Overview

Solving the Attack Surface Risk Management Challenge

Executive summary

The global pandemic has forced organizations to deal not only with health, safety, and supply chain challenges, but also with increasing political turmoil that can negatively impact ongoing operations. Digital transformation has accelerated to an almost frenetic pace, introducing a level of complexity to the IT ecosystem that is difficult to manage and driving increased cyber risk.

As organizations drive forward and support the realities of hybrid working, cloud-first application delivery, and an IT infrastructure that is continuously changing, the digital attack surface must be a focus for better managing overall business risk. Trend One, a unified cybersecurity platform that builds on over 30 years of experience, foresight, and innovation, addresses these critical challenges by enabling organizations to better understand, communicate, and mitigate cyber risk across the enterprise.

Continuous digital transformation

The world we know is changing at a pace that is exciting but also overwhelming. Digital transformation, accelerated by the needs of the global pandemic, has introduced changes to all aspects of the enterprise.

Remote work, necessitated for safety reasons, is expected to remain a permanent reality of the global workforce, which has turned short-term elevated risk into increased long-term exposure.[1] Supporting new business goals and a remote workforce's needs have changed the way the cloud is used. While initially focused on the migration of existing applications to the cloud, more organizations—increasing to 50% in 2022[2]—are adopting a cloud-native approach and shifting their cloud strategy for supporting both employees and customers.

Adding complexity is the fact that the number of connected devices continues to increase dramatically, with over 55.7 billion devices worldwide expected by 2025[3]. This includes not only traditional devices, but also operational technologies (OT) that are a critical part of the manufacturing supply chain.

These changes impact more than just the IT department, with technologies like cloud and artificial intelligence (AI) potentially changing company culture, business operations, customer experience, and more.

Digital transformation is also not happening in isolation. Geopolitical instability and increasingly impactful data privacy regulations like the GDPR make risk management even more complex.

An increasingly complex attack surface

Digital transformation has unquestionably increased our ability to deliver more, faster. However, it also introduces a new level of complexity that is challenging IT and SecOps teams to deal with an increasingly complicated attack surface while using multiple disconnected security tools.

From more modern challenges like open-source vulnerabilities, misconfigured cloud services, and use of unsanctioned SaaS applications to traditional issues like unpatched operating systems and endpoint or network vulnerabilities susceptible to threats like ransomware, the digital attack surface is a primary source of cyber risk for an organization.

