply chains of countries or affiliated companies — and access the company's assets by moving laterally. Recent IT infrastructures tend to be divided into silos, but microsegmentation can let you visualize and manage in a unified manner.



SCROLL 2

SIMPLIFY MULTICLOUD NETWORK MANAGEMENT

Do you move IT assets across locations such as on-premises, AWS, and Azure? After choosing the optimal infrastructure for each system, communication from the hybrid cloud and multicloud environments between those infrastructures can be complex. You can free yourself from needing to control complex communication from IP addresses by setting labels, which are not dependent on location. By using microsegmentation, network administrators no longer have to manage communication policies for all of the different firewalls and infrastructures.



SCROLL 3

POLICY-BASED FILTERING TO BLOCK MALICIOUS ACTORS

Microsegmentation is useful for rule-based internal communication control because it has a clear policy of determining where connections can start and end, and can reject unmanaged traffic. This can stop even attackers that can bypass detection-based solutions such as EDR and NDR. This internal access control has been provided by internal firewalls and router ACLs. However, they don't work with the modern hybrid environment. That's why microsegmentation is getting popular. Similar to how EDR evolved from antivirus solutions, microsegmentation is an evolution of internal firewalls.

Akamai Guardicore Segmentation

Stop Lateral Movement with Granular Visibility and Microsegmentation Controls

Enterprise IT infrastructure is still evolving from traditional on-premises data centers to cloud and hybrid cloud architectures, with a blend of platforms and application deployment models. Although this digital transformation is helping many organizations achieve greater business agility, reduce infrastructure costs, and enable remote work, it is also creating a larger and more complex attack surface that does not have a well-defined perimeter. Each individual server, virtual machine, cloud instance, and endpoint is now a possible point of exposure; with the prevalence of threats like ransomware and zero-day vulnerabilities, attackers are becoming more adept at moving laterally toward high-value targets when — not if — they find a way in.

Key point

Not only for microsegmentation!

Use cases are diverse and they're more than just network segmentation. It helps the business through compliance promotion, cloud migration, and more. The following are the eight most common applications that users use microsegmentation for.

USE CASES

- **Prevent Ransomware**
- **Secure Cloud Migration**
- **Achieve Zero Trust**
- **Safeguard Remote Workforce**
- **Accelerate Compliance**
- **Protect Your Endpoints**
- **Ringfence Critical Applications**
- **Replace Internal Firewalls**

KEY SOLUTION CAPABILITIES

Granular, AI-Powered Segmentation

Implement policies in a few clicks using AI recommendations, templates for remediating ransomware and other common use cases, and precise workload attributes like processes, users, and domain names

Real-Time and Historical Visibility

Map application dependencies and flows down to the user and process levels on a real-time or historical basis

Broad Platform Support

Cover modern and legacy operating systems across bare-metal servers, virtual machines, containers, IoT, and cloud instances

Flexible Asset Labeling

Add rich context with a customizable labeling hierarchy and integration with orchestration tools and configuration management databases

Multiple Protection Methods

Integrate threat intelligence, defense, and breach detection capabilities to reduce incident response time

How It Works

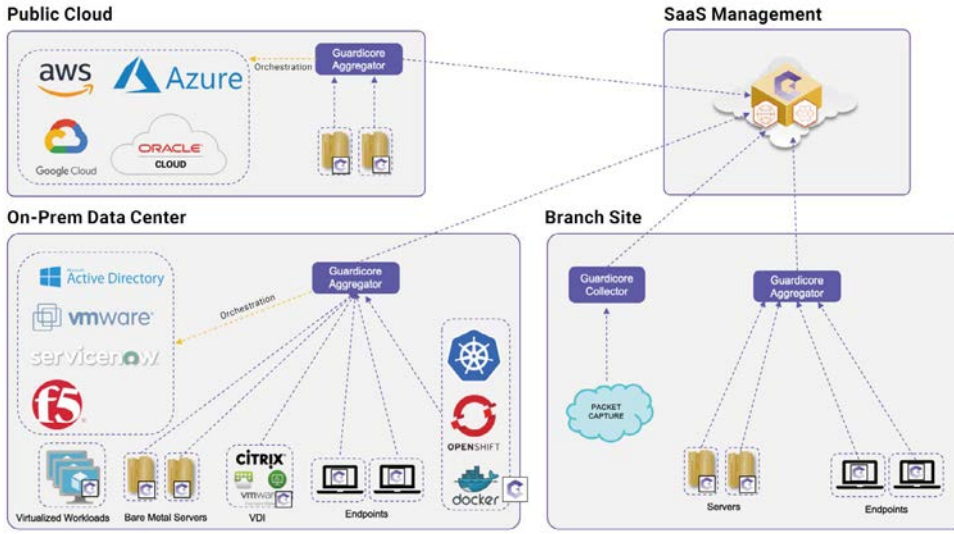
Akamai Guardicore Segmentation collects detailed information about an organization's IT infrastructure through a mix of agent-based sensors, network-based data collectors, virtual private cloud flow logs from cloud providers, and integrations that enable agentless functionality. Relevant context is added to this information through a flexible and highly automated labeling process that includes integration with existing data sources, such as orchestration systems and configuration management databases.

Key point

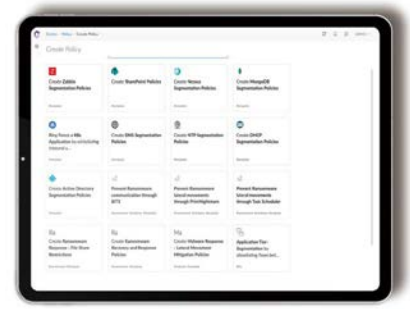
Microsegmentation can be developed anywhere!

You can deploy anywhere, whether it is on the cloud, on-premises, or on containers. By managing separate environments in a unified manner, you can greatly reduce costs and work.

INFRASTRUCTURE TOPOLOGY



Most customers utilize SaaS management, but on-premises management options are also available.



Network Map

The output is a dynamic map of the entire IT infrastructure that allows security teams to view activity with user- and process-level granularity on a real-time or historical basis. These detailed insights, combined with AI-powered policy workflows, make the creation of segmentation policies fast, intuitive, and based on real workload context.

Key point

Visualize your distributed network!

One feature of Akamai Guardicore Segmentation is the ability to visualize internal communication. It can let you see where signals are coming from and where they are going in real time, or what transactions happened in the past retroactively. It can optimize application migration and reduce time spent on incident response.

Templates

Policy creation is made easy with prebuilt templates for the most common use cases. Policy enforcement is completely decoupled from the underlying infrastructure, so security policies can be created or altered without complex network changes or downtime. In addition, policies follow the workload no matter where it resides — in on-premises data centers or public cloud environments. Our segmentation capabilities are complemented by a sophisticated set of threat defense and breach detection capabilities, as well as threat hunting services provided by Akamai's security researchers.

We can answer any questions you have

Visit our Akamai Guardicore Segmentation page to:

- **Request a product demonstration**
- **See new features and case studies**
- **Register for workshops on Zero Trust and microsegmentation**

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn.