World Wide Technology

Capture the Flag

WWT's Annual Cyber Range Event
Exclusive to Financial Services Customers

July 22, 2021

Letter from the Editor

To Our Customers, Partners, and Colleagues:

WWT has made significant investments in support of our employees and customers during these turbulent times, and, of course, cybersecurity has been no exception. As such, I am thrilled to announce our first annual Capture the Flag event and introduce our new, state-of-the-art Cyber Range, a $1M+ add-on to our Advanced Technology Center (ATC), where people can explore, test, evaluate, integrate, understand, and train with cybersecurity solutions against real-world scenarios.

Cybersecurity attacks are among the top global risks businesses face today. Putting the right safeguards in place can be costly, so we've made finding, understanding, and training on cybersecurity solutions easy and affordable. WWT's Cyber Range is a controlled cybersecurity environment that eliminates the costs of expensive infrastructure by using cloud-based access coupled with the ability to control consumption-based usage. It also serves as a cost-effective way of delivering a safe and realistic haven for training staff on micro to full-scale simulations of cyberattacks, and a safe space where cross-functional teams can work in conjunction to improve their cyber readiness and address vulnerabilities.

As part of the Cyber Range initiative, we will be hosting an annual Capture the Flag event to bring together OEMs and customers to train in a fun and competitive way. Up to 20 teams will compete head-to-head in solving practical, simulated cyber challenges. Our strategic partners will also present 20-min talks throughout the day (think, TED Talks), providing fresh and unique perspectives for security practitioners.

At WWT, our greatest resource is not the technology in the ATC, but our people. Our Cyber Range combines our labs and our people to produce an experience unlike any other. We have strong partnerships with 200+ security OEMs, some of which have invested heavily in this Cyber Range. On behalf of WWT, I wanted to thank our partners and our staff for making this Cyber Range a reality.

Lastly, organizations must continually practice to mature their cyber tradecraft. We view our new Cyber Range as a game-changer for teams to defend and respond to advanced threats. On behalf of WWT, I wanted to thank you, our customers, for your partnership and the opportunity to collaborate.

Michael J. McGlynn

Vice President, Global Security

Table of Contents

WWT's Cyber Range

Hosted in our Advanced Technology Center, this complex environment allows companies to practice responding to specific real-world scenarios using force-on-force gameplay, evaluate advanced technologies, and integrate security controls to support a company-wide cyber defense strategy.

The WWT Cyber Range is a state-of-the-art cyber range used to evaluate the effectiveness of current and proposed security architecture and strategies against real-world attacks.

Test and evaluate advanced technologies

Customers can test networks and systems by exposing them to realistic nation-state cyber threats in a secure facility with the latest tools, techniques and malware.

Conduct force-on-force cyber games/ exercises

Train in gamified, high-pressure situations, led by people that have been on the front lines. See the impacts of untrained teams and an unprepared response plan.

Evaluate the latest security solutions in cyber protection

Engage with multiple tools to investigate a cyber incident. Experience cutting-edge capabilities, such as artificial intelligence and automated incident response solutions, and how to apply them to modern investigations.

Profile your cyber attackers in a controlled environment

Combat threats by understanding your adversaries and the tools, techniques, and processes (TTPs) they're likely to weaponize. Use real hacker tools and malware to role-play attacks in a safe and air-gapped environment.

The WWT Cyber Range has been built to accommodate even the most complex and demanding customer requirements. Through WWT's partnership with Dell and VMware, our cyber-specific software-defined data center can accommodate up to one hundred (100) concurrent users as terform complex solution evaluation, use-case driven development integrations, and gamified capture-the-flag exercises.

The following technical domains can be targeted:

- Remote worker networks
- Vulnerable web applications
- Misconfigured container environments
- Workloads spanning multiple data centers
- Unmanaged IoT and ICS devices
- Compromised third-party vendor networks
- Data exfiltration from insecure datastores

Your security stack is only as good as the people who use it. The WWT Cyber Range provides your operations team with a suite of commercial tools they'd actually use in a real-world cyber incident.

Customers can also leverage WWT's Advanced Technology Center support staff, and our expansive list of OEM partnerships, to build their own customized cyber range environment to suit their unique needs.

Growing list of technologies currently represented in the architecture

Capture the Flag 2021

WWT's 1st Cyber Range Event Exclusive to Financial Service Customers

WWT is excited to announce our first Capture the Flag (CTF) competition, tailored for our customers in global financial services. This competition is designed to help sharpen cybersecurity skills and provide hands-on learning and networking opportunities for participants. Hosting in our Advanced Technology Center (ATC), WWT's Cyber Range provides the flexible and scalable platform to facilitate these large-scale force-on-force simulations.

This CTF event's scenario focuses on a vulnerable financial institution, Iron Guardian, who is attacked by player participants on compromised third-party networks. Teams will need to attack the banking network to discover flags and win points, all while defending their own foothold from opponents.

The objective of the competition is to solve practical cyber challenges in a simulated environment. The goal of each challenge is to find a "flag" in order to receive points. Challenges award varying amounts of points depending on difficulty. The team with the most points at the end of the competition wins. In the event of a tie for points, the fastest team wins.

Each event will be an all-day experience, with the actual scenario expected to last 4-6 hours. WWT invites our customers to bring one or more teams of 3-4 players each. Up to 20 teams will compete head-to-head for points, prizes and WWT's special edition Cyber Range Challenge Coins. Our strategic partners will also present 20-min talks throughout the day (like TED Talks), providing fresh and challenging thought leadership for security practitioners.

Cyber Range Patnership Highlight

meshco™
Real Hacking — Right Now!

WWT is proud to partner with Meshco, creators of Packetwars(TM), the world's first cyber sport. Their mission is to be the premier provider of Security Themed Content, "Edutainment" and Extreme Cyber Experiences. Real Hacking - Right Now!"

Event agenda:

08:00 - Welcome

08:10 - Keynote Address

08:30 - Pre-Game Overview

09:00 - Stage 1: Reconnaissance

10:30 - Stage 2: Exploitation

12:00 - Mid-Day Break

13:00 - Stage 3: Privilege Escalation

14:30 - Stage 4: Data Exfiltration

16:00 - Post-Game Debrief

16:30 - Award Ceremony

Bank of the Future with WWT

Banks have the greatest need for an adaptable ecosystem to explore and validate reference architectures, to see how many different solutions can integrate together, to see how they function and speed and scale. But technologically, they are at a huge disadvantage.

And this is why...

Banks are weighed down by IT complexities caused by past mergers and acquisitions, tools bought by disconnected teams, and contracts renewed unnecessarily before review.

Cross-team disconnect and drawn out approval processes prevent banks from innovating at a speed that outpaces attackers and the competitive market landscape.

Being heavily regulated, with trillions of dollars at stake, prevents banks from risk-taking, exploring the "art of the possible," and making bold decisions for the future.

What gives WWT the right? Well...

WWT's $800m Advanced Technology Center is an ecosystem spanning four data centers, with a presence in Equinix for our customers, partners and employees. Through our relationships with 300+ OEMs, we bring in products quickly for proof of concepts, bakeoffs, and complex solution validation.

With over 30 years' experience building bespoke labs to support some of the largest networks in the world, our methodologies and in-house expertise make the perfect extension for our banking customers. We currently house a single customer lab that spans over 50 racks.

As a solution provider to over 40 of the world's largest banks and financial services firms, as well as 78 of the Fortune 100, we are in a unique position to understand and execute on the most critical cybersecutity threats and solution trends.

Our thought-leadering experts in security strategy, architecture and daily defense will make sure your investments garner value, adapt within your architecture, and mature your security posture now and well into the future.

A TRUE AND LOYAL PARTNER

We help some of the largest banks in the world reimagine "a better way." A perfect paring: the banks merge their prestigious goals and world-class talent with our lab capabilities, in-house SMEs and access to hundreds of OEM solutions to build their Bank of the Future lab environments.

We lend our foremost in-house application developers to weave complex security landscapes into unified, orchestrated defense platforms. OEMs alone cannot do this—but we've done it successfully for customers spread across six continents with over 800,000 devices.

We have a world-class malware detonation and testing ecosystem. Banks can see how their cyber models will operate in the real world through our Lab as a Service (LaaS). Our easily consumed modules and flexible pricing makes it fiscally conservative, yet innovative. and flexible.

We make a new world happen

We are **thinkers** and **doers**. We provide services that span strategy through execution to help solve complex business and technology challenges, accelerating meaningful outcomes for our customers globally. Our approach is the direct result of a culture that champions the courage to embrace change and the spirit of innovation to make that change count.

DIVERSITY & INCLUSION

INTEGRATED MANAGEMENT AND LEADERSHIP

We are driven to support your organization's success

Throughout the last 30 years, we have partnered with some of the world's largest organizations and developed insight and intellectual capital that reaches into every aspect of enterprise technology, across every sector of the economy. Our track record of overcoming obstacles to advance digital transformation ensures you a trusted partner on which you can rely. We provide a healthy and agile culture, a vast portfolio of services, hyperscale innovation labs and a sophisticated global supply chain. **We create new realities for our customers.**

Our greatest innovations: our people and our culture

Our employees drive the results you want. Our team is committed to your success. Our company culture is reflected in our core values, our Integrated Management & Leadership Program and our Diversity & Inclusion initiatives. These are principles we live by. They shape who we are and how we interact with each other, with our partners and with you.

Minority-owned, privately held for 30 years

7,000+ employees globally

WWT's founders, **Dave Steward** and **Jim Kavanaugh**

$13.4B in annual revenue

Global presence in 60+ countries

Technology provider to more than 70% of Fortune 100 companies

Award-winning culture, Great Place to Work 10 years in a row

A Top Partner with Cisco, HPE, Dell Technologies, NetApp, F5, VMware and Intel

Our Vision

To be the best technology solution provider in the world

Our Mission

To create a profitable growth company that is also a great place to work for all

Awards and recognition

FORTUNE 100 BEST COMPANIES TO WORK FOR 2020

glassdoor 2019 BEST PLACES TO WORK EMPLOYEES' CHOICE

Best Workplaces Great Place To Work. UK 2020

Best Workplaces Great Place To Work. SINGAPORE 2020

THE WEBBY AWARDS
PEOPLE'S VOICE 2020
HEALTH & FITNESS 2020

Plus, more than one hundred awards from our partners, clients and communities recognizing our dedication to our company culture and the innovative work we do for our customers.

Gold Sponsor: VMware

Adaptive Prevention Delivers Better Protection

The majority of today's cyberattacks feature advanced tactics such as lateral movement and island hopping that target legitimate tools to inflict damage. These sophisticated hacking methods pose a tremendous risk to targets with decentralized systems protecting high-value assets, including money, intellectual property and state secrets.

VMware Carbon Black Cloud™ thwarts attacks by making it easier to:

- Analyze billions of system events to understand what is normal in your environment
- Prevent attackers from abusing legitimate tools
- Automate your investigation workflow to respond efficiently

All of this is unified into one console and one agent, so that infrastructure and InfoSec teams have a single, shared source of truth to improve security together.

Stronger Protection with Intrinsic Security

Built In, Not Bolted On

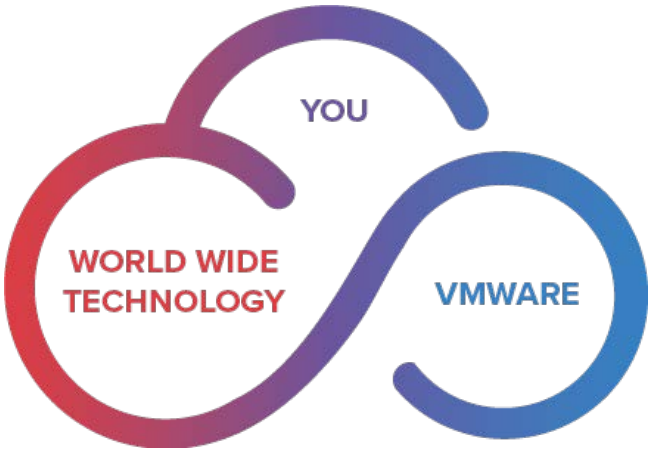
Visibility into all endpoints and workloads

Security That Provides Context

Comprehensive analysis lets you know what's good and what's bad

Security That's Unified

Simplify your existing digital infrastructure to build custom extensions



VMware in WWT's ATC

WWT's Advanced Technology Center (ATC) is a collaborative ecosystem where customers are able to explore how VMware products fit into integrated architectural solutions that further accelerate their digital transformation. The ATC, itself a software-defined next-generation data center, helps customers explore and prove out any VMware technology, including:

VMware Workspace ONE
VMware Horizon
VMware Cloud Foundation
VMware vSphere and Tanzu Kubernetes Grid Lab
VMware VMC on AWS
VMware vSAN
VMware NSX-T
VMware vRealize Automation
VMware Carbon Black
VMware Avi Ansible Automation
VMware SD-WAN by VeloCloud
VMware vCloud NFV for MobiledgeX Cloudlet

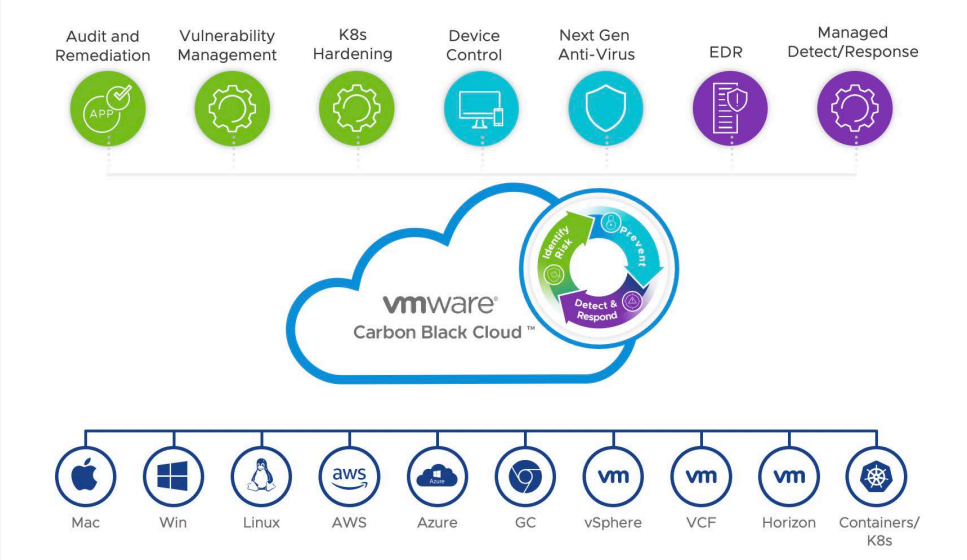
Why VMware Carbon Black + WWT

Secure and protect your infrastructure, applications and endpoint devices through built-in VMware security solutions and sound micro-segmentation strategies.