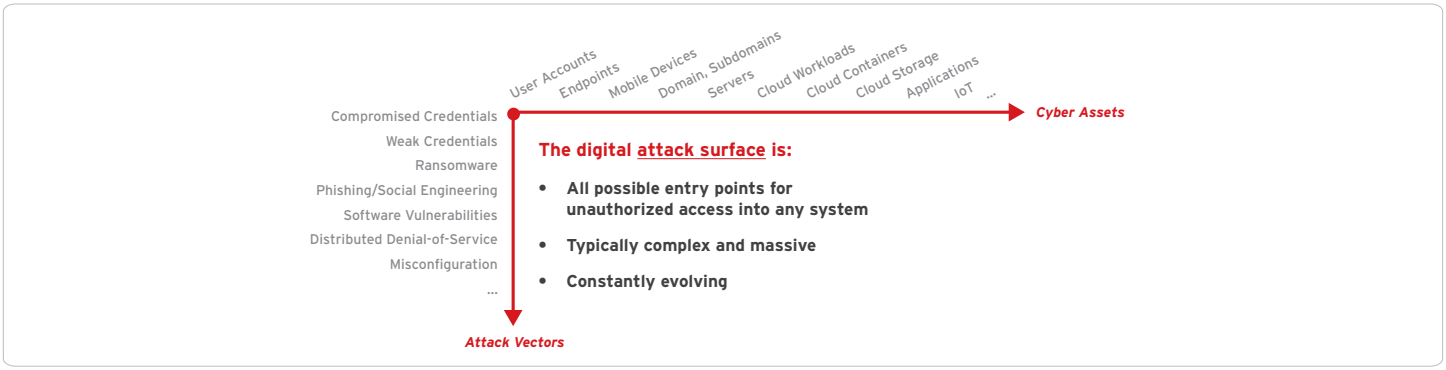


Figure: The digital attack surface of a modern organization

[1] Gartner, 2022 Planning Guide for Security and Risk Management, October 2021

[2] Forrester, Predictions 2022: Cloud Computing", October 27, 2021

[3] IDC, IoT Growth Demands Rethink of Long-Term Storage Strategies, Jul 2020

Regardless of the tactics used, this broadened attack surface is where threat actors will focus their efforts. This impacts organizations in multiple ways, including how cyber insurance is used as a part of a risk management strategy.

The rampant success of ransomware attacks over the past few years has transformed the cyber insurance industry. Many new requirements—including mandating the use of endpoint detection and response—were added to insurance renewals. Along with critical issues like lost revenue, it's clear that security leaders have a lot to deal with.

Trend Research's 2023 predictions report[4] highlighted that organizations need to remain vigilant and focused on cyber risk management. We believe attacks will shift left, targeting DevOps tools and the development pipeline, including developer credentials and build systems that can serve as entry points for spreading malware across multiple companies via supply chain attacks.

Our researchers believe that vulnerabilities will be weaponized in record time, with more zero-day exploits and an influx in blended attacks that will target multiple software products at once by daisy-chaining.

We also see that ransomware impacts are going to continue to intensify, which is daunting given that multiple industry surveys suggest that most organizations were impacted in some way by ransomware in 2022. With Ransomware-as-a-Service (RaaS) providers like REvil and Conti, who were responsible for millions of attacks globally, we believe that ransomware will become more targeted, with attackers strong-arming prominent victims into paying large sums of money via quadruple extortion.

TOP 5 negative consequences of an attack:

1. Lost revenues
2. Stolen or damaged equipment
3. Customer turnover
4. Cost of outside consultants and experts
5. Disruption or damages to critical infrastructure

Source: The cyber Risk Index 2H-2021, Trend Micro Research and Institute, March 2022

Managing and communicating risk is complex

While managing the attack surface is critical, having the skills and ability to do so is challenging. Despite an increase in cybersecurity professionals in 2022, there is still a global cybersecurity skills shortage of over 3.4 million people[5].

Lack of resources and skills makes effectively managing attack surface risks introduced by disconnected tools, siloed data, and alert overload increasingly challenging for security teams. This is compounded further by the fact that users, applications, and data can be anywhere and compliance with challenging data privacy regulations is increasingly important for the businesses.

Equally important and challenging is the task of communicating risk. Cyber risk has become a board-level concern, with almost 1 in 3 business leaders citing cybersecurity as the biggest business risk today[6] according to our global risk study. And yet, less than 50% of non-security focused C-levels fully understand the risks of cybersecurity.

Communicating risk is challenged by the realities you face daily: too many alerts, limited visibility, silos of data, and security tool overload. 62% of IT leaders said that better reporting and insights to help explain the business risk of cyber threats were essential. Given 82% have felt pressure to downplay the severity of risk to the board, the need for better tools to help communicate risk has never been greater.

Close to

1 in 3

IT decision leaders cite cybersecurity as the top business risk

Source: Trend Micro Global Risk Survey of IT Decision Makers and C-Level Executives, October 2021

[4] Trend Micro Security Predictions for 2023: Future/Tense

[5] ISC2 Cybersecurity Workforce Study 2022

[6] Trend Micro Global Risk Survey of IT Decision Makers and C-Level Executives, October 2021

Managing the digital attack surface lifecycle

Your digital attack surface is both complex and dynamic, making it an attractive target for attackers. To better manage your cyber risk, it is important to treat it as a lifecycle that requires constant management.

You need to be able to continuously discover your evolving attack surface across all environments, gathering key data that enables you to assess potential risks.