WWT and VMware work together to help you accelerate your digital transformation journey. By combining WWT's IT consulting, solutions and other services with VMware's technology platforms, we develop the flexible, scalable, and secure technology solutions you need to achieve your business ambitions.

Fueled by WWT's proven approach and powerful infrastructure, our experts help you discover, evaluate, architect and implement advanced technology lab testing in our Advanced Technology Center (ATC), and deploy rapidly through our global integration centers.

VMware Carbon Black Cloud™ is a cloud native endpoint, workload, and container protection platform that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single lightweight agent and an easy-to-use console. By analyzing more than 1 trillion security events per day, VMware Carbon Black Cloud proactively uncovers attackers' behavior patterns and empowers defenders to detect and stop emerging attacks. As a key means to realizing intrinsic security, VMware Carbon Black Cloud simplifies and strengthens your approach to security across any app, any cloud, and any device.



Better Protection

Lower TCO

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit www.vmware.com/company.

Easily implemented consistent security across environments in less than a week

Enabled frictionless collaboration between security and IT teams

Reduced complexity and saved CPU memory through security consolidation

World Wide Technology Increases Visibility Through Unified Security

As a major technology solutions provider to organizations
around the globe, World Wide Technology (WWT) has been able to operationalize consistent security across their environment while enabling a frictionless cross-team experience with VMware Carbon Black Cloud™ and VMware Carbon Black Cloud Workload™. The solutions have allowed for increased visibility and shared data between security and operations teams.

Consolidation for a single source of truth

WWT needed to consolidate their security agents to minimize operational overhead. Previously, they were using Cylance Protect for endpoint protection needs, and Tanium Threat Response for endpoint detection and response. The two agents spanned workstations, virtual desktop infrastructures (VDIs), and servers, and were taking up too much CPU memory utilization. WWT wanted to decrease compute resource utilization and simplify processes.

In addition to overconsumption of compute resources, WWT's incident response workflows were overcomplicated because their computer security incident response team relied on two separate panes of glass: Cylance for pre-breach information and Tanium for post-breach.

Increased visibility for better protection and performance

After confirming that VMware Carbon Black Cloud was the best option for WWT, the security team pivoted to rip and replace their existing Cylance and Tanium instances. In just 45 days with assistance from the VMware Professional Services group, they replaced more than 8,000 endpoints with VMware Carbon Black Cloud. The team experienced visibility right out of the box.

"What our responders noticed as soon as it was deployed was an excellent amount of visibility. A very notable improvement," says Berry. In the past, with Cylance and Tanium, the visibility was poor and required teams to go through a lengthy process of tuning. Issues with day-to-day performance was something WWT wanted to address, and by consolidating with VMware Carbon Black Cloud, "we've been able to clear up a lot of those end-user experience issues," says Berry.

> " The interface of VMware Carbon BlackCloud Workload allows security and operations teams to look at the same information without forcing them to use the same pane of glass and potentially lose functionality. Now we have shared data that we can start working together as a team to resolve challenges."
>
> MATT BERRY
> MANAGING ADVISOR, GLOBAL FINANCIALS,
> WORLD WIDE TECHNOLOGY

Securing modern workloads

WWT originally tested and purchased VMware Carbon Black Cloud, but as they started to learn more about VMware's security capabilities, their interests piqued at potential integrations with the broader portfolio. Just 5 months after their initial purchase, WWT was invited to be among the first to take part in the VMware Carbon Black Cloud Workload beta program. Being a valued customer and partner of VMware, WWT provided the dual perspective necessary to enrich the beta program.

Gold Sponsor: Rubrik

Be Security Forward.

Problem: It's not a matter of if, but when, an organization will be impacted by a ransomware attack. Organizations are destined to pay a ransom if they can't recover quickly. But ransomware isn't just costly from a payment perspective. Ransomware related outages can cost companies cost significant sums associated with lost revenues and brand damage.

Solution: Achieve security at the point of data. Our file system was built to be immutable, so backups can't be encrypted or deleted by ransomware. Use Rubrik to identify what data was encrypted and sensitive data that may have been exposed. Machine learning helps detect suspicious behavior. Then, with just a few clicks, restore back to the most recent clean state. Simply put, when an attack occurs Rubrik provides alerts that uncover unusual behavior, visibility into the

Be Data Forward.

Problem: As data continues to grow, managing infrastructure for backup, recovery, and compliance can become exceptionally complex. Organizations today require IT teams to manage all the infrastructure necessary for mission-critical applications while also delivering new services that drive innovation. In the face of mass complexity, many organizations are looking for data management solutions that can scale without compromising performance.

Solution: Cut admin time up to 90% by replacing 1000s of backup jobs with just a few policies to automate data protection across hybrid and multi-cloud IT environments. Slash recovery times from hours to minutes. Deliver near-zero RTOs to radically accelerate data access. Save money and space at the same time. Rubrik can help you reduce your data center footprint and your TCO by 30%-50%.

Be Cloud Forward.

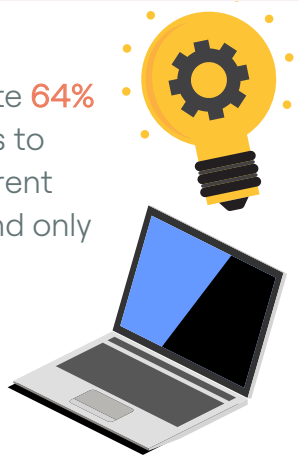
Problem: As enterprises migrate applications to the cloud, IT will need to deliver core data protection (back up, disaster recovery, and archival) at scale in the event of service outages, data loss and natural disaster.

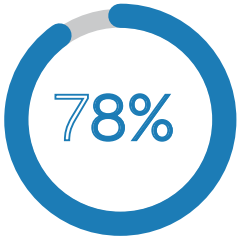
Solution: With cloud playing a greater role in overall enterprise strategy the need for a cloud-scale data management platform becomes paramount to protect and manage data born in the cloud and elsewhere. Rubrik allows you to automate at scale by eliminating manual, time-consuming job scheduling by automatically applying SLA policies (with tag-based protection). Achieve near-zero RTO's with radically simplified recovery workflows. Centrally manage backup, recovery, security, and reporting for greater visibility and control.

75%

75% of companies infected with ransomware were running up-to-date endpoint protection.[2]

IT departments currently allocate 64% of their budgets to running the current environment, and only 36% to growth and innovation.





78% of IT decision makers believe they aren't getting the most out of the cloud because of vendor lock-in concerns.

[1] 2020 Cost of a Data Breach Report, IBM Security

[2] Understanding Ransomware and the Impact of Repeated Attacks, Sophos

Rubrik + WWT

WWT and Rubrik are solving cyber resiliency challenges and providing security at the point of data. Advanced ransomware is now targeting backups - modifying or completely wiping them out. Rubrik stores all data in an immutable format, meaning that ransomware cannot access your data. But there's so much more to having a strong recovery and resiliency plan...

WWT has grown to become one of Rubrik's most strategic partners, assuring that data is stored securely and efficiently so that our customers can drive innovation. WWT and Rubrik have aligned to create a collective of experts ready to support our joint customers.

Recover from Ransomware

Statistically speaking, you are going to be breached - the question is, how quickly can you restore your data? WWT and Rubrik's data management solutions enable a continuous stream of recovery points to minimize data loss in the event of a failure, and our immutable file systems assure customers that backups cannot be encrypted or deleted by a ransomware attack.

Recover faster from ransomware.

Rubrik's Radar helps you defend against ransomware by making it faster and easier to recover from an attack. Radar proactively analyzes behavioral patterns and flags any unusual activity as your last line of defense. In the event of an attack, quickly identify which applications and files were impacted and where they are located. Easily restore to the most recent clean version of your data, whether you need to do a full or partial system restore.

Reduce sensitive data exposure.

The costs of a data breach and non-compliance with data privacy regulations are increasing. With the surge in data, it's difficult to track at-risk data. Often, this is a time-consuming, manual process. Rubrik's Sonar can automate discovery of personally identifiable information (PII) and regulated data hiding in your unstructured data. Sonar helps you accelerate compliance by creating an up-to-date inventory to meet current and future regulations and help document what sensitive data resides where. Gain instant visibility to high risk files that could be at risk of data breach or insider threat. Identify what data is potentially exposed in a data exfiltration or ransomware attack along with rapid recovery using Rubrik's core platform.

Automate DR Orchestration.

Automate recovery from errors, or ransomware attacks to reduce human error and achieve RTOs of minutes. Rubrik's Polaris AppFlows provides radically simple disaster recovery (DR) orchestration with failover/failback, testing, and compliance reporting. AppFlows allows organizations to eliminate multiple point solutions, reduce management complexity and avoid unnecessary costs.

Downtime vs. Ransom...

How about none of the above?

Organizations should not be forced to trade off paying a ransom for costly downtime. Instead they should be able to rely on their backups to recover quickly with as little data loss and financial impact as possible.

Despite advising against paying ransoms, the FBI estimates that extortionists will earn over $1 billion.[1]

Extortionists are getting more creative and utilizing various delivery mechanisms including phishing emails and exploit kits.

Problem

As enterprises adopt data-driven business models to increase agility, data has become more lucrative for cyberattacks. Even with defense mechanisms in place, ransomware attacks continue to rise and successfully encrypt organizations' data. In the first quarter of 2019 alone, ransomware attacks grew by 118% with new ransomware families detected[2].

Solution

To ensure proper protection against ransomware, best-in-breed backup and recovery vendors implement strong security controls by design. Here are a few technical requirements when evaluating the underlying architecture:

- Access to the filesystem to perform read/write operations is available to only the vendor and never to an external client.
- Vendor does not expose standard storage protocols, such as NFS or SMB, for interacting with the filesystem.
- Vendor does not allow read access of data in its native format to external clients.
- Vendor performs backup validation checks to ensure backup data is never changed, ensuring you only restore exactly what was in the original copy.
- Immutability is native to the filesystem with no user configuration or management needed.

[1] McAfee Labs Threats Report, August 2019

[2] Fall 2019 OCR Cybersecurity Newsletter - The U.S. Department of Health and Human Services

COHESITY

Silver Sponsor: Cohesity

The threat of ransomware is real, but organizations can rely on Cohesity to help counter ransomware attacks without having to pay ransom.

Cohesity's comprehensive, end-to-end solution features a multi-layered approach that enables you to protect backup data against ransomware, detect intruders, and rapidly recover from an attack.

Ransomware has grown by more than 700% in the last few years, according to Gartner,1 and the threats are becoming more sophisticated with higher monetary demands, "seed spreading" across networks, and increased targeting of backup data.

Specific areas of concern are...

- More sophisticated attacks. Cybercriminals enter through an endpoint and delete or compromise backup data before taking your production environment hostage.
- Expanding attack surfaces. Exploding data growth and the proliferation of siloed backup data have combined to make your backup data more accessible to cybercriminals.
- Intermittent monitoring. Relying on inconsistent backup ingest rates can cause attacks to be missed.
- Public cloud vulnerability. Data in the public cloud is not necessarily immune to a ransomware attack.
- Long backup and recovery cycles. Relying on legacy backups that require synthetic full backups mean that, if an attack occurs, your IT team can spend weeks in recovery mode.handles the ransomware negotiation and collecting of the ransom.

Ransomware by the numbers

Every **14 seconds** ransomware attacks

700% growth since 2016

35% of attackers get paid

$2B in financial loses

$11B in financial, productivity, and downtime issues

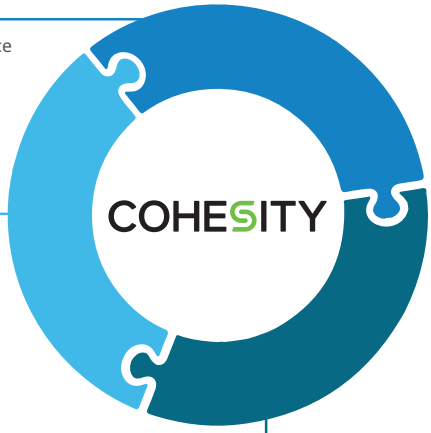
How Cohesity goes to market

Detect

Machine-driven intelligence establishes patterns and automatically reports anomalies.

Protect Backup

The immutable backup snapshots, combined with DataLock (WORM), RBAC, air-gap and multi-factor authentication prevent your backup data from becoming a target.



Rapid Recovery

Simple search and instant recovery to any point in time gets you back in business fast. Cohesity's unique instant mass restore quickly recovers hundreds of virtual machines (VMs), databases, files and objects.

Why Cohesity + WWT

The power of two in your data management technology equation

WWT's Advanced Technology Center designs, builds, educates, demonstrates, and deploys innovative technology solutions. With Cohesity's innovative technologies — now including Data Management as a Service (DMaaS) — you can efficiently protect, secure, and manage your data your way.

- **2018:** Cohesity begins their partnership with WWT in January.
- **2019:** WWT becomes a #1 ranking partner with Cohesity by August.
- **2020:** Cohesity's 2020 Partner of the Year, WWT expands to international sales.

Growing together.

Nationally recognized as a top start-up, Cohesity earned WWT Advantage Partner status in 2020. As Cohesity's fastest-growing partner, WWT became Cohesity's 2020 Partner of the Year. You're in good company.

Your business, your way.

With Cohesity's first-of-its-kind DMaaS on AWS, you choose whether to manage your data on-premise, as-a-service, or both. WWT brings a highly certified professional team committed to your success. It's your way, every day.

Outperforming the top performers.

Cohesity outperforms its nearest competitors on key criteria including Webscale Architecture, Simple Converged Management, Non-Disruptive Operations and Instant Mass Restore.* WWT has grown into a global technology solution provider to more than 70 of the FORTUNE 100.

Powered by powerhouses.

Both WWT and Cohesity partner with industry giants Cisco, HPE, and Pure Storage, as well as with the top cloud service providers AWS, Microsoft Azure, and Google Cloud. We have the power to agilely meet your needs.

Customer and community driven.