Risk can be found in individual or multiple elements of the attack surface, making it difficult to understand your risk posture at any given moment.

Furthermore, risk mitigation can come in multiple forms, including configuration changes, policy adjustments, and applying specific security controls to both proactively prevent an attack or quickly stop an attack in progress.

As the attack surface can change at any moment—for example, mid-session for a user that is compromised and starts to act suspiciously—it is critical that you are able to continuously monitor and assess your cyber risk with visibility across your entire IT ecosystem.

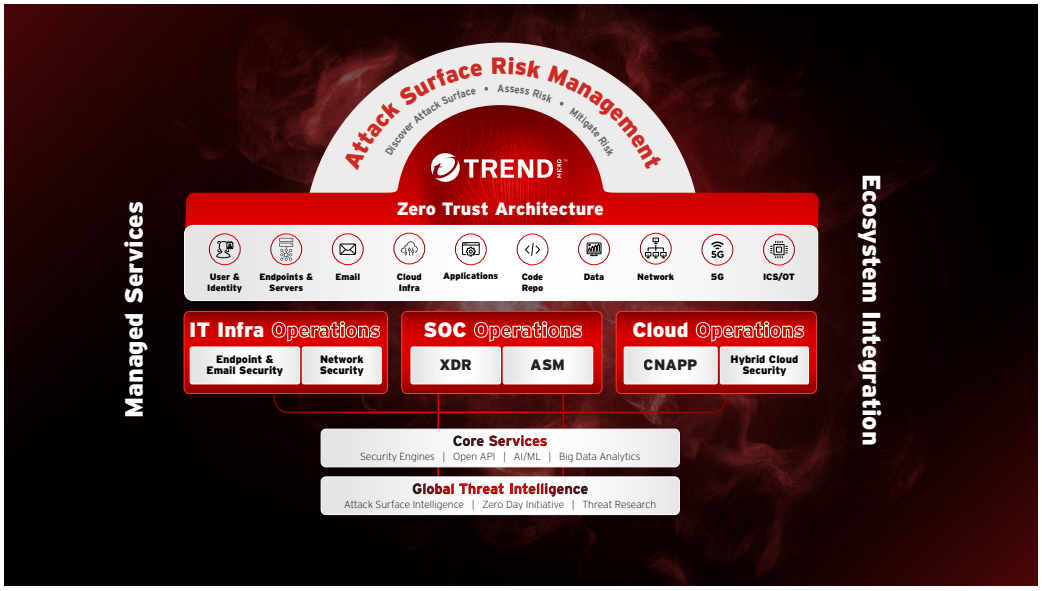
Trend One: a unified cybersecurity platform

Building on over 30 years of experience, foresight, and innovation, Trend One is a unified cybersecurity platform that enables organizations to understand, communicate, and mitigate cyber risk across the enterprise.

Security professionals are empowered to continuously discover their ever-changing attack surface, understand and prioritize vulnerabilities, rapidly detect and respond to threats, and apply the right security at the right time to mitigate risk.

Built-in security capabilities like industry-leading XDR, risk insights, and threat assessment combined with deep integration across the broader IT infrastructure helps security operations teams manage the attack surface risk lifecycle more effectively with fewer resources.

With broad protection capabilities across the entire enterprise, Trend One empowers organizations to be more agile and adapt quickly to new business and compliance needs, including supporting security strategies like Zero Trust and helping to address cyber insurance requirements. With unparalleled threat intelligence and vulnerability insights from our global threat research team and expert services like managed XDR and incident response, Trend One is designed to help you better manage your digital attack surface lifecycle.



Detect and respond to attacks faster

Fueled by industry-leading XDR[7] capabilities, Trend One helps you see your full security picture with native sensors across endpoint, email, cloud, IoT/OT, and network environments. These native sensors enable the platform to collect data for correlated detection, in-depth investigation, and threat hunting.

In addition, integration with a growing list of ecosystem partners—firewalls, vulnerability management products, Microsoft Active Directory (AD), SIEMs, and SOARs—delivers more data for analytical enrichment, as well as optimizing processes and workflows.