Cohesity was named a 2020 Gartner Peer Insights Customers' Choice for Data Center Backup and Recovery Solutions—for the third year running—and WWT launched a $1 million Global Community Impact program to accelerate research into COVID-19 vaccines and treatment and assist families affected by the disease.

Great places to work.

Cohesity has received numerous awards for workplace excellence from the Bay Area NewsGroup, TMCnet.com, and Entrepreneur. WWT has spent 9 consecutive years on the FORTUNE "100 Best Companies to Work For®" list.

Silver Sponsor: F5

F5 Security Solutions

Your apps' data—credentials, personally identifiable information (PII), or intellectual property (IP)—is your business's most valuable asset but it's valuable to attackers too. Today's sophisticated and quickly evolving threats often evade traditional defenses, but F5 can help.

Application security

Protect apps and APIs across architectures, clouds, and third-party integrations to reduce risk and speed digital transformation. Increase application development velocity to improve time to market and reduce friction. Protect your applications from:

- Credential-based attacks
- Software and code-level vulnerabilities (OWASP Top 10)
- Denial of Service (DoS) attacks

Access & authorization

F5 has developed best practices for secure access solutions to meet the needs of a wide variety of customers. Whether you need to quickly scale and secure your remote access solution or accelerate your zero trust application access plans, F5 can help you:

- Secure corporate apps with a Zero Trust Security Model
- Extend access management through Azure Active Directory
- Manage APIs across any data center or cloud
- Customize user experience with single sign-on (SSO)
- Enable trusted remote access with SSL VPN

Network security

Organizations need visibility and robust protection to combat attacks that traditional security solutions were not designed to defend against. Keep your network secure and available, even as network threats evolve. With F5 network security solutions you can:

- Gain visibility into encrypted traffic to stop hidden threats
- Keep your applications secure and available from DDoS attacks
- Scale to handle millions of DNS queries to ensure top performance

Online fraud prevention

Protect online commerce and digital initiatives such as customer loyalty and brand awareness by defeating attacks that compromise customer experiences and damage brand reputation—all without frustrating users. F5 can help protect your organization from:

- Account takeover attacks
- Inventory hoarding
- Content scraping
- Carding
- Skewed analytics

Explore F5's On-Demand security labs

- Secure Cloud Architecture — Financial Services
- Privileged User Access - Financial Services
- Advanced Web Traffic Visibility with F5 SSL Orchestrator
- Hybrid Cloud Identity and Access
- Declarative AWAF Policy Lifecycle in CI/CD Pipeline

Explore F5's most popular labs

- Red Hat OpenShift Lab
- Ansible Automation Training Lab
- Terraform Automation Lab
- Advanced Web Traffic Visibility With F5 SSL Orchestrator
- Adaptive Application Services with NGINX

Security use cases

- Manage and secure APIs
- Mitigate app vulnerabilities
- Mitigate bots and automated attacks
- Inspect encrypted traffic for threat analysis
- Stop human-driven fraud

Click here to learn more about F5 security solutions

F5 & WWT: a true partnership

WWT and F5 are focused on delivering value to our customers through our innovative technology solutions to digitally transform their organizations. Together, we provide market leading services and capabilities to support customers with quickly achieving their desired business outcomes. Our joint security and strategic services and solutions deliver elevated and continuous protection from sophisticated online attacks, leveraging F5's world-class software development services. WWT and F5 work side-by-side to drive significant customer impact by helping customers be more efficient and do less, better.

Partnership awards

North America Partner of the Year	North America Partner of the Year	North America Partner of the Year	Innovation Partner of the Year
2020	2018	2016	2015

F5 in WWT's ATC

WWT has a wide array of F5 technology integrations. The Advanced Technology Center (ATC) is a collaborative ecosystem comprised of a rich set of F5 demos and labs that allow customers to view new product functionality, while on-demand sandbox environments provide engineering teams with technology stick time. This software-defined next-generation data center enables customers to explore F5 technology and further accelerate their digital transformation, faster.

Available demos

- Automating F5 and Infoblox IPAM Configurations using Ansible Tower
- F5 Self-Service Requests using Ansible Tower and ServiceNow
- F5 Federated Single-Sign On using Okta and F5 APM
- F5 Multi-cloud Management with F5 BIG-IQ and F5 Cloud Edition
- Advanced Traffic Inspection using F5 SSLO Service Chaining
- RDP and SSH Multifactor CAC Authentication with F5 PUA and F5 APM
- Web Application Security with F5 ASM/Advanced WAF
- Integrating F5 with OpenShift using F5 Container Connector
- Dedicated F5 Automation Sandbox containing Ansible Tower, Infoblox IPAM, Docker, and F5 LTM

Why F5?

Secure and deliver extraordinary digital experiences	Simplify traditional application delivery	Enable modern app delivery at scale	Secure every application wherever it's deployed	Use data to unlock the value of insights and automation

Silver Sponsor: FireEye

To successfully predict, prevent, detect, respond to and recover from cyber attacks, you need in-depth knowledge of attackers, their tactics, and their techniques. You also need to be able to automate your intelligence capabilities and security investments to scale their use as needed.

After choosing the right intelligence-led security solution, you need to apply an effective automation strategy. When your organization is attacked, you can immediately put your security tools, teams, and techniques to work mitigating those threats.

And automation of security effectiveness validation can also help ensure that your intelligence is up to date, which can reduce risk and maximize the value of your intelligence and security investments.

Top 3 cyber security concerns for the enterprise

The number of ransomware incidents Mandiant has responded to has doubled every year for the last three years. Not only did adversaries get smarter—they also began working together. While one group of attackers might focus on establishing a foothold, another would follow up by spreading malware, and a third might handle ransom negotiation and collection.

Digital transformation that moves services, data, and apps into the cloud can reveal or create gaps and vulnerabilities. To better protect your assets, you need to analyze the efficacy of current security programs and specific security controls and practices, ensure proper deployment, integration, and configuration of services, assess the stack against known vulnerabilities, and configure your security solutions based on industry and regional risks.

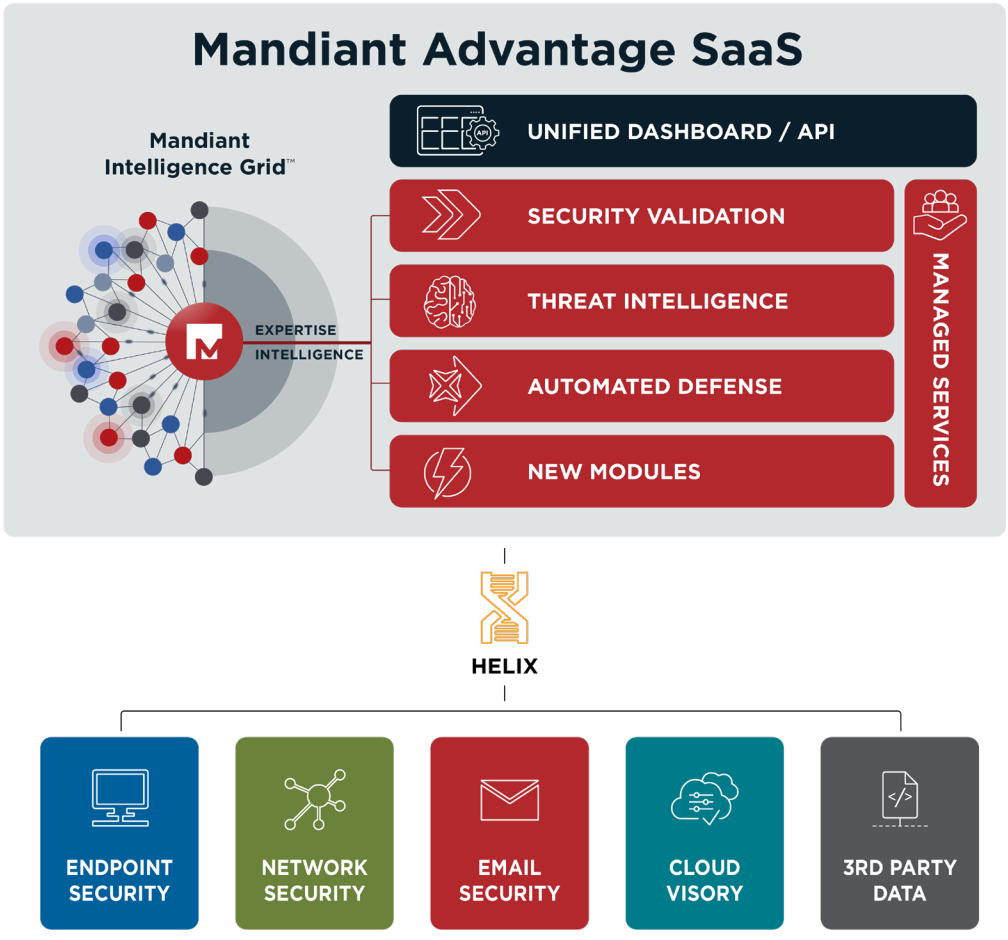
When it comes to IT expertise, talent and resources, not only can overhead be steep, but hiring niche expertise can be both risky and costly. Organizations need reliable and efficient ways to supplement internal resources. Working together, WWT and FireEye can equip your teams with expertise and technologies that enable more efficient, effective and proactive security. Ultimately, you'll be better able to defend against threats, design programs, and respond to incidents.

The FireEye & WWT partnership

Together, the team of FireEye and WWT create a security powerhouse that helps organizations, predict, prevent, resolve, and recover from known, advanced and unknown malware attacks. For example, customers are using WWT's ATC lab ecosystem to test and prove FireEye solutions in a controlled, simulated replica of their own environment to determine how effective they will be, which one works best for their needs, and how to maximize its potential. A win-win for all!

Act deliberately, security definitively. First, choose the right intelligence solution to know who the attackers are, what malware they're using, which industries they're attacking, and how to identify their IOCs and TTPs. Next, operationalize, personalize, and validate your security with automation to get the most from your intelligence.

Intelligence should not be a report that sits in your inbox, a monthly check-in with your intelligence team, or a dashboard used during an investigation. You want intelligence to lead your security efforts. And you can get that with intelligence-led security from WWT, FireEye, and Mandiant solutions.



Silver Sponsor: Fortinet

WWT and Fortinet Datacenter, Network Edge, Operational, and Distributed Workforce Security Strategies

Best Practice Solutions and Services for NGFW, SD-WAN, SASE, Endpoints, Teleworkers, and OT.

In response to the ever-increasing cyber attacks that threaten security landscapes within the enterprise, the security experts at WWT and Fortinet have partnered to provide best-in-class solutions and services including:

- WWT's Advanced Technology Center(ATC) to facilitate lab tests, proofs of concept (POCs), and integrated solution demonstrations across the Fortinet Security Fabric
- Zero Trust security model expertise and implementation
- Software-defined wide area networking (SD-WAN) solutions and services
- Secure access service edge (SASE) and Remote Teleworker
- Endpoint security solutions and operational technology (OT) security best practices and ICS expertise
- Security Challenges

WWT and Fortinet partnership

WWT and Fortinet collaborate to drive market evolution with security-driven networking and consolidated industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection and automated threat protection. WWT and Fortinet meet performance needs of highly scalable, hybrid IT architectures, enabling organizations around the world to reduce complexity and manage security

Partnership awards

Fortinet Partner of the Year	Fortinet National Partner of the Year	Fortinet Partner of the Year	Fortinet FED Partner of the Year
2020	2019	2018	2017

Fortinet in WWT's ATC

Fortinet Solutions

- NGFW-HA6501,7060,3700,100
- VM04,08,32
- Secure SDWAN POC and Lab
- Fortinet Teleworker
- ZTNA w FortiNAC
- FortiSandbox
- FortiSwitch,FortiMail,FortiDDOS

POCs

- NGFW Perimeter Testing
- SDWAN
- Ultra Low Latency
- Integration Testing

Integration testing

- Public Cloud Segmentation – NGFW
- Next Generation Central Office: Cloudify Orchestration for Fortinet SD-WAN
- Fortinet FGT integration in ACI using PBR Service Graph redirection Lab
- Equinix Network Edge with Fortinet SSL-VPN

About Fortinet

Fortinet is the #1 cybersecurity company in the world with 480,000 worldwide customers and more than 30 cybersecurity product lines, including advanced solutions for NGFW,SD-WAN, Teleworkers, SASE,OT, and Endpoints. Fortinet secures the largest enterprises and government organizations around the world with intelligent, seamless protection across an expanding.

www.fortinet.com

Together, Fortinet and WWT are addressing these top security challenges

SD-WAN

Security-driven networking for branch networks with outstanding performance enabled by fast application identification and automated path intelligence.

- Application awareness for improved service levels
- Optimal application experience with accurate detection
- Effective business policies based on application signature
- Continuous application database updates from FortiGuard Labs research

Zero Trust model

WWT has found that adopting a Zero Trust security model should be consideration in all security plans. The proven framework dictates that trust extends beyond network proximity and Internet-of-Things (IoT) devices. Trust should never be assumed, but instead proven through a set of intentional actions, such as device and user verification.

- WWT can help your team implement a Zero Trust model using a five-step process:
- Expand your audience by securing alignment and executive support within your firm
- Address asset discovery inventory by gaining visibility into all IoT devices and endpoints
- Understand data classification by ensuring you have a set of data labels and data tags
- Address user and device access by implementing the right identity access technologies
- Address enterprise segmentation risks by dividing your network into isolated segments

SASE

Ensures security for every edge and solves much of the scalability and infrastructure issues that arise in large, distributed organizations that are highly dependent upon Infrastructure-as-a-Service (IaaS)/Software-as-a-Service (SaaS).

- Combines network and security functions with WAN capabilities for dynamic, secure access
- SASE solutions bring security to the edge and solve infrastructure vulnerability issues
- WWT offers expertise, test labs, and concept testing to determine appropriate SASE solutions
- Industry-leading managed security services backed by multiple security operations centers

Teleworkers

Advanced security controls for remote teleworkers including FortiGate virtual private networks (VPNs), FortiToken identity authentication, FortiAP secure wireless connectivity, and FortiGate next-generation firewalls (NGFWs).

- Defend against escalating cyberattacks on unsecure remote workforces
- Ensure the right hardware processing power to support encrypted tunnels for remote workers
- Create safe connections by combining FortiClient endpoint fabric agents with FortiGate NGFWs

Operational technologies

WWT and Fortinet operational technology cyberthreat solutions integrate with an automated security architecture to deliver visibility, control, and real-time traffic analysis to proactively neutralize threats.