The result is rapid identification and correlation of activities to produce high-confidence detections—with the power to search, investigate, analyze, and respond from a single console. Combined with comprehensive visibility, your security teams are empowered to improve response time by 70%[8] and better communicate cyber risk to key stakeholders, including senior executives and the board.

Simplify and strengthen cloud security

Designed for cloud builders, Trend One delivers security automation, customizable APIs, and turnkey integrations to meet your cloud security needs across AWS, Microsoft Azure, Google Cloud, and more.

Trusted by more organizations worldwide to protect their digital transformation projects in the cloud[9], Trend One includes powerful capabilities for managing your cloud security posture, assessing risk from open-source code, and protecting your workloads, containers, serverless, storage, and cloud networks. Delivered as a cloud-native platform, it not only helps to strengthen cloud security and lower your risk, but can also increase your security investment ROI by up to 188%[10].

Secure your workforce on any device, any application, anywhere

Whether your enterprise is working remotely, from the office, or in a hybrid model, you need to be able to protect your users wherever they are from today's ever-changing threats, like fileless malware, targeted attacks, ransomware, and cryptomining.

A consistent leader in protecting the enterprise workforce according to Gartner[11] and Forrester[12], Trend One delivers multiple layers of advanced security that can adapt, predict, and stay ahead of threats across the endpoint, email, web, and SaaS applications like Microsoft 365.

Protect your network from zero-day attacks and advanced threats

The network has expanded far beyond traditional offices—it now includes not only remote branches but also cloud and mission-critical operational environments like factories and more.

Trend One goes beyond traditional network protection with capabilities that help you detect the unknown and protect the unmanaged, including IT and OT resources.

Backed by the Trend Micro™ Zero Day Initiative™ (ZDI), the world's largest bug bounty program, you can defend against undisclosed threats an average of 102 days before a vendor patch is released. This early protection helps you to better mitigate your attack surface risk while enabling the organization to innovate and drive digital transformation forward.

---

[7] Forrester New Wave: Extended Detection and Response (XDR), Q4, 2021

[8] ESG: Analyzing the Economic Benefits of Trend Micro Vision One, May 2021

[9] Worldwide Cloud Workload Security Market Shares, 2020 IDC #US47837121, June 2021

[10] Forrester TEI Study: Trend Micro Cloud One, June 2021

[11] Gartner "Magic Quadrant for Endpoint Protection Platforms," by Rob Smith, Paul Webber, Mark Harris, Peter Firstbrook and Prateek Bhajanka

[12] The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021

Security experts ready, willing, and able, 24/7/365

Scarce and overburdened resources impact both your ability to manage the attack surface lifecycle as well as effectively communicate risk across the organization. With Trend One, limited resources don't have to slow you down. Our world-class experts can help you to be more resilient with premium support that focuses on getting you up and running fast while ensuring your solutions are optimally configured. Managed XDR can help identify and investigate threats, and incident response services are ready to assist during critical attacks.

Leveraging our in-depth knowledge gleaned from over 500,000 customers and 250 million global sensors, our targeted attack detection service scans for early indicators of compromise (IoC), providing proactive, qualified high-risk alerts of potential threats with expert resources to help you take quick action.

Simplify security in a complex digital landscape

The world is a complicated place, getting more and more complex every day. Your attack surface is constantly changing as you support digital transformation and evolving business goals. You need to be able to manage risk across your digital attack surface by continuously discovering, assessing, and mitigating risk. We can help.

Trend One is a unified cybersecurity platform that enables you to understand, communicate, and mitigate cyber risk across your organization. It includes key capabilities like XDR, attack surface risk management, and market-leading protection across your IT infrastructure, enabling you to support strategies like Zero Trust and better manage your business risk, including cyber insurance requirements. Combined with unparalleled threat intelligence and vulnerability insights from our global threat research team, our unified cybersecurity platform truly enables your organization to go further and do more.