- Single-vendor, end-to-end, integrated cybersecurity architecture across IT and OT, from protection to detection to response
- Provide visibility on OT risks to identify assets and potential vulnerabilities, provide proactive threat defense, and classify and prioritize risks
- Minimize risk by constantly analyzing traffic for threats and vulnerabilities
- Control access through role-based access and identity management
- Secure both wired and wireless access, including bring-your-own-device (BYOD) devices

Endpoints

WWT experts have found that traditional endpoint detection and response (EDR) solutions often require manual triage and responses that are not fast enough to stay ahead of risks. They also create a large volume of "false positive" alerts that burden analysts and security teams. To properly secure endpoints, WWT recommends the following:

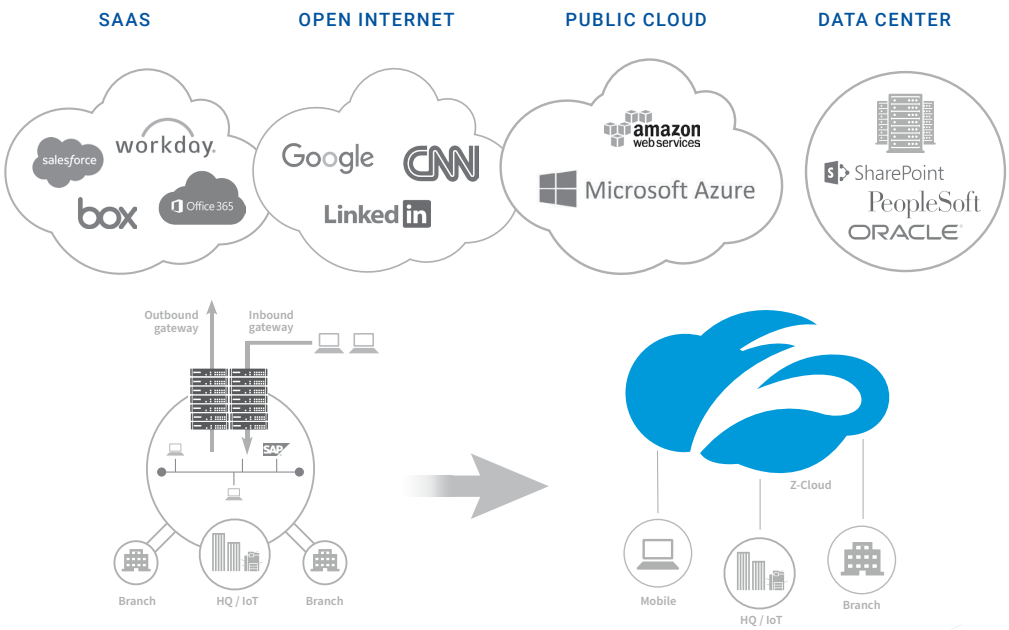
- FortiEDR advanced, real-time, pre- and post-infection threat protection for endpoints
- FortiClient to strengthen endpoint security through integrated visibility, control, and defense
- WWT services to ensure compliance, mitigate risks, and reduce false positive alerts

Silver Sponsor: ZScaler

Enabling secure transformation to the cloud is no longer a question of if. It's a question of how.

Welcome to the era of cloud and mobility. Your applications are moving to the cloud — Salesforce, Office 365, AWS, and Azure — but your security appliances are still sitting on-premises, protecting your corporate network. And, if you no longer control the network, how can you protect users and applications?

To secure this new world of IT, you simply need a new approach. One that transforms the way applications are accessed and security controls are enforced. Zscaler provides an architectural approach to secure IT transformation, in which software-defined policies, not networks, securely connect the right user to the right app or service.



FROM

Hub & spoke architecture

- Secure the network to protect users and apps
- Internal app access requires network access
- All users must be on the network for protection
- Internet traffic must be backhauled for protection

TO

Cloud-enabled architecture

- Cloud-enabled architecture
- Software-defined policies connect users to apps, not networks
- Access policies determine which apps are visible and which are dark
- On-net or off-net, the protection is identical
- Secure local Internet breakouts

What sets Zscaler apart?

- Full inline content inspection
- Native SSL inspection
- Cloud intelligence
- Real-time threat correlation
- 60+ industry threat feeds

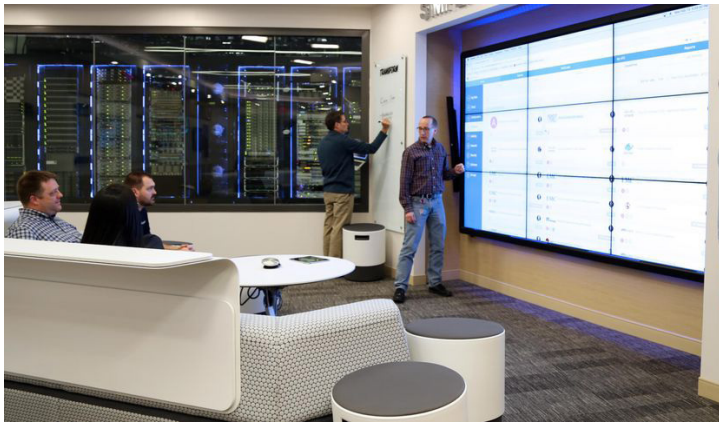
The Zscaler architecture is the best approach for secure SD-WAN and Office 365 deployments

In it together.

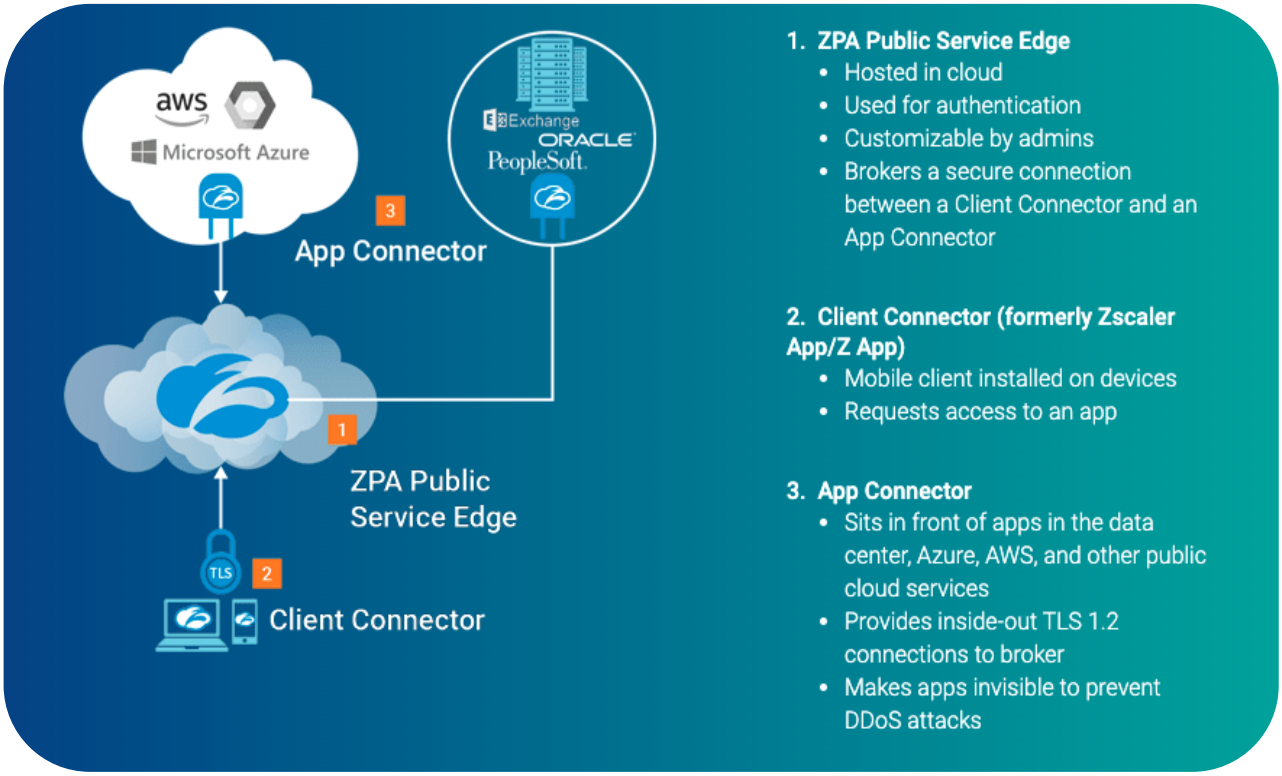
Zscaler & WWT: Rethinking networking and security to support your company's transformation

WWT is a Zscaler Zenith Partner, the highest level of attainment in the Summit Partner Program. The Security and Networking practices at WWT, along with the capabilities in the Advanced Technology Center (ATC), are helping clients transform their security to the Cloud as they migrate workloads from on-prem to the cloud.

Whether you're upgrading your Security posture, moving to Gartner's recommended Secure Access Services Edge (SASE) architecture, or implementing SASE or Zero Trust Networking Access (ZTNA), WWT and Zscaler will work with you collaboratively to support your networking and security needs.



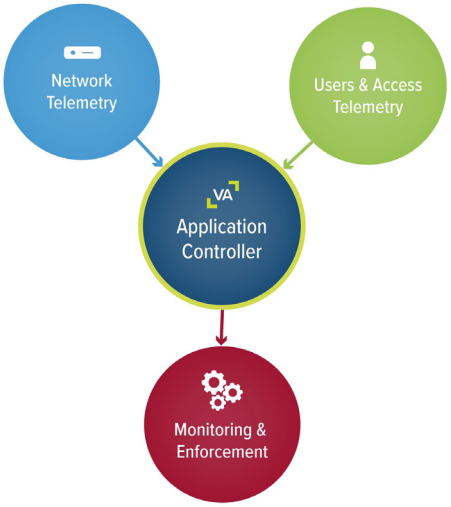
See Zscaler in action with the WWT's ZeroTrust lab in WWT's ATC



vArmour

Relationships Matter

Bronze Sponsor: vArmour



Every application, every user, every data element.

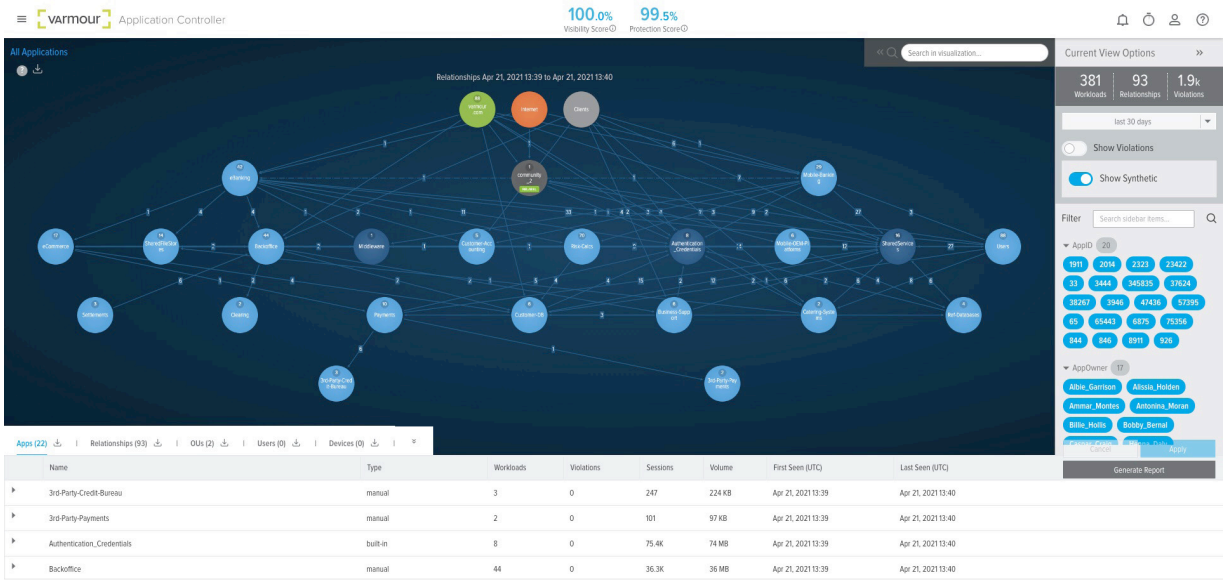
vArmour enables organizations to protect their data, digital assets, and themselves through a complete understanding of all applications and identities—and the information relationships between them.

vArmour, the leading provider of Application Relationship Management.

vArmour is the leading provider of advanced Application Relationship Management (ARM) software designed to solve contemporary security, risk, and operational challenges now prevalent due to the growth of the "digitally defined" enterprise.

In the world of zero perimeters and accelerated digital transformation, businesses are more dependent than ever on connecting people within and outside the enterprise, and on applications that connect with one another between cloud and legacy environments. vArmour's transformative approach to security enables organizations to protect their data, digital assets, and themselves through a complete understanding of all applications and identities—and the information relationships between them.

vArmour's unique, API-first approach leverages an enterprise's existing infrastructure and does not require additional agents or appliances. The platform identifies, maps, monitors, and controls relationships among users, apps, and data regardless of source. This enables organizations to accelerate their Zero Trust journey and create business and security policies to secure their assets and their business, significantly decreasing risk, ensuring compliance and building resiliency.



Map relationships across your entire dynamic enterprise in one view.

To learn more, visit www.varmour.com
or contact alliances@varmour.com

OEM partnerships

WWT partners with the world's leading technology manufacturers to amplify the value of their solutions. We maintain the highest levels of certification and feature a wide array of OEM products in our Advanced Technology Center (ATC). Our global supply chain operation is tightly integrated with our OEM Partners and has become a vital resource in helping our customers accelerate technology deployment.

Strategic partnerships

Advantage partnerships

Disruptive partnerships

Our security experts & client executives

To learn more about our security offerings or to see how WWT's security practice can help your organization be secure as humanly and technologically possible, reach out to someone helpful our team.

Meet the team

Chris Konrad
Director, Global
Financial Security
Chris.Konrad@wwt.com

Matt Berry
Managing Advisor Security,
Global Accounts
Matt.Berry@wwt.com

Chris Nicholson
Client Executive, GES
Global Accounts
Chris.Nicholson@wwt.com

Tracy Sever
Client Executive, GES
Global Accounts
Tracy.Sever@wwt.com

Lamar Hawkins
Solutions Architect, GES
Global Field Engineering
Lamar.Hawkins@wwt.com

World Wide Technology

Make a new world happen